Guía del usuario

AWS Organizations

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Organizations: Guía del usuario

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

¿Qué es AWS Organizations? 1
Características de AWS Organizations 1
Precios de AWS Organizations 4
Acceso a AWS Organizations 4
Soporte y comentarios de AWS Organizations 5
Otros recursos de AWS 5
Introducción a AWS Organizations 7
Más información sobre... 7
Terminología y conceptos de AWS Organizations 7
Tutoriales 14
Tutorial: Creación y configuración de una organización 14
Requisitos previos 16
Paso 1: Crear la organización 16
Paso 2: Crear las unidades organizativas 19
Paso 3: Crear las políticas de control de servicios 22
Paso 4: Probar las políticas de la organización 27
Tutorial: supervisión con Amazon EventBridge 27
Requisitos previos 29
Paso 1: Configuración de un registro de seguimiento y un selector de eventos 29
Paso 2: Configuración de la función Lambda 31
Paso 3: Creación de un tema de Amazon SNS que envía correos electrónicos a los suscriptores 32
Paso 4: Creación de una regla de Amazon EventBridge 32
Paso 5: Comprobación de la regla de Amazon EventBridge 33
Limpieza: Elimine los recursos que ya no necesite 35
Prácticas recomendadas para la administración de varias cuentas 36
Administrar cuentas dentro de una sola organización 36
Utilizar una contraseña segura para el usuario raíz 37
Documentar los procesos para el uso de las credenciales de usuario raíz 37
Habilitar MFA para las credenciales de usuario raíz 38
Aplicar controles para monitorear el acceso a las credenciales del usuario raíz 39
Mantener actualizado el número de teléfono de contacto 39
Utilizar una dirección de correo electrónico de grupo para todas las cuentas raíz 40

Agrupar cargas de trabajo en función del propósito empresarial y no de la estructura de informes ... 40
Utilizar varias cuentas para organizar cargas de trabajo ... 40
Habilitar los servicios de AWS en el nivel de la organización mediante la consola de servicios o las operaciones de la API o de la CLI ... 41
Utilizar las herramientas de facturación para realizar un seguimiento de los costos y optimizar el uso de los recursos ... 41
Planificar la estrategia de etiquetado y la aplicación de las etiquetas en todos los recursos de la organización ... 41
Prácticas recomendadas para la cuenta de administración ... 42
Limitar quién tiene acceso a la cuenta de administración ... 42
Revisar quién tiene acceso y realizar un seguimiento ... 42
Utilice la cuenta de administración solo para tareas que requieren la cuenta de administración ... 43
Evitar la implementación de cargas de trabajo en la cuenta de administración de la organización ... 43
Delegar responsabilidades fuera de la cuenta de administración para la descentralización ... 43
Prácticas recomendadas para cuentas de miembros ... 44
Definir el nombre y los atributos de la cuenta ... 44
Ampliar el entorno y el uso de la cuenta de manera eficiente ... 44
Utilice una SCP para restringir lo que puede hacer el usuario raíz en tus cuentas de miembro ... 45
Creación y administración de una organización ... 47
Creación de una organización ... 48
Crear una organización ... 48
Verificación de dirección de correo electrónico ... 51
Habilitar todas las características ... 52
Antes de habilitar todas las características ... 52
Comienzo del proceso para habilitar todas las características ... 54
Aprobación de la solicitud para habilitar todas las características o volver a crear el rol vinculado al servicio ... 57
Finalización del proceso para habilitar todas las características ... 60
Consultar detalles de la organización ... 63
Consultar detalles de una organización desde la cuenta de administración ... 63
Visualización de los detalles del contenedor de nodo raíz ... 65
Consultar los detalles de una unidad organizativa ... 66

Consultar detalles de una cuenta ... 69
Consultar detalles de una política ... 70
Eliminar una organización ... 73
Eliminar una organización ... 74
Administración de las Cuentas de AWS de su organización ... 76
Impacto de estar en una organización ... 76
¿Cuál es el impacto en un Cuenta de AWS que une una organización? ... 76
Impacto en una Cuenta de AWS que se crea en una organización ... 77
Invitar a una cuenta a su organización ... 78
Envío invitaciones a Cuentas de AWS ... 80
Administrar las invitaciones pendientes de su organización ... 83
Aceptar o rechazar una invitación de una organización ... 88
Creación de una cuenta miembro ... 92
Crear una Cuenta de AWS que forme parte de la organización ... 94
Acceso a las cuentas miembro ... 97
Acceso a una cuenta miembro como usuario raíz ... 99
Crear la OrganizationAccountAccessRole cuenta en un miembro invitado ... 99
Acceso a una cuenta miembro con un rol de acceso a la cuenta de administración ... 101
Exportación de los detalles de las cuentas ... 104
Exportación de una lista de todas las Cuentas de AWS de su organización ... 104
Eliminación de una cuenta miembro ... 106
Consideraciones antes de eliminar una cuenta de una organización ... 106
Eliminar una cuenta de miembro de su organización ... 108
Abandonar una organización desde su cuenta de miembro ... 112
Cerrar una cuenta miembro ... 116
Cómo cerrar una cuenta miembro ... 116
Protección de cuentas miembro contra el cierre ... 118
Cerrar una cuenta de administración ... 120
¿Cómo cerrar una cuenta de administración ... 120
Actualización de contactos alternativos ... 121
Actualización de la información de contacto principal ... 121
Actualización habilitada Regiones de AWS ... 121
Administración de políticas de la organización ... 123
Tipos de políticas ... 123
Políticas de autorización ... 123
Políticas de administración ... 123

Uso de políticas en su organización ... 124
Habilitar y deshabilitar tipos de política ... 125
Habilitar un tipo de política ... 125
Deshabilitar un tipo de política ... 126
Obtener detalles de la política ... 128
Enumeración de todas las políticas ... 128
Listado de políticas adjuntas ... 130
Listado de todos los adjuntos ... 131
Obtener información sobre una política ... 133
Administrador delegado para AWS Organizations ... 135
Creación o actualización de una política de delegación basada en recursos ... 135
Ver una política de delegación basada en recursos ... 140
Eliminar una política de delegación basada en recursos ... 141
Ejemplo de políticas de delegación ... 142
Políticas de administración ... 146
Descripción de la herencia de políticas ... 146
Políticas de exclusión de servicios de IA ... 164
Políticas de copia de seguridad ... 187
Políticas de etiquetas ... 241
Políticas de control de servicios ... 302
Comprobación de los efectos de las políticas SCP ... 303
Tamaño máximo de las políticas SCP ... 304
Adjuntar las SCP a diferentes niveles de la organización ... 304
Efectos de las SCP en los permisos ... 304
Uso de datos de acceso para mejorar las políticas SCP ... 305
Tareas y entidades no restringidas por SCP ... 306
Creación, actualización y eliminación ... 307
Adjuntar y desconectar ... 319
Evaluación de SCP ... 324
Sintaxis de SCP ... 331
Ejemplos de SCP ... 343
Administración de unidades organizativas ... 369
Navegar por el árbol ... 369
Crear una unidad organizativa ... 371
Cambiar el nombre de una unidad organizativa ... 373
Etiquetado de una unidad organizativa ... 375

Mover cuentas entre unidades organizativas ... 377
Eliminar una unidad organizativa ... 379
Etiquetado de recursos ... 381
Utilizar etiquetas ... 382
Agregar, actualizar y quitar etiquetas ... 382
Adición de etiquetas a un recurso cuando lo crea ... 382
Adición o actualización de etiquetas en un recurso existente ... 383
Uso de otros servicios de AWS ... 386
Permisos necesarios para habilitar el acceso de confianza ... 387
Permisos necesarios para deshabilitar el acceso de confianza ... 388
Cómo habilitar o deshabilitar el acceso de confianza ... 390
AWS Organizations y roles vinculados al servicio ... 392
Servicios que funcionan con Organizations ... 393
AWS Account Management ... 446
AWS Application Migration Service ... 450
AWS Artifact ... 455
AWS Audit Manager ... 459
AWS Backup ... 463
Conjuntos de pilas de AWS CloudFormation ... 465
AWS CloudTrail ... 470
AWS Compute Optimizer ... 474
AWS Config ... 479
Centro de optimización de costes de AWS ... 482
AWS Control Tower ... 485
Amazon Detective ... 487
Amazon DevOps Guru ... 491
AWS Directory Service ... 496
AWS Firewall Manager ... 498
Amazon GuardDuty ... 503
AWS Health ... 506
Amazon Inspector ... 510
AWS License Manager ... 514
Amazon Macie ... 517
AWS Marketplace ... 520
AWS Marketplace Marketplace privado ... 523
Administrador de red de AWS ... 527

AWS Resource Access Manager 530
Explorador de recursos de AWS 534
AWS Security Hub 539
Amazon S3 Storage Lens 541
Amazon Security Lake 544
AWS Service Catalog 549
Service Quotas 554
AWS IAM Identity Center 555
AWS Systems Manager 559
Políticas de etiquetas 564
AWS Trusted Advisor 566
AWS Well-Architected Tool 569
Amazon VPC IP Address Manager (IPAM) 573
Analizador de accesibilidad de Amazon VPC 577
Administrador delegado para los servicios integrados de AWS 581
Permisos concedidos a cuentas de administrador delegado 582
Seguridad 584
AWS PrivateLink 585
Limitaciones y restricciones de la forma AWS PrivateLinkAWS Organizations 585
Creación de un punto de conexión de VPC 586
Creación de una política de punto de conexión de VPC para AWS Organizations 586
IAM y Organizations 587
Autenticación 588
Control de acceso 589
Administración de permisos en su organización de AWS 590
Uso de políticas basadas en identidad (políticas de IAM) para AWS Organizations 599
Control de acceso basado en atributos con etiquetas 603
Registro y monitoreo 609
Registro de llamadas a la API de AWS Organizations con AWS CloudTrail 609
Amazon EventBridge 619
Validación de conformidad 620
Resiliencia 621
Seguridad de infraestructuras 622
AWS OrganizationsReferencia de 623
Cuotas para AWS Organizations 623
Directrices de nomenclatura 623

Valores mínimos y máximos 623
Límites de limitación 628
Políticas administradas 630
política de IAM AWS administradas 631
Políticas de control de servicios administradas por AWS 636
Solución de problemas de AWS Organizations 637
Solución de problemas generales 637
Aparece un mensaje de "acceso denegado" al realizar una solicitud a AWS Organizations . 638
Aparece un mensaje de "acceso denegado" al realizar una solicitud con credenciales de seguridad temporales 638
Obtengo un mensaje de "acceso denegado" cuando intento dejar una organización como cuenta miembro o eliminar una cuenta miembro como cuenta de administración. 639
Obtengo un mensaje de "cuota superada" cuando intento agregar una cuenta a mi organización 639
Aparece un mensaje que indica que "esta operación requiere un periodo de espera" al añadir o eliminar cuentas 640
Obtengo un mensaje de "organización todavía inicializando" cuando intento añadir una cuenta a mi organización 640
Aparece el mensaje "Invitations are disabled" cuando intento invitar a una cuenta a mi organización. 640
Los cambios que realizo no están siempre visibles inmediatamente 640
Solución de problemas de políticas de 641
Políticas de control de servicios 641
Realizar solicitudes de consulta HTTP 645
puntos de conexión 646
HTTPS obligatorio 646
Firma de solicitudes API de AWS Organizations 646
Historial de documentos 647
Glosario de AWS 660
..... dclxi

¿Qué es AWS Organizations?

AWS Organizations es un servicio de gestión de cuentas que le permite consolidar varias Cuentas de AWS en una organización que cree y administre de forma centralizada. AWS Organizations incluye todas las prestaciones de facturación unificada y posibilidades de administración de cuentas para que pueda satisfacer mejor las necesidades presupuestarias, de seguridad y de conformidad de su negocio. 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
- Precios de AWS Organizations
- Acceso a AWS Organizations
- Soporte y comentarios de AWS Organizations

Características de AWS Organizations

AWS Organizations ofrece las siguientes características:

Administración centralizada de todas sus 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 su organización para consolidar y pagar los gastos de todas las cuentas miembro. En la facturación unificada, las cuentas de administración también pueden acceder a la información de facturación, la información de la cuenta y la actividad de las cuentas miembro de su organización. Esta información se puede utilizar para servicios como Cost Explorer, lo 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 de los servicios de y las acciones de la API de AWS 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 el número máximo de permisos de las cuentas de los miembros 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 de miembro conceda dichos permisos de forma explícita en una política del IAM.

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

Políticas para estandarizar 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.

Políticas para controlar cómo la inteligencia artificial (IA) AWS y los servicios de Machine Learning 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 los servicios de IA AWS que no quiera utilizar.

Para obtener más información, consulte Políticas de exclusión de servicios de IA.

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

Puede usar políticas de copia de seguridad para configurar y aplicar automáticamente los planes AWS Backup de recursos de todas las cuentas de su organización.

Para obtener más información, consulte Políticas de copia de seguridad.

Integración y compatibilidad con AWS Identity and Access Management (IAM)

IAM permite un control pormenorizado de los usuarios y las funciones en las cuentas individuales. AWS Organizations amplía ese control al nivel de cuenta para permitirle controlar lo que los usuarios y las funciones de una cuenta o grupo de cuentas pueden hacer. Los permisos resultantes son la intersección lógica de lo que permite AWS Organizations en el nivel de cuenta y los permisos que IAM concede explícitamente en el nivel de usuario o de rol dentro de esa cuenta. En otras palabras, el usuario solo puede tener acceso a lo que permiten tanto las políticas de AWS Organizations como las políticas del IAM. Si alguna bloquea una operación, el usuario no puede tener acceso a esa operación.

Integración con otros servicios de AWS

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 AWS servicios que puede utilizar con AWS Organizations.

Cuando habilita un servicio de AWS para realizar tareas en su nombre en las cuentas de los miembros de su organización, AWS Organizations crea un rol vinculado al servicio de IAM para ese servicio en cada cuenta miembro. El rol vinculado al servicio tiene permisos de IAM predefinidos que permiten al otro servicio de AWS realizar tareas específicas en la organización y en las cuentas de esta. Para que esto funcione, todas las cuentas de una organización disponen automáticamente de un rol vinculado a servicios. Este rol permite que el servicio de AWS Organizations cree los roles vinculados a servicios que requieren los servicios de AWS en los que ha habilitado el acceso de confianza. Estos roles vinculados a servicios adicionales están adjuntos a políticas de permiso de IAM que permiten que el servicio especificado lleve a cabo solamente las tareas necesarias según sus opciones de configuración. Para obtener más información, consulte Uso de AWS Organizations con otros servicios de AWS. .

Acceso global

AWS Organizations es un servicio global con un único punto de enlace que funciona desde cualquier Regiones de AWS. No es necesario seleccionar de forma explícita 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 .

Uso gratuito

AWS Organizations es una característica de su Cuenta de AWS que se ofrece sin cargo adicional. Solo se le cobrará cuando acceda a otros servicios AWS de las cuentas de su organización. Para obtener información acerca de los precios de otros productos AWS, consulte la Página 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 las funciones de las cuentas miembro. Para obtener información acerca de los precios de otros servicios de AWS, consulte los Precios AWS.

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.

Herramientas de línea de comandos de AWS

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 de la instalación y el uso de la AWS CLI, consulte la Guía del usuario de AWS Command Line Interface.
- AWS Tools for Windows PowerShell. Para obtener información acerca de la instalación y el uso de Tools for Windows PowerShell, consulte la Guía del usuario de AWS Tools for Windows PowerShell.

SDK de AWS

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.

API de consulta HTTPS de AWS Organizations

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, consulte Llamar a la API mediante solicitudes de consulta HTTP y la Referencia de API AWS Organizations.

Soporte y comentarios de AWS Organizations

Agradecemos sus comentarios. Puede enviar sus comentarios a feedback-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

- Capacitación y cursos de AWS: enlaces a cursos especializados y basados en roles, así como a laboratorios autoguiados para ayudarlo a desarrollar sus conocimientos sobre AWS y obtener experiencia práctica.
- Herramientas para desarrolladores de AWS - Enlaces a herramientas y recursos para desarrolladores que incluyen documentación, ejemplos de código, notas de la versión y otra información para ayudarle a crear aplicaciones innovadoras con AWS.
- Centro AWS Support - El centro para crear y administrar sus casos de Support AWS. También incluye enlaces a otros recursos útiles como foros, preguntas técnicas frecuentes, estado de los servicios y AWS Trusted Advisor.
- Support AWS - La página web principal para obtener información acerca de Support AWS, un canal de soporte individualizado y de respuesta rápida que le ayudará a crear y ejecutar aplicaciones en la nube.
- Contacte con nosotros – Un punto central de contacto para las consultas relacionadas con la facturación AWS, cuentas, eventos, abuso y demás problemas.
- Términos del sitio de AWS: 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]

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.

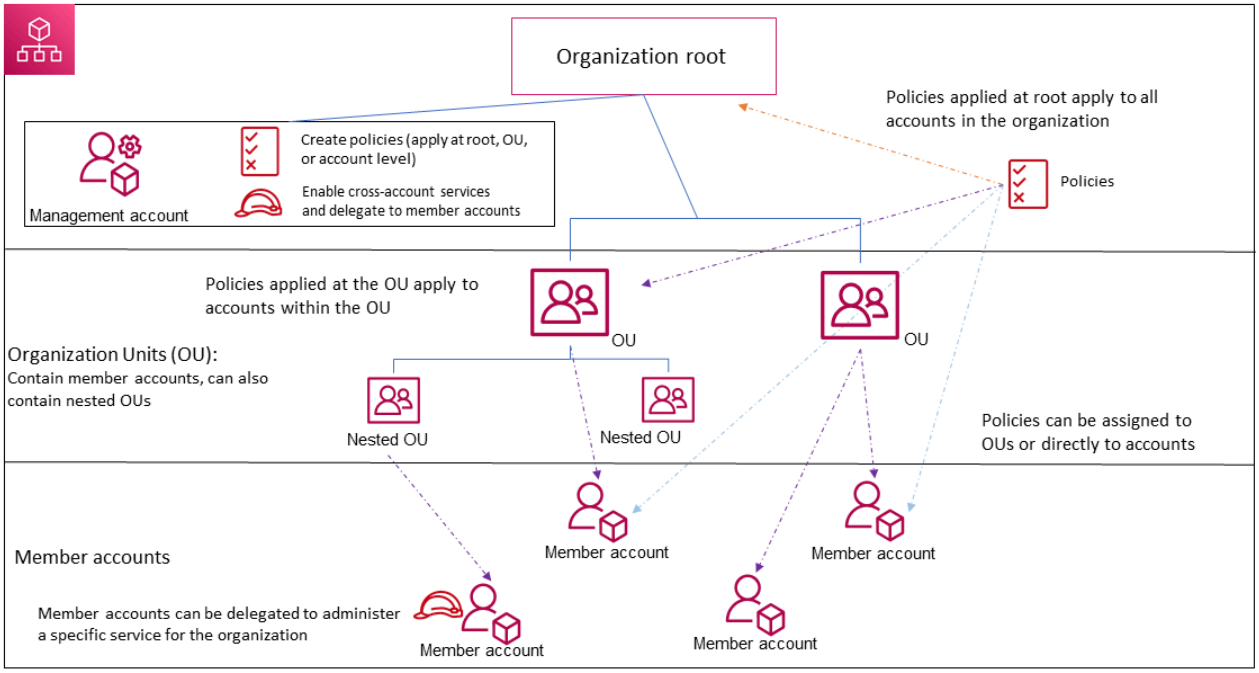
[Facturación unificada para organizaciones]

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. Este contenido está en la Guía del usuario de AWS Billing.

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 nodo 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.



Organización

Una entidad que crea para consolidar sus cuentas AWS para que pueda administrarlas 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 en la parte superior y unidades organizativas 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 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 y cuentas 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 (OU)

Un contenedor para las cuentas de un nodo raíz. 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 Cuenta de AWS estándar que contiene sus recursos AWS y las identidades que pueden acceder a esos recursos.

> **Tip**
>
> Una cuenta de AWS no es lo mismo que una cuenta de usuario. Un usuario deAWS es una identidad que se crea usando AWS Identity and Access Management (IAM) y toma la forma de Usuario de IAM con credenciales a largo plazo, o un rol de IAM con credenciales a corto plazo. Una sola cuenta AWS puede, 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.

- La cuenta de administración es 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
  - Designar cuentas de administrador delegado
  - Administrar invitaciones
  - Aplicar políticas a entidades (nodos raíz, unidades organizativas o cuentas) dentro de la organización
  - Habilite la integración con los servicios AWS admitidos para proporcionar funcionalidad de servicio en todas las cuentas de la organización.

La cuenta de administración tiene las responsabilidades de una cuenta de pago y es responsable de todos los cargos devengados por las cuentas miembro. No puede cambiar la cuenta de administración de una organización.

- Las cuentas de miembros componen el 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.

> **Note**
>
> Puede designar algunas cuentas de miembros para que sean cuentas de administrador delegado. Consulte Delegated administrator a continuación.

Administrador delegado

Le recomendamos que utilice la cuenta de administración de Organizations y sus usuarios y roles solo para las tareas que deba realizar dicha cuenta. Almacene todos sus recursos de AWS en otras cuentas de miembros de la organización y manténgalos fuera de la cuenta de administración. Esto se debe a que las características de seguridad, como las políticas de control de servicios (SCP) de las organizaciones, no restringen ningún usuario usuarios ni rol de la cuenta de administración. Separar los recursos de su cuenta de administración también lo ayudará a comprender los cargos de sus facturas. Desde la cuenta de administración de la organización, puede designar una o más cuentas de miembros como cuentas de administrador delegado para ayudarlo a implementar esta recomendación. Hay dos tipos de administradores delegados:

- Administrador delegado de Organizations: desde estas cuentas, puede administrar las políticas de la organización y adjuntar políticas a las entidades (raíces, unidades organizativas o cuentas) de la organización. La cuenta de administración puede controlar los permisos de delegación en niveles detallados. Para obtener más información, consulte Administrador delegado para AWS Organizations.
- Administrador delegado de un servicio de AWS: desde estas cuentas, puede administrar los servicios de AWS que se integran con las organizaciones. La cuenta de administración puede registrar diferentes cuentas de miembros como administradores delegados para diferentes servicios, según sea necesario. Estas cuentas tienen permisos administrativos para un servicio específico, así como permisos para las acciones de solo lectura de las organizaciones. Para obtener más información, consulte Administrador delegado para los servicios de AWS que funcionan con Organizations.

Invitación

El proceso de pedir a otra cuenta que se una a su organización. 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 a admitir todas las características de la organización. Las invitaciones funcionan mediante el intercambio de protocolos de enlace (handshakes) 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. 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 a admitir todas las características 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 para AWS 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 pueden hacer las cuentas miembro. La cuenta de administración puede aplicar SCP para restringir los servicios y las acciones a los que los usuarios (incluido el usuario raíz) y los roles de una cuenta pueden acceder. Con la cuenta de administración también se puede evitar que las cuentas de miembros dejen la organización. También puede habilitar la integración con los servicios de AWS admitidos para que proporcionen funcionalidad de servicio 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, pero no incluye las características más avanzadas de AWS Organizations. Por ejemplo, no puede habilitar otros servicios de AWS para que se integren con su organización a fin de trabajar en todas sus cuentas, ni usar políticas para restringir lo que los usuarios y roles de diferentes cuentas pueden hacer. Para utilizar las características avanzadas de AWS Organizations, debe habilitar todas las características 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. 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 para filtrar los permisos que están disponibles para las cuentas.

- Estrategia de lista de permisos: especifique de forma explícita el acceso que está permitido. 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, cuando cree su organización, nada estará bloqueado 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 lista de denegaciones: especifique de forma explícita el acceso que no está permitido. 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)

Tipo de política que le ayuda a estandarizar la configuración de inhabilitación para Servicios de IA AWS de todas las cuentas de su organización. Ciertos servicios de IA AWS 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 cliente AWS, puede usar las políticas de exclusión de servicio de IA para optar por no tener su contenido almacenado o utilizado para mejorar el servicio.

Política de copia de seguridad

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 una Política de copia de seguridad, 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 en todos los recursos de las cuentas de su organización. En una política de etiquetas, 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

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).

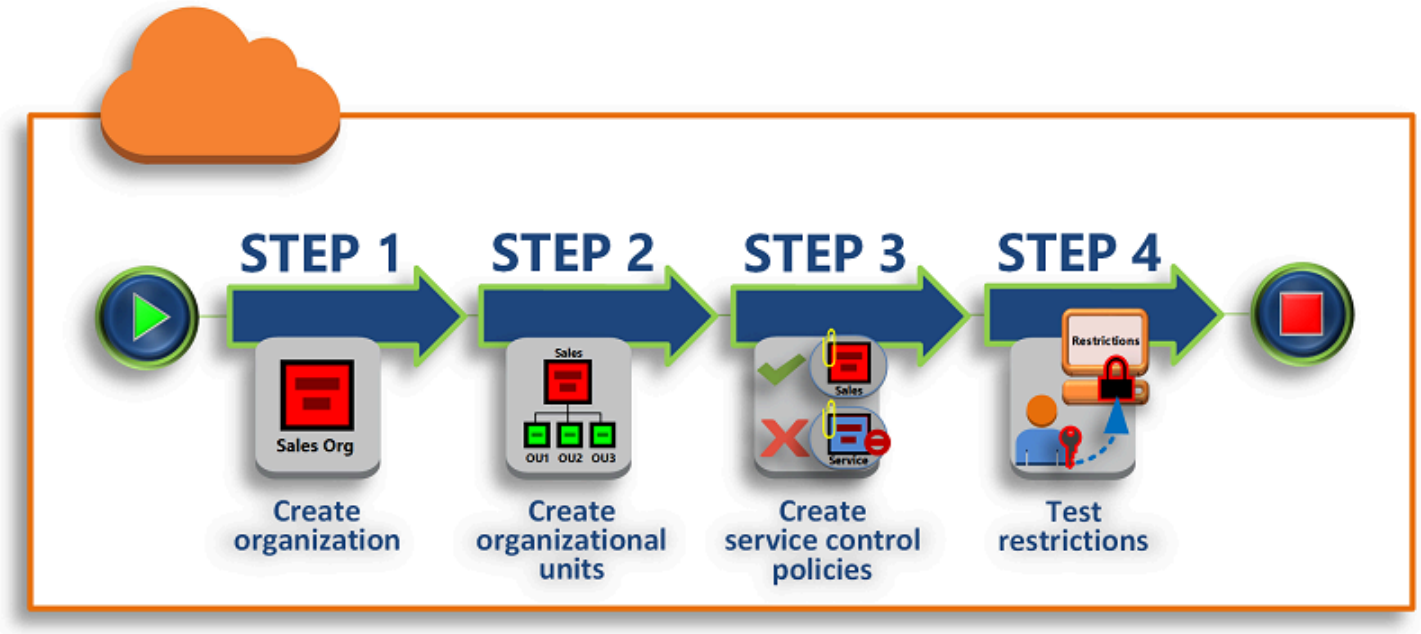
Tutorial: supervisión de cambios importantes en la organización mediante Amazon EventBridge

Para monitorear los cambios clave de su organización, puede configurar Amazon EventBridge 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, usará la técnica de lista de permitidos 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. El tutorial también muestra cómo utilizar listas de denegación para asegurarse de que ningún usuario de una cuenta miembro pueda cambiar la configuración de los registros de auditoría creados por AWS CloudTrail.

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



Paso 1: Crear la organización

En este paso, crea una organización con su Cuenta de AWS actual como cuenta de administración. También invita a una Cuenta de AWS a que se una a su organización y crea una segunda cuenta como cuenta miembro.

Paso 2: Crear las unidades organizativas

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

Las políticas de control de servicios (SCP) 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 la organización

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.

Requisitos previos

En este tutorial se supone que tiene acceso a dos Cuentas de AWS existentes (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 222222222222, a unirse como cuenta miembro.

AWS Management Console

1. Inicie sesión en AWS como administrador de la cuenta 111111111111 y abra la consola de AWS Organizations.
2. En la página de introducción, elija Crear organización.
3. En el cuadro de diálogo de confirmación, elija Crear 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 habilitadas.

AWS crea la organización y le muestra la página Cuentas de AWS. Si está en una página diferente, elija Cuentas de AWS en el panel de navegación de la izquierda.

Si la cuenta que utiliza nunca ha tenido su dirección de correo electrónico verificada por AWS, se 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.

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 página Cuentas de AWS y elija Agregar un Cuenta de AWS.
2. En la página Agregar una Cuenta de AWS, seleccione Invitar a una Cuenta de AWS existente.
3. En el cuadro ID de cuenta o correo electrónico de un Cuenta de AWS para invitar, ingrese la dirección de correo electrónico del propietario de la cuenta a la que desea invitar, similar a lo siguiente: **`member222@example.com`**. Alternativamente, si conoce el número de ID Cuenta de AWS, entonces puede ingresarlo en su lugar.
4. Escriba el texto que desee en el cuadro de texto Mensaje a 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. Seleccione Enviar invitación y AWS Organizations enviará la invitación al propietario de la cuenta.

> **Important**
>
> Expanda el mensaje de error si se indica. Si el error 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 mensaje de correo electrónico enviado desde la cuenta de administración de AWS y elija el enlace para aceptar la invitación. Cuando se le pida que inicie sesión, hágalo como administrador de la cuenta miembro invitada.
   - Abra la consola de AWS Organizations y navegue hasta la página de Invitaciones.

7. En la página Cuentas de AWS , elija Aceptar y, a continuación, elija Confirmar.

> **Tip**
>
> La recepción de la invitación podría retrasarse y es posible que tenga que esperar antes de poder aceptarla.

8. Cierre 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 una Cuenta de AWS que se convierte automáticamente en miembro de la organización. En este tutorial, a esta cuenta la llamaremos 333333333333.

AWS Management Console

Para crear una cuenta miembro

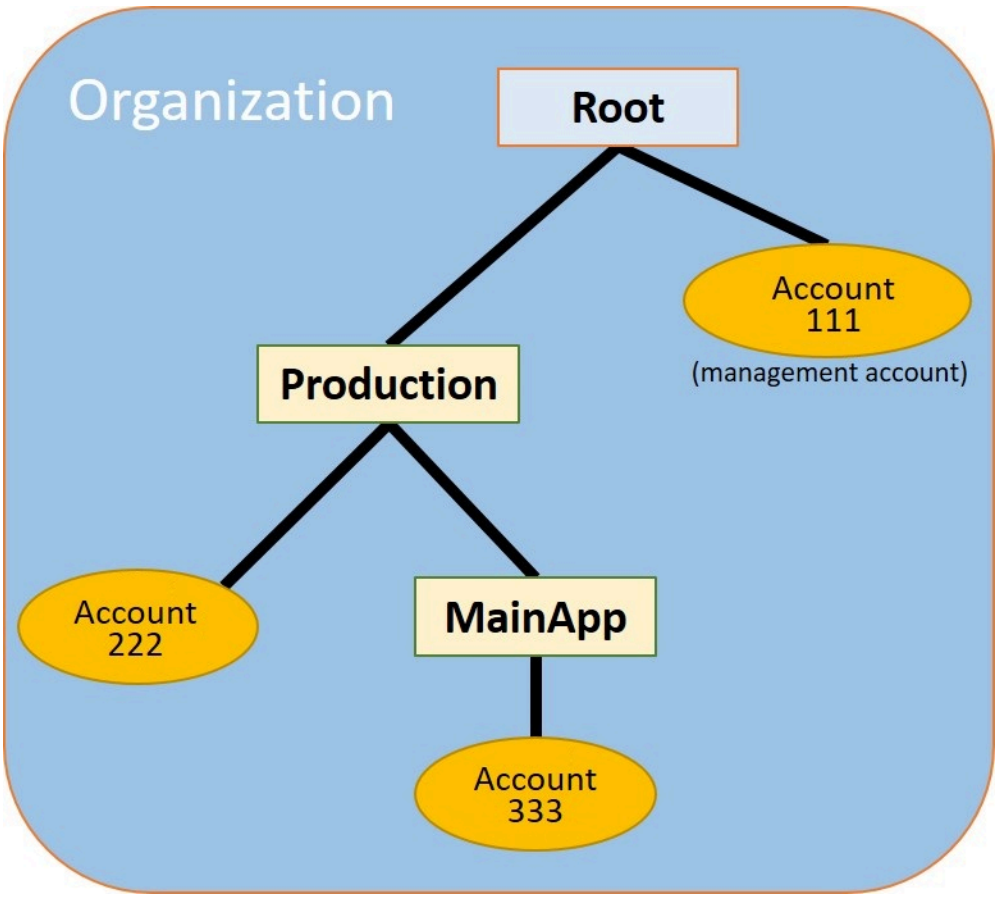
1. En la consola AWS Organizations, en la página Cuentas de AWS, elija AgregarCuenta de AWS.
2. En la páginaAgregar unCuenta de AWS, elija Crear un Cuenta de AWS.

3. En Nombre Cuenta de AWS, ingrese un nombre para la cuenta, como **`MainApp Account`**.
4. En Dirección de correo electrónico del usuario del nodo raíz de la cuenta, ingrese 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. Este rol 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 Crear Cuenta de AWS. Es posible que tenga que esperar un rato y actualizar la página para ver la nueva cuenta en la página Cuentas de AWS.

> **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 haya finalizado, 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 consola de AWS Organizations, vaya a la página Cuentas de AWS.
2. Active la casilla de verificación
   ☑
   junto al contenedor de Nodo raíz.
3. En la página Secundarias, elija Acciones y, a continuación, en Unidad organizativa, elija Crear nuevo.
4. En la página Crear unidad organizativa en Nodo raíz, para el Nombre de la unidad organizativa, ingrese **`Production`** y luego Crear unidad organizativa.
5. Active la casilla de verificación
   ☑
   junto a su nueva OU de Producción.
6. Seleccionar Acciones y, a continuación, en Unidad organizativa, elija Crear nuevo.
7. En la página Crear unidad organizativa en Producción, para el nombre de la segunda OU, ingrese **`MainApp`** y luego elija Crear unidad organizativa.

   Ahora puede mover sus cuentas miembro a estas unidades organizativas.
8. Vuelva a la página Cuentas de AWS y, a continuación, expanda el árbol bajo la unidad organizativa Production (Producción) eligiendo el triángulo
   ▶
   situado junto a ella. Esto muestra el dispositivo MainApp OU como secundario de Producción.
9. Junto a 333333333333, elija la casilla de verificación☑
   (no su nombre), elija Acciones y, a continuación, en Cuenta de AWS, elija Mover.
10. En la página Mover Cuenta de AWS “333333333333”, seleccione el triángulo situado junto a Producción para expandirlo. Junto a MainApp elija el botón de opción◉
    (no su nombre) y luego elija Mover Cuenta de AWS.
11. Junto a 222222222222, elija la casilla de verificación☑
    (no su nombre), elija Acciones y, a continuación, en Cuenta de AWS, elija Mover.
12. En la página Mover Cuenta de AWS “222222222222”, junto a Producción, seleccione el botón de opción (no su nombre) y, a continuación, seleccione Mover 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) 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 CloudTrail SCP, debe crear cualquier registro desde dicha cuenta de administración.

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

Antes de asociar una política de cualquier tipo a un nodo raíz o unidad organizativa dentro de un nodo raíz, debe habilitar el tipo de política para esa organización. Los tipos de políticas no están habilitados predeterminado. 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 SCP para su organización.

1. Vaya a la página de Políticas y, a continuación, elija Políticas de control de servicios.
2. En la página Políticas de control de servicios, elija Habilitar políticas de control de servicios.

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

Cree sus SCP

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

AWS Management Console

Para crear la primera SCP que bloquea acciones de configuración de CloudTrail

1. Vaya a la página de Políticas y, a continuación, elija Políticas de control de servicios.
2. En la página Políticas de control de servicios, seleccione Crear política.
3. Para Policy name (Nombre de política), introduzca **`Block CloudTrail Configuration Actions`**.

4. En la sección de Política, en la lista de servicios de la derecha, seleccione CloudTrail para el servicio. A continuación, elija las acciones siguientes: AddTags, CreateTrail, DeleteTrail, RemoveTags, StartLogging, StopLogging y UpdateTrail.
5. En el panel de la derecha, elija Agregar recurso y especifique CloudTrail y Todos los recursos. A continuación, elija Add resource (Añadir recurso).

   La declaración de la política ubicada a la izquierda tendrá un aspecto similar a la 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 Crear política.

La segunda política define una lista de permitidos 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. En la página Políticas de control de servicios, seleccione Crear 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 Crear política.

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

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. En la página Políticas de control de servicios, seleccione Crear política.

2. Para Policy name (Nombre de política), introduzca **`Deny List for MainApp Prohibited Services`**.
3. En la sección Policy (Política) de la izquierda, seleccione el servicio Amazon DynamoDB. Para la acción, elija All actions (Todas las acciones).
4. En el panel de la izquierda, elija Add resource (Agregar recurso) y especifique DynamoDB y All Resources (Todos 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 Root (Raíz) (su nombre, no el botón de opción) para desplazarse a su página de detalles.
3. En la página de detalles de Nodo raíz, elija la pestaña Políticas y, a continuación, en Políticas de control de servicios, elija Adjuntar.
4. En la página Adjuntar una política de control de servicios, elija el botón de opción situado al lado del SCP denominado `Block CloudTrail Configuration Actions`, y luego

elija Adjuntar. En este tutorial, la adjunta al nodo raíz para que afecte a todas las cuentas miembro para impedir que alguien modifique la forma en que ha configurado CloudTrail.

La página de detalles del Nodo raíz, la pestana Políticas muestra ahora que hay dos SCP asociadas al nodo raíz: la que acaba de asociar y la predeterminada `FullAWSAccess` SCP.

5. Vuelva a la página Cuentas de AWS y elija la unidad organizativa Production (Producción) (su nombre, no el botón de opción) para desplazarse a su página de detalles.
6. En la página de detalles de la OU de Producción, elija la pestaña Políticas.
7. Bajo Políticas de control de servicios, elija Adjuntar.
8. En la página Adjuntar una política de control de servicios, elija el botón de opción situado al lado de `Allow List for All Approved Services`, y luego elija Adjuntar. Esto le permite a los usuarios o roles de las cuentas miembro en la unidad organizativa de Producción tener acceso a los servicios aprobados.
9. Elija la pestaña Políticas nuevamente para ver que hay dos SCP asociadas a la OU: la que acaba de asociar y la SCP `FullAWSAccess` predeterminada. Sin embargo, como la política SCP `FullAWSAccess` también permite todos los servicios y acciones, ahora debe desconectar esta política SCP para asegurarse de que solo se permitan los servicios aprobados.
10. Para eliminar la política predeterminada de la OU de Producción, elija el botón de opción a FullAWSAccess, elija Desconectar y luego en el cuadro de diálogo de confirmación, elija Desconectar política.

    Después de eliminar esta política predeterminada, todas las cuentas miembro bajo la OU de Producción pierden 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 el paso anterior. 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, desplácese hasta la página Cuentas de AWS, elija el icono del triángulo para expandir la rama de la OU Production (Producción) y, a continuación, elija la unidad

organizativa MainApp (MainApp) (su nombre, no el botón de opción) para desplazarse hasta su contenido.

12. En la página de detalles MainApp, elija la pestaña Políticas.
13. Bajo Políticas de control de servicios, elija Adjuntar y, a continuación, en la lista de políticas disponibles, elija el botón de opción situado junto a Lista de denegación de servicios prohibidos por MainApp, y luego haga clic en Adjuntar política.

Paso 4: Probar las políticas de la organización

Ahora puede iniciar sesión como usuario en cualquiera de las cuentas miembro e intentar realizar diversas acciones de AWS:

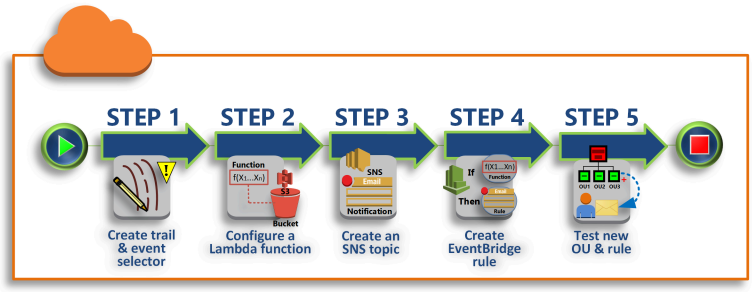
- Si inicia sesión como un usuario de la cuenta de administración, puede realizar cualquier operación permitida por las políticas de permisos de IAM. Las SCP no afectan a ningún usuario o rol de la cuenta de administración, independientemente de en qué nodo raíz o unidad organizativa se encuentre la cuenta.
- Si inicia sesión como usuario en la cuenta 222222222222, puede realizar cualquier acción que esté permitida en la lista de lo permitido. AWS Organizations deniega todo intento de realizar una acción en cualquier servicio que no aparezca en la lista de lo permitido. Asimismo, AWS Organizations deniega cualquier intento de realizar alguna de las acciones de configuración de CloudTrail.
- Si inicia sesión como un usuario en la cuenta 333333333333, puede realizar cualquier acción permitida por la lista de permitidos y que no esté bloqueada por la lista de denegación. AWS Organizations deniega cualquier intento de realizar una acción en cualquier servicio que no esté en la política de la lista de permitidos y cualquier acción que esté en la de la lista de denegación. Asimismo, AWS Organizations deniega cualquier intento de realizar alguna de las acciones de configuración de CloudTrail.

Tutorial: supervisión de cambios importantes en la organización mediante Amazon EventBridge

En este tutorial se muestra cómo configurar Amazon EventBridge, antes Eventos de Amazon CloudWatch, para supervisar los cambios en la organización. Para comenzar, se configura una regla que se activa cuando los usuarios invocan determinadas operaciones de AWS Organizations. A continuación, se configura Amazon EventBridge para que ejecute una función AWS Lambda cuando

se active la regla y se configura Amazon SNS para que envíe un correo electrónico con información detallada acerca del evento.

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



[Paso 1: Configuración de un registro de seguimiento y un selector de eventos]

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

[Paso 2: Configuración de la función Lambda]

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

[Paso 3: Creación de un tema de Amazon SNS que envía correos electrónicos a los suscriptores]

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

[Paso 4: Creación de una regla de Amazon EventBridge]

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

[Paso 5: Comprobación de la regla de Amazon EventBridge]

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.

> **Sugerencia**
>
> 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 acerca del uso de AWS CloudTrail y Amazon EventBridge con AWS Organizations, consulte Registro y monitoreo en AWS Organizations.

Requisitos previos

Este tutorial se basa en los siguientes supuestos:

- Puede iniciar sesión en la AWS Management Console como usuario de IAM desde 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 Amazon EventBridge. Para obtener más información sobre la concesión de permisos, consulte Access Management (Administración de accesos) en la guía del usuario IAM o en 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 este momento, AWS Organizations se aloja únicamente en la región 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 registro de seguimiento y un selector de eventos

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

Para crear un registro de seguimiento

1. Inicie sesión en AWS como administrador de la cuenta maestra de la organización y, a continuación, abra la consola de CloudTrail en https://console.aws.amazon.com/cloudtrail/.
2. En la barra de navegación de la esquina superior derecha de la consola, elija la región EE. UU. Este (Norte de Virginia). Si elige otra región, AWS Organizations no aparecerá entre las opciones de la configuración de Amazon EventBridge, en cuyo caso CloudTrail no capturará la información de AWS 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 deben entregarse los registros de CloudTrail.
   - Si necesita crear un bucket, seleccione Create new S3 bucket (Crear nuevo bucket de S3) y, a continuación, introduzca un nombre para el nuevo bucket y la carpeta de registro de seguimiento.

     > **Note**
     >
     > Los nombres de los buckets de S3 deben ser únicos de forma global.

   - Si ya dispone de un bucket, seleccione Use existing S3 bucket (Usar bucket S3 existente) y, a continuación, elija el nombre del bucket en la lista de buckets S3.
7. Elija Siguiente.
8. En la página Elegir eventos de registro, en la sección Eventos de administración, elija Read (Lectura) y Write (Escritura).
9. Elija Siguiente.
10. Revise las selecciones y elija Create trail (Crear ruta).

Amazon EventBridge 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 la 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 la función Lambda

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

Para crear una función de Lambda que registra eventos de Amazon EventBridge

1. Abra la consola de AWS Lambda en https://console.aws.amazon.com/lambda/.
2. Si es nuevo en Lambda, elija Get Started Now (Comenzar ahora) en la página de bienvenida; de lo contrario, elija Create a function (Crear una función).
3. En la página Create function (Crear función), seleccione Use a blueprint (Utilizar un proyecto).
4. En el cuadro de búsqueda Blueprints (Proyectos), escriba **`hello`** para el filtro y elija el proyecto hello-world.
5. Elija Configurar.
6. En la página Basic information (Información básica), haga lo siguiente:

   a. Para el nombre de la función Lambda, ingrese **`LogOrganizationEvents`** en el cuadro desde el cuadro de texto Name (Nombre).

   b. Para Role (Rol), elija Create a new role with basic Lambda permissions (Crear un nuevo rol con permisos básicos de Lambda) Este rol concede a la función Lambda permisos para obtener acceso a los datos que requiere y para escribir en su registro de salida.
7. Edite el código de la función de Lambda tal y como se muestra en el siguiente ejemplo.

   ```
   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. Elija Crear función.

Paso 3: Creación de 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 Amazon EventBridge 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 en https://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 Crear nuevo tema.
4. Ahora puede crear una suscripción para el tema. Elija el ARN del tema que acaba de crear.
5. Elija Crear una 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: Creación de una regla de Amazon EventBridge

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

Para crear una regla de EventBridge

1. Abra la consola de Amazon EventBridge en https://console.aws.amazon.com/events/.

2. Debe configurar la consola en la región de Este de EE. UU. (Norte de Virginia) o la información acerca de Organizations no estará disponible. En la barra de navegación de la esquina superior derecha de la consola, elija la región EE. UU. Este (Norte de Virginia).
3. Para obtener más información acerca de la creación de reglas, consulte Introducción a Amazon EventBridge en la Guía del usuario de Amazon EventBridge.

Paso 5: Comprobación de la regla de Amazon EventBridge

En este paso, se crea una unidad organizativa (OU) y se comprueba que la regla de Amazon EventBridge genere una entrada de registro y le envíe un correo electrónico con información detallada del evento.

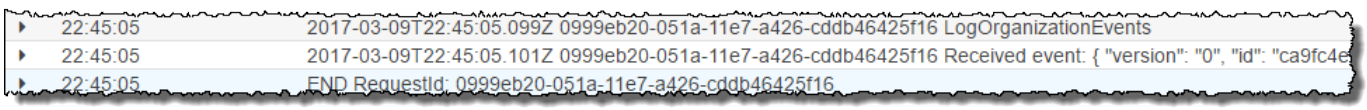
AWS Management Console

Para crear una unidad organizativa (OU)

1. Abra la página Cuentas de AWSen la consola de AWS Organizations.
2. Seleccionar la casilla de verificación
   ☑
   OU de Nodo raíz, elija Acciones y, a continuación, en Unidad organizativa, elija Crear nuevo.
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 EventBridge

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Logs (registros).
3. En la página Log Groups (Grupos de registros), elija el grupo 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 por OrgsCWEvnt (el nombre que mostrar 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. Utilice la consola de CloudTrail para eliminar el registro de seguimiento denominado **`My-Test-Trail`** que creó en el paso 1.
2. Si ha creado un bucket de Amazon S3 en el paso 1, utilice la consola de Amazon S3 para eliminarlo.
3. Utilice la consola de Lambda para eliminar la función denominada **`LogOrganizationEvents`** que se creó en el paso 2.
4. Utilice la Consola de Amazon SNS para eliminar el tema de Amazon SNS denominado **`OrganizationsCloudWatchTopic`** que creó en el paso 3.
5. Utilice la consola de CloudWatch para eliminar la regla de EventBridge denominada **`OrgsMonitorRule`** que creó en el paso 4.
6. Finalmente, utilice la consola de Organizations para eliminar la OU denominada **`TestCWEOU`** que creó en el paso 5.

Y ya está. En este tutorial, ha configurado EventBridge; para monitorear los cambios en su 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 acerca de dicho evento.

Prácticas recomendadas para la administración de varias cuentas

Siga estas recomendaciones como ayuda para configurar y administrar un entorno de varias cuentas en AWS Organizations.

Temas

- Administrar cuentas dentro de una sola organización
- Utilizar una contraseña segura para el usuario raíz
- Documentar los procesos para el uso de las credenciales de usuario raíz
- Habilitar MFA para las credenciales de usuario raíz
- Aplicar controles para monitorear el acceso a las credenciales del usuario raíz
- Mantener actualizado el número de teléfono de contacto
- Utilizar una dirección de correo electrónico de grupo para todas las cuentas raíz
- Agrupar cargas de trabajo en función del propósito empresarial y no de la estructura de informes
- Utilizar varias cuentas para organizar cargas de trabajo
- Habilitar los servicios de AWS en el nivel de la organización mediante la consola de servicios o las operaciones de la API o de la CLI
- Utilizar las herramientas de facturación para realizar un seguimiento de los costos y optimizar el uso de los recursos
- Planificar la estrategia de etiquetado y la aplicación de las etiquetas en todos los recursos de la organización
- Prácticas recomendadas para la cuenta de administración
- Prácticas recomendadas para cuentas de miembros

Administrar cuentas dentro de una sola organización

Se recomienda crear una sola organización y administrar todas las cuentas que se encuentran en ella. Una organización es una barrera de seguridad que le permite mantener la coherencia entre las cuentas de su entorno. Puede aplicar políticas o configuraciones de nivel de servicio de forma centralizada en todas las cuentas de una organización. Si desea habilitar políticas coherentes,

visibilidad central y controles programáticos en su entorno de varias cuentas, lo mejor es hacerlo dentro de una sola organización.

Utilizar una contraseña segura para el usuario raíz

Se recomienda utilizar una contraseña segura y única. Existen varios administradores de contraseñas y algoritmos y herramientas de generación de contraseñas seguras que pueden ayudar a lograr estos objetivos. Para más información, consulte Cambiar la contraseña para Usuario raíz de la cuenta de AWS. Utilice 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. Se recomienda almacenar la contraseña en un sistema de administración de contraseñas o equivalente que cumpla con los requisitos de seguridad de su organización. Para evitar crear una dependencia circular, no almacene la contraseña del usuario raíz con herramientas que dependen de AWS en los que inicia sesión con la cuenta protegida. Sea cual sea el método que elija, se recomienda que priorice la resiliencia y que considere la posibilidad de solicitar a varios actores que autoricen el acceso a este almacén para mejorar la protección. Se debe registrar y supervisar cualquier acceso a la contraseña o a su ubicación de almacenamiento. Para obtener recomendaciones adicionales sobre contraseñas del usuario raíz, consulte Mejores prácticas del usuario raíz para su Cuenta de AWS.

Documentar los procesos para el uso de las credenciales de usuario raíz

Documente la ejecución de procesos importantes a medida que se llevan a cabo para asegurarse de que tiene un registro de las personas involucradas en cada paso. Para administrar la contraseña, se recomienda utilizar un administrador de contraseñas cifradas que sea seguro. También es importante proporcionar documentación sobre las excepciones y eventos imprevistos que se puedan presentar. Para obtener más información, consulte Solución de problemas de inicio de sesión de AWS Management Console en la Guía del usuario de inicio de sesión AWS y Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Compruebe y valide que sigue teniendo acceso al usuario raíz y que el número de teléfono de contacto funcione al menos trimestralmente. Esto ayuda a asegurar al negocio que el proceso funciona y que usted mantiene el acceso al usuario raíz. También demuestra que las personas responsables del acceso raíz comprenden los pasos que deben seguir para que el proceso se complete correctamente. Para aumentar el tiempo de respuesta y el éxito, es importante asegurarse de que todo el personal que participa en un proceso comprenda exactamente lo que debe hacer en caso de que sea necesario acceder.

Habilitar MFA para las credenciales de usuario raíz

Le recomendamos que habilite varios dispositivos de autenticación multifactor (MFA) para el usuario raíz de la Cuenta de AWS y los usuarios de IAM en sus Cuentas de AWS. Esto le permite subir el nivel de seguridad en sus Cuentas de AWS y simplificar la administración del acceso a usuarios altamente privilegiados, como el usuario raíz de la Cuenta de AWS. Para satisfacer las diferentes necesidades de los clientes, AWS admite tres tipos de dispositivos MFA para IAM, que incluyen las claves de seguridad FIDO, las aplicaciones de autenticación virtual y los tokens de hardware de contraseña temporal de un solo uso (TOTP) por tiempo.

Cada tipo de autenticador tiene propiedades físicas y de seguridad ligeramente diferentes que son las más adecuadas para diferentes casos de uso. Las claves de seguridad FIDO2 ofrecen el nivel de seguridad más alto y son resistentes a la suplantación de identidad. Cualquier forma de MFA ofrece una postura de seguridad más sólida que la autenticación solo con contraseña; le recomendamos encarecidamente que agregue algún tipo de MFA a su cuenta. Seleccione el tipo de dispositivo que mejor se adapte a sus requisitos operativos y de seguridad.

Si elige un dispositivo que funciona con batería para ser su autenticador principal, como un token de hardware de TOTP, considere también la posibilidad de registrar un autenticador que no dependa de la batería como mecanismo de respaldo. También es esencial comprobar periódicamente la funcionalidad del dispositivo y reemplazarlo antes de la fecha de caducidad para mantener un acceso ininterrumpido. Independientemente del tipo de dispositivo que elija, se recomienda registrar al menos dos dispositivos (IAM admite hasta ocho dispositivos MFA por usuario) para aumentar la resiliencia ante la pérdida o los errores del dispositivo.

Siga la política de seguridad de la información de su organización para almacenar el dispositivo MFA correctamente. Se recomienda que guarde el dispositivo MFA por separado de la contraseña asociada. Esto garantiza que el acceso a la contraseña y al dispositivo MFA requiera diferentes recursos (personas, datos y herramientas). Esta separación agrega una capa adicional de protección contra el acceso no autorizado. También se recomienda registrar y supervisar cualquier acceso al dispositivo MFA o a su ubicación de almacenamiento. Esto ayuda a detectar accesos no autorizados y responder ante ellos.

Para obtener más información, consulte Asegure el inicio de sesión de su usuario raíz con el autenticación multifactor (MFA) en en la Guía del usuario de IAM. Para obtener instrucciones sobre cómo habilitar la MFA, consulte Uso de autenticación multifactor (MFA) en AWS y Habilitación de dispositivos MFA para usuarios en AWS.

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

El acceso a las credenciales de usuario raíz debe ser un evento raro. Cree alertas con ayuda de herramientas como Amazon EventBridge para anunciar el inicio de sesión y el uso de las credenciales de usuario raíz de la cuenta de administración. Esta alerta debe incluir, entre otras cosas, la dirección de correo electrónico utilizada para el propio usuario raíz. Esta alerta debe ser significativa y difícil de pasar por alto. Para ver un ejemplo, consulte Monitorear y notificar en actividad del usuario raíz Cuenta de AWS. Compruebe que el personal que recibe dicha alerta entienda cómo validar que se espera el acceso del usuario raíz y cómo escalar si se cree que un incidente de seguridad está en curso. Para más información, consulte Informar acerca de correos electrónicos sospechosos o Informes de vulnerabilidad. Como alternativa, puede ponerse en contacto con AWS para obtener ayuda y orientación adicional.

Mantener actualizado el número de teléfono de contacto

Para recuperar el acceso a su Cuenta de AWS, es crucial tener un número de teléfono de contacto válido y activo que le permita recibir mensajes de texto o llamadas. Se recomienda que utilice un número de teléfono específico para asegurarnos de que AWS puede ponerse en contacto con usted con fines de soporte y recuperación de la cuenta. Puede ver y administrar fácilmente los números de teléfono de su cuenta a través de la AWS Management Console o de nuestras API de administración de cuentas.

Hay varias formas de obtener un número de teléfono específico que garantice que AWS pueda comunicarse con usted. Se recomienda encarecidamente que consiga una tarjeta SIM dedicada y un teléfono físico. Guarde el teléfono y la tarjeta SIM de forma segura y a largo plazo para garantizar que el número de teléfono permanezca disponible para la recuperación de la cuenta. Asegúrese también de que el equipo responsable de la factura del móvil comprenda la importancia de este número, incluso si permanece inactivo durante periodos prolongados. Es esencial mantener la confidencialidad de este número de teléfono dentro de su organización para garantizar protección adicional.

Documente el número de teléfono en la página de la consola de información de contacto de AWS y comparta su información con los equipos específicos que deben conocerla dentro de su organización. Este enfoque ayuda a minimizar el riesgo asociado con la transferencia del número de teléfono a una tarjeta SIM diferente. 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. Se debe registrar y supervisar cualquier acceso al teléfono o a su ubicación de almacenamiento. Si el número de teléfono asociado a una cuenta cambia, implemente procesos para actualizar dicho número en la documentación existente.

Utilizar una dirección de correo electrónico de grupo para todas las cuentas raíz

Utilice una dirección de correo electrónico administrada por su empresa. Utilice una dirección de correo electrónico que reenvíe los mensajes recibidos directamente a un grupo de usuarios. En el caso de que AWS necesite ponerse en contacto con el titular de la cuenta, por ejemplo, para confirmar el acceso, el mensaje de correo electrónico se distribuirá 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.

Agrupar cargas de trabajo en función del propósito empresarial y no de la estructura de informes

Se recomienda aislar los entornos de carga de trabajo de producción y los datos en sus unidades organizativas de nivel superior orientadas a las cargas de trabajo. Sus unidades organizativas deben basarse en un conjunto común de controles, en lugar de reproducir la estructura de informes de la empresa. Además de las unidades organizativas de producción, se recomienda que defina una o más unidades organizativas que no sean de producción y que contengan cuentas y entornos de carga de trabajo que se utilicen para desarrollar y comprobar las cargas de trabajo. Para más información, consulte Organizing workload-oriented OUs.

Utilizar varias cuentas para organizar cargas de trabajo

Una Cuenta de AWS ofrece seguridad natural, acceso y límites de facturación para sus recursos de AWS. El uso de varias cuentas tiene sus ventajas, ya que permite distribuir las cuotas de nivel de cuenta y los límites de tasa de solicitudes de API, además de las ventajas adicionales que se enumeran a continuación. Se recomienda utilizar varias cuentas básicas de toda la organización, como cuentas de seguridad, registro e infraestructura. En el caso de las cuentas de carga de trabajo, debe separar las cargas de trabajo de producción de las cargas de trabajo de comprobación o desarrollo en cuentas independientes.

Habilitar los servicios de AWS en el nivel de la organización mediante la consola de servicios o las operaciones de la API o de la CLI

Como práctica recomendada, se sugiere habilitar o deshabilitar cualquier servicio con el que quiera integrarse en AWS Organizations con la consola de ese servicio, las operaciones de la API o los equivalentes de comandos de la CLI. Con este método, el servicio de AWS puede llevar a cabo todos los pasos de inicialización necesarios para su organización, como crear los recursos necesarios y eliminar recursos al deshabilitar el servicio. AWS Account Management es el único servicio que requiere el uso de la consola de AWS Organizations o las API para habilitarlo. Para revisar la lista de servicios con los que se integra AWS Organizations, consulte AWS servicios que puede utilizar con AWS Organizations.

Utilizar las herramientas de facturación para realizar un seguimiento de los costos y optimizar el uso de los recursos

Al administrar una organización, recibe una factura consolidada que cubre todos los cargos de las cuentas de su organización. Para los usuarios empresariales que necesiten acceder a la visibilidad de los costes, puede proporcionar una función en la cuenta de administración con permisos restringidos de solo lectura para revisar las herramientas de facturación y costos. Por ejemplo, puede crear un conjunto de permisos que proporcione acceso a los informes de facturación o utilizar el AWS Cost Explorer Service (una herramienta de visualización de tendencias de los costos a lo largo del tiempo) y servicios rentables, como Lente de almacenamiento de Amazon S3 y AWS Compute Optimizer.

Planificar la estrategia de etiquetado y la aplicación de las etiquetas en todos los recursos de la organización

A medida que las cuentas y cargas de trabajo aumentan, las etiquetas pueden ser una característica útil para el seguimiento de costos, el control de acceso y la organización de los recursos. Para las estrategias de etiquetado y nomenclatura, siga las instrucciones que se indican en Tagging your AWS resources. Además de los recursos, puede crear etiquetas en la raíz de la organización, las cuentas, las unidades organizativas y las políticas. Consulte la sección Building your tagging strategy para obtener más información.

Prácticas recomendadas para la cuenta de administración

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

Temas

- Limitar quién tiene acceso a la cuenta de administración
- Revisar quién tiene acceso y realizar un seguimiento
- Utilice la cuenta de administración solo para tareas que requieren la cuenta de administración
- Evitar la implementación de cargas de trabajo en la cuenta de administración de la organización
- Delegar responsabilidades fuera de la cuenta de administración para la descentralización

Limitar quién tiene acceso a la cuenta de administración

La cuenta de administración es clave para todas las tareas administrativas mencionadas, como la administración de cuentas, las políticas, la integración con otros servicios de AWS, la facturación consolidada, etc. Por lo tanto, debe restringir y limitar el acceso a la cuenta de administración solo a los usuarios administradores que necesiten derechos para realizar cambios en la organización.

Revisar quién tiene acceso y realizar un seguimiento

Para asegurarse de mantener el acceso a la cuenta de administración, revise periódicamente el 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. Agregue 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.

Utilice la cuenta de administración solo para tareas que requieren la cuenta de administración

Se recomienda que utilice la cuenta de administración y sus usuarios y roles para tareas que solo puede realizar esa cuenta. Almacene todos sus recursos de AWS en otras Cuentas de AWS en la organización y manténgalos fuera de la cuenta de administración. Una razón importante para mantener los recursos en otras cuentas es porque las políticas de control de servicios (SCP) de Organizations no funcionan para restringir ningún usuario o rol en la cuenta de administración. Separar los recursos de la cuenta de administración también lo ayudará a comprender los cargos de sus facturas.

Evitar la implementación de cargas de trabajo en la cuenta de administración de la organización

Las operaciones privilegiadas se pueden realizar dentro de la cuenta de administración de una organización y las SCP no se aplican a dicha cuenta. Por eso, debe limitar los recursos y datos de la nube que contenga la cuenta de administración únicamente a los que deben administrarse en esta cuenta.

Delegar responsabilidades fuera de la cuenta de administración para la descentralización

Siempre que sea posible, se recomienda delegar responsabilidades y servicios fuera de la cuenta de administración. Proporcione a sus equipos permisos en sus propias cuentas para administrar las necesidades de la organización sin necesidad de acceder a la cuenta de administración. Además, puede registrar varios administradores delegados para los servicios que admiten esta funcionalidad, como es el caso de AWS Service Catalog, para compartir software en toda la organización o StackSets de AWS CloudFormation para crear e implementar pilas.

Para obtener más información, consulte Security Reference Architecture, Organizing Your AWS Environment Using Multiple Accounts y AWS servicios que puede utilizar con AWS Organizations para obtener sugerencias sobre cómo registrar las cuentas de los miembros como administradores delegados de varios servicios de AWS. Para obtener más información sobre la configuración de administradores delegados, consulte Enabling a delegated admin account for AWS Account Management and Administrador delegado para AWS Organizations.

Prácticas recomendadas para cuentas de miembros

Siga estas recomendaciones para proteger la seguridad de las cuentas de los miembros de su organización. Estas recomendaciones suponen que también se adhiere a las Prácticas recomendadas de utilizar el usuario raíz exclusivamente para aquellas tareas que realmente lo requieran.

Temas

- Definir el nombre y los atributos de la cuenta
- Ampliar el entorno y el uso de la cuenta de manera eficiente
- Utilice una SCP para restringir lo que puede hacer el usuario raíz en tus cuentas de miembro

Definir el nombre y los atributos de la cuenta

En el caso de las cuentas de los miembros, utilice una estructura de nombres y una dirección de correo electrónico que reflejen el uso de la cuenta. Por ejemplo, `Workloads+fooA+dev@domain.com` para `WorkloadsFooADev`, `Workloads+fooB+dev@domain.com` para `WorkloadsFooBDev`. Si ha definido etiquetas personalizadas para su organización, se recomienda que asigne esas etiquetas a las cuentas que reflejen el uso de la cuenta, el centro de costos, el entorno y el proyecto. Esto facilita la identificación, organización y búsqueda de las cuentas.

Ampliar el entorno y el uso de la cuenta de manera eficiente

A medida que vaya escalando, antes de crear cuentas nuevas, asegúrese de que ya no existan cuentas para necesidades similares a fin de evitar duplicaciones innecesarias. Las Cuentas de AWS deben basarse en requisitos de acceso comunes. Si tiene previsto volver a utilizar las cuentas, como una cuenta de entorno aislado o una cuenta equivalente, se recomienda que elimine las cargas de trabajo o los recursos innecesarios de las cuentas, pero que guarde las cuentas para utilizarlas en el futuro.

Antes de cerrar cuentas, tenga en cuenta que están sujetas a los límites de cuota de cierre de cuentas. Para obtener más información, consulte Cuotas para AWS Organizations. Considere la posibilidad de implementar un proceso de limpieza para reutilizar las cuentas en lugar de cerrarlas y crear otras nuevas cuando sea posible. De esta forma, evitará incurrir en costos derivados de la ejecución de los recursos y alcanzar los límites de la API CloseAccount.

Utilice una SCP para restringir lo que puede hacer el usuario raíz en tus cuentas de miembro

Se recomienda crear una política de control de servicios (SCP) en la organización y adjuntarla al nodo raíz de la organización para que se aplique a todas las cuentas miembros. Para obtener más información, consulte Proteja las credenciales de usuario raíz de su cuenta de Organizations.

Puede denegar todas las acciones raíz, excepto una acción específica exclusiva para usuarios raíz que debe realizar en su cuenta de miembro. Por ejemplo, la siguiente SCP de ejemplo impide que el usuario raíz de cualquier cuenta de miembro realice llamadas a la API de servicio de AWS, excepto "Actualizar una política de bucket de S3 que estaba mal configurada y deniega el acceso a todas las entidades principales" (una de las acciones que requieren credenciales de usuario raíz). Para obtener más información, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

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

    "Statement": [

        {

            "Effect": "Deny",

            "NotAction":[

            "s3:GetBucketPolicy",

            "s3:PutBucketPolicy",

            "s3:DeleteBucketPolicy"

                 ],

            "Resource": "*",

            "Condition": {
 "StringLike": { "aws:PrincipalArn": "arn:aws:iam::*:root" }

            }
```

```
        }

    ]
}
```

En la mayoría de las circunstancias, un rol de AWS Identity and Access Management (IAM) puede realizar cualquier tarea administrativa en la cuenta de miembro que tiene permisos de administrador pertinentes. Cualquiera de estos roles debe tener controles adecuados implementados que limiten, registren y supervisen la actividad.

Creación y administración de una organización

Puede llevar a cabo las tareas siguientes a través de la consola AWS Organizations o ejecutando un comando AWS Command Line Interface (AWS CLI) o las operaciones AWS del API de SDK equivalentes:

- Crear una organización. 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. 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). Las SCP ofrecen control centralizado de los máximos permisos disponibles para todas las cuentas de la organización. Esto le ayuda a asegurarse de que sus cuentas respeten en todo momento las directrices de control de acceso de la organización.
- Ver información detallada de su organización. Vea información detallada de su organización y sus nodos raíz, unidades organizativas y cuentas.
- Eliminar una organización. 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 administración. Cuando crea una organización, puede elegir si la organización admitirá todas las características (opción recomendada) o solo las de facturación unificada.

Una vez creada la organización, puede agregar cuentas desde la cuenta de administración tal y como se indica a continuación:

- Puede crear otras Cuentas de AWS que se incorporen automáticamente a la organización como miembros.
- Después de verificar la dirección de correo electrónico, puede invitar a otras Cuentas de AWS existentes para que se unan a su organización como cuentas miembro.

Crear una organización

Puede crear una organización utilizando la AWS Management Console o mediante un comando del AWS CLI o una de las API de SDK.

> **Permisos mínimos**
>
> Para crear una organización con su Cuenta de AWS actual, debe contar con 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

2. De forma predeterminada, la organización se crea con todas las características habilitadas. Sin embargo, puede elegir cualquiera de los siguientes pasos:

   - Para crear una organización con todas las características habilitadas, en la página de introducción, elija Creación de una organización.
   - Para crear una organización con funciones de Facturación unificada únicamente, en la página de introducción y en Creación de una organización, elija características de facturación unificada y, a continuación, en el cuadro de diálogo de confirmación, elija Crear una organización.

   Si elige accidentalmente la opción incorrecta, puede ir inmediatamente a la página Configuración y, a continuación, elija Eliminar organización y empiece de nuevo.

3. Se crea la organización y se visualizará la página Cuentas de AWS. La única cuenta presente es su cuenta de administración, y actualmente está almacenada en la Unidad organizativa raíz (OU).

   Organizations envía automáticamente un correo electrónico de verificación a la dirección asociada a su 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 . Puede crear cuentas a 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 administración Cuenta de AWS de inicio de sesión 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**
>
> El campo `AvailablePolicyTypes` está obsoleto y no contiene información precisa sobre las políticas habilitadas en su organización. Para ver la lista precisa y completa de los tipos de política que están realmente habilitados para la organización, utilice el comando `ListRoots`, tal y como se describe en la parte AWS CLI de la siguiente sección.

- SDK de AWS: CreateOrganization

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

- Para crear una Cuenta de AWS que forme parte automáticamente de su organización de AWS, consulte Creación de una cuenta miembro en su organización.
- Para invitar a una cuenta existente a la organización, consulte Invitar Cuenta de AWS a un hombre a unirse a su organización.

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, AWS envía 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 otras 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, consulte Consultar detalles de una organización desde la cuenta de administración.
- Para cambiar la dirección de correo electrónico asociada a la cuenta de administración, consulte Administración de una Cuenta de AWS en la Guía del usuario AWS Billing.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Vaya a la página de Configuración y, a continuación, elija Solicitud de verificación de envío. 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, podrá invitar a otras Cuentas de AWS para que se unan a su organización. Para obtener más información, consulte Invitar Cuenta de AWS a un hombre a unirse a su organización .

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 invitó 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 verifique 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:

- All features (Todas las características) - Esta característica es la mejor forma de trabajar con AWS Organizations e incluye las características de facturación unificada. 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 en AWS Organizations como Integración con servicios admitidos de AWS y políticas de administración de la organización.
- Consolidated billing features (Características de facturación unificada) - 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 unificada o con todas las funciones habilitadas.
  - Si invita a una cuenta durante el 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. Solo debe invitar a la cuenta para que sea miembro de una organización con características de facturación unificada.
  - Si invita a una cuenta y la invitación aún no está aceptada antes de que inicie el proceso para habilitar todas las características, esa invitación se cancela porque la invitación indica que la organización solo tiene funciones de facturación unificada. Debe invitar de nuevo a la cuenta 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 Organizations también verifica que todas las cuentas tengan un rol vinculado con el servicio denominado `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, 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 políticas 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 las cuentas miembro pueden eliminar, si lo desean, el rol vinculado al servicio denominado `AWSServiceRoleForOrganizations`. Si luego 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.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

2. En la página Configuración, elija Iniciar proceso para habilitar todas las características.
3. En la página Habilitar todas las características, confirme que entiende que no puede volver a las características de facturación unificada después de cambiar seleccionando Iniciar proceso para habilitar todas las características.

   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 la lista de Estado de las solicitudes de aprobación para las cuentas invitadas.

   > **Tip**
   >
   > Para volver a esta página más adelante, abra la página Configuración y en la sección de Solicitud enviada fecha, elija Ver estado.

4. La página Habilitar todas las características muestra el estado de la solicitud actual para cada cuenta de la organización. Las cuentas que han aceptado la solicitud muestran un estado de ACEPTADA. Las cuentas que aún no han acordado muestran un estado de ABIERTA.

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: enable-all-features

  El siguiente comando inicia el proceso para habilitar todas las características en 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.

- SDK de AWS: EnableAllFeatures

Notas

- 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.
- Cuando realice la solicitud para habilitar todas las funciones, se cancelarán todas las invitaciones a cuentas existentes que no se hayan aceptado.
- Durante el proceso de migración de todas las funciones, aún puede iniciar invitaciones nuevas a cuentas y crear cuentas nuevas.

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 ninguna cuenta miembro invitada. Para finalizar el proceso, continúe con Finalización del proceso para habilitar todas las características.

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

Cuando inicia sesión en una de las cuentas miembro invitadas de la organización, puede aprobar una solicitud desde una 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 habilita todas las funciones, 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 es necesario si el rol `AWSServiceRoleForOrganizations` debe crearse de nuevo en la cuenta miembro.

AWS Management Console

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

1. Inicie sesión en la consola de AWS Organizations en consola AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en una cuenta de 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 de 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:
  - accept-handshake
  - list-handshakes-for-account

  En el ejemplo siguiente se indica cómo enumerar los protocolo de enlace disponibles para su cuenta. 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"
            }
        ]
    }
}
```

- SDK de AWS
  - list-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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Configuración, si 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 página Habilitar todas las características, elija Finalizar y, a continuación, en el cuadro de diálogo de confirmación, elija Finalizar de 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
  - accept-handshake

```
$ 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 protocolo 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"
            }
        ]
    }
}
```

- SDK de AWS
  - AcceptHandshake
  - AcceptHandshake

Los siguientes pasos:

- Habilitar 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 en AWS Organizations.
- Habilite la integración con los servicios compatibles. Para obtener más información, consulte Uso de AWS Organizations con otros servicios de AWS..

Consultar detalles de su organización

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

Temas

- Consultar detalles de una organización desde la cuenta de administración
- Visualización de los detalles del contenedor de nodo raíz
- Consultar los detalles de una unidad organizativa
- Consultar detalles de una cuenta
- Consultar detalles de una política

Consultar detalles de una organización desde la cuenta de administración

Cuando inicia sesión en la cuenta de administración de la organización en la AWS Organizationsconsola de , 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Vaya a la página de Configuración. En esta página se muestran detalles sobre la organización, incluido el ID de la organización, el nombre de la 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 los resultados 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**
>
> El campo `AvailablePolicyTypes` está obsoleto y no contiene información precisa sobre las políticas habilitadas en su organización. Para ver la lista precisa y completa de los tipos de política que están realmente habilitados para la organización, utilice el comando `ListRoots`, tal y como se describe en la parte AWS CLI de la siguiente sección.

- SDK de AWS: DescribeOrganization

Visualización de los detalles del contenedor de nodo raíz

Cuando inicia sesión en la cuenta de administración de la organización en la consola de AWS Organizations, puede ver los detalles del contenedor del nodo raíz.

> **Permisos mínimos**
>
> Para ver los detalles de un nodo raíz, debe contar con los siguientes permisos:
>
> - `organizations:DescribeOrganization` (solo consola)
> - `organizations:ListRoots`

El nodo 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 el nodo raíz afectan a todas las demás OU y cada Cuenta de AWS en la organización.

AWS Management Console

Para ver los detalles del nodo raíz

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

2. Vaya a la página Cuentas de AWS y elija la opción Nodo raíz OU (su nombre, no el botón de opción).
3. La página de detalles del Nodo raíz aparece y muestra los detalles del nodo raíz.

AWS CLI & AWS SDKs

Para ver los detalles del nodo raíz

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

- AWS CLI: list-roots

  El siguiente ejemplo muestra cómo recuperar los detalles del nodo raíz, incluidos los tipos de política 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"
                }
            ]
        }
    ]
}
```

- SDK de AWS: ListRoots

Consultar los detalles de una unidad organizativa

Cuando inicia sesión en la cuenta de administración de la organización en la consola de AWS Organizations, puede ver los detalles de las OU en 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 los detalles de una unidad organizativa

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En 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 OU, elija el icono del triángulo situado junto a su unidad organizativa principal para expandirla y verlos en el siguiente nivel de la jerarquía. Repita la operación hasta que encuentre la OU que desea.

   El cuadro de Detalles de la unidad organizativa muestra la información sobre la OU.

AWS CLI & AWS SDKs

Para ver los detalles de una unidad organizativa

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

- AWS CLI, SDK de AWS
  - list-roots
  - list-children

- describe-organizational-unit

El siguiente ejemplo muestra cómo buscar el ID de una OU utilizando AWS CLI. Encontrará el ID de unidad organizativa atravesando la jerarquía comenzando por el comando `list-roots` y, a continuación, realizar `list-children` en el nodo raíz e iterativamente en cada uno de las secundarias hasta que encuentre la 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 OU.

```
$ 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"
    }
```

```
}
```

- SDK de AWS
  - ListRoots
  - ListChildren
  - DescribeOrganizationalUnit

Consultar detalles de una cuenta

Cuando inicia sesión en la cuenta de administración de la organización en la consola de AWS Organizations, puede ver los detalles de las cuentas.

> **Permisos mínimos**
>
> Para ver los detalles de una Cuenta de AWS, debe disponer de 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 una Cuenta de AWS

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Vaya a la página 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 secundaria de una OU, es posible que tenga que elegir el icono del triángulo junto a una unidad organizativa para expandirla y ver a sus secundarias. Repetir hasta que encuentre la cuenta.

El cuadro Detalles de la cuenta muestra la información sobre la cuenta.

AWS CLI & AWS SDKs

Para ver los detalles de una Cuenta de AWS

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

- AWS CLI:
  - list-accounts — enumera los detalles de todas las cuentas de la organización
  - describe-account — muestra los detalles de solo la cuenta especificada

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

  El siguiente ejemplo muestra cómo recuperar los detalles sobre 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"
    }
}
```

- SDK de AWS
  - ListAccounts
  - DescribeAccount

Consultar detalles de una política

Si ha iniciado sesión en la cuenta maestra de la organización en la consola de AWS Organizations, puede ver los detalles de las 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Lleve a cabo una de las siguientes operaciones:
   - Vaya a la página Políticas y, a continuación, elija el tipo de política para la política que desea examinar.
   - Vaya a la página Cuentas de AWS y, a continuación, desplácese hasta una unidad organizativa o cuenta a la que está asociada la política. Por último, seleccione la pestaña Políticas para ver la lista de políticas adjuntas.
3. Elija el nombre de la política (no el botón de opción).

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

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 solo la cuenta especificada

El siguiente ejemplo muestra cómo buscar el ID de política de la política que desea examinar. Debe especificar un tipo de política y el comando devuelve todas las políticas 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 solo la política especificada, incluido el documento de política 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\"]}}}}}}"
    ]
}
```

- SDK de AWS
  - ListPolicies
  - DescribePolicy

Eliminar una organización

Cuando ya no necesite una organización, puede eliminarla. Al eliminar una organización no se cierra la cuenta de administración, sino que se elimina, así como la propia organización. La cuenta de administración anterior pasa a ser una Cuenta de AWS independiente que AWS Organizations ya no administra. 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 alguna política dentro de la organización, también se eliminará y no se podrá recuperar.
- 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 independiente. Para obtener más información sobre cómo proporcionar dicha información y eliminar la cuenta, consulte Abandonar una organización desde su cuenta de miembro.
- 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 eliminando la propia organización, la cuenta se puede ver afectada 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 IAM Identity Center requiere una organización para operar, por lo que si elimina una cuenta de una organización que admite IAM Identity Center, 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.

Temas

- Eliminar una organización

Eliminar una organización

Utilice el siguiente procedimiento para eliminar una organización que convierta la cuenta de administración anterior en una Cuenta de AWS independiente que AWS Organizations ya no administra.

> **Permisos mínimos**
>
> Para eliminar una organización, debe iniciar sesión como usuario o rol 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 una organización

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. 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.
3. Vaya a la página Configuración y, a continuación, elija Eliminar organización.
4. En el cuadro de diálogo de confirmación Eliminar organización, ingrese el ID de la organización que se muestra en la línea situada encima del cuadro de texto. A continuación, elija Eliminar organización.

> **Important**
>
> Esta operación no cierra la cuenta de administración, pero la devuelve a una Cuenta de AWS independiente. Para cerrar la cuenta, siga los pasos que se indican en Cierre de una cuenta miembro de la organización.

AWS CLI & AWS SDKs

Para eliminar una organización

Utilice uno de los siguientes comandos para eliminar una organización:

- AWS CLI: delete-organization

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

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

  Este comando no genera ninguna salida si se realiza correctamente.
- SDK de AWS: DeleteOrganization

Administración de las Cuentas de AWS de su organización

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

- Consultar los detalles de las cuentas de su organización. Puede ver el número de ID único de la cuenta, su Nombre de recurso de Amazon (ARN) y sus políticas asociadas.
- Exportar una lista de todas las Cuentas de AWS de su organización. Puede descargar un archivo .csv que contenga los detalles de la cuenta de cada cuenta de su organización.
- Invitar a Cuentas de AWS existentes a que se unan a su organización. Cree invitaciones, administre las invitaciones que ha creado y acepte o rechace invitaciones.
- Crear una Cuenta de AWS como parte de su organización. Cree y obtenga acceso a una Cuenta de AWS que forme parte de su organización automáticamente.
- Actualice contactos alternativos en su organización. Actualice contactos alternativos para su Cuenta de AWS en su organización.
- Eliminar una Cuenta de AWS de su organización. 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. Cuando ya no necesite una Cuenta de AWS, puede cerrar la cuenta para evitar su uso o la acumulación de cargos.

Impacto de estar en una organización

- ¿Cuál es el impacto de una Cuenta de AWS que se une a una organización?
- ¿Cuál es el impacto de una Cuenta de AWS que se crea en una organización?

¿Cuál es el impacto en un Cuenta de AWS que une una organización?

Si invita a una Cuenta de AWS a unirse a una organización y el propietario de la cuenta acepta la invitación, AWS Organizations realiza automáticamente los siguientes cambios de configuración en la cuenta miembro nueva:

- AWS Organizations crea un rol vinculado al servicio denominado `AWSServiceRoleForOrganizations`. 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 al nodo 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 habilitar la confianza de servicio para otro servicio de AWS en la 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**
>
> En el caso de las cuentas de miembros invitados, AWS Organizations no crea automáticamente el rol OrganizationAccountAccessRolede IAM. 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 a la cuenta invitada, puede agregar manualmente el rol. Para obtener más información, consulte Crear la OrganizationAccountAccessRole cuenta en un miembro invitado.

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 que se crea en una organización

Cuando se crea una Cuenta de AWS en una organización, AWS Organizations realiza automáticamente los siguientes cambios en la cuenta miembro nueva:

- AWS Organizations crea un rol vinculado al servicio denominado `AWSServiceRoleForOrganizations`. 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 IAM. OrganizationAccountAccessRole Este rol concede a la cuenta de administración acceso a la nueva cuenta miembro. Aunque este rol puede eliminarse, le recomendamos que no elimine para que esté disponible como opción de recuperación.
- Si tiene política asociadas a la raíz del árbol de la OU, 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 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 Cuenta de AWS a un hombre a unirse a su organización

Después de crear una organización y comprobar que eres el propietario de la dirección de correo electrónico asociada a la cuenta de administración, puedes invitar a una persona existente Cuentas de AWS a unirse a tu organización.

Al invitar a una cuenta, AWS Organizations envía una invitación al propietario de la cuenta, quien decide si acepta o rechaza la invitación. Puedes usar la AWS Organizations consola para iniciar y administrar las invitaciones que envíes a otras cuentas. Solo puede enviar una invitación a otra cuenta desde la cuenta de administración de su organización.

> **Note**
>
> El historial de facturación y los informes de todas las cuentas permanecen en la cuenta del pagador de una organización. Antes de trasladar la cuenta a una nueva organización, descargue los historiales de facturación e informes de cualquier cuenta de miembro que desee conservar. Por ejemplo, informes de costes y uso, informes de facturación detallados o informes generados por el servicio Cost Explorer.

Si eres el administrador de una organización Cuenta de AWS, también puedes 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 y ésta está en el modo Todas las funciones, la cuenta de administración tiene pleno acceso administrativo y control sobre la cuenta del miembro invitado. Sin embargo, a diferencia de las cuentas creadas, la función de `OrganizationAccountAccessRole` IAM no se crea automáticamente en la cuenta del miembro con los permisos que debe asumir la cuenta de administración. Para crearla y configurarla después de que la cuenta invitada se convierta en miembro, sigue estos pasosCrear la OrganizationAccountAccessRole cuenta en un miembro invitado.

> **Note**
>
> Al crear una cuenta en su organización, en lugar de invitar a una cuenta existente a unirse, crea AWS Organizations automáticamente una función de IAM (denominada de forma `OrganizationAccountAccessRole` predeterminada) que puede utilizar para conceder a los usuarios de la cuenta de gestión el acceso de administrador a la cuenta creada.

AWS Organizations crea automáticamente un rol vinculado al servicio en las cuentas de los miembros invitados para facilitar la integración entre AWS Organizations y otros servicios. AWS Para obtener más información, consulte AWS Organizations y roles vinculados al servicio.

Para ver el número de invitaciones que puede enviar por día, consulte Valores mínimos y máximos. 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 una cuenta miembro en su organización.

Important

Debido a restricciones legales y de facturación, Cuentas de AWS solo puedes invitar desde el mismo AWS vendedor y AWS partición que la cuenta de administración. Por ejemplo, en una organización de AWS EMEA, solo puedes invitar a cuentas del vendedor registrado de SARL en AWS EMEA.

- Todas las cuentas de una organización deben proceder del mismo vendedor registrado que la cuenta de administración si Amazon Internet Services Pvt. Ltd (AISPL) creó la cuenta de administración de su organización. Por ejemplo, como AWS vendedor en la India, solo puedes invitar a otras cuentas AISPL a tu organización. No puedes combinar cuentas de AISPL AWS ni de ningún otro vendedor. AWS
- Todas las cuentas de una organización deben provenir de la misma AWS partición que la cuenta de administración. Las cuentas de la Regiones de AWS partición comercial no pueden estar en una organización con cuentas de la partición de regiones de China o cuentas de la partición de AWS GovCloud (US) regiones.

Envío invitaciones a Cuentas de AWS

Para poder 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. Una vez que haya verificado la dirección de correo electrónico, siga los pasos que se describen a continuación para invitar a otras cuentas a que se unan a su organización.

Permisos mínimos

Para invitar a un usuario Cuenta de AWS a unirse a tu organización, debes tener 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Si ya has verificado tu dirección de correo electrónico con AWS, omite este paso.

   Si la dirección de correo electrónico aún no se ha verificado, siga las instrucciones del correo electrónico de verificación en un plazo de 24 horas después de crear la organización. Puede pasar algún tiempo hasta que reciba el correo electrónico de verificación. No puede invitar a una cuenta a unirse a su organización hasta que no verifique su dirección de correo electrónico.
3. Vaya a la página Cuentas de AWS y elija Agregar una cuenta AWS .
4. En la página Agregar un Cuenta de AWS, elija Invitar una cuenta AWS existente.
5. En la AWS página Invitar a una cuenta existente, en la dirección de correo electrónico o ID de cuenta de la persona Cuenta de AWS a la que se va a invitar, introduce la dirección de correo electrónico asociada a la cuenta a la que se va a invitar o su número de ID de cuenta.
6. (Opcional) Para Mensaje a incluir en el mensaje de correo electrónico de invitación, ingrese el texto que desee incluir en la invitación por correo electrónico al propietario de la cuenta invitada.
7. (Opcional) En la sección Agregar etiquetas, especifique una o más etiquetas que se apliquen automáticamente a la cuenta después de que su administrador acepte la invitación. Para ello, elija Agregar etiqueta y, a continuación, ingrese 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 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 la página de Invitaciones donde 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 has invitado a la organización. Este mensaje de correo electrónico incluye un enlace a la AWS Organizations consola, donde el propietario de la cuenta puede ver los detalles y elegir si acepta o rechaza la invitación. Como alternativa, el propietario de la cuenta invitada puede omitir el mensaje de correo electrónico, ir directamente a la AWS Organizations consola, 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 la rechaza, 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"
    }
}
```


- AWS SDK: InviteAccountToOrganization

Administrar las invitaciones pendientes de su organización

Tras iniciar sesión en su cuenta de administración, puede ver todas las cuentas vinculadas de Cuentas de AWS de su organización y cancelar cualquier invitación pendiente (abierta). 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Vaya a la página Invitaciones.

   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

   junto a la invitación que desee cancelar y luego elija Cancelar invitación. Si el botón de opción está atenuado, entonces esa invitación no se puede cancelar.

   El estado de la invitación cambia de OPEN a CANCELED.

   AWS envía un mensaje de correo electrónico al propietario de la cuenta indicándole que has 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, cancel-apretón de manos
- 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.

```
$ 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
    }
}
```

- AWS SDK:, ListHandshakesForOrganizationCancelHandshake

Aceptar o rechazar una invitación de una organización

Cuenta de AWS Es posible que reciba 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.

Note

Solo las cuentas de miembros y las cuentas independientes pueden aceptar o rechazar una invitación para unirse a una organización. Si se envía una invitación a la cuenta de un miembro, dicha cuenta debe abandonar la organización actual antes de aceptar la invitación. Si se envía una invitación a una cuenta de administración que ya forma parte de una organización de AWS , esa cuenta no podrá aceptar la invitación hasta que se eliminen todas las cuentas de miembros de la organización y se elimine la organización.

Permisos mínimos

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

- `organizations:ListHandshakesForAccount`— Necesario para ver la lista de invitaciones en la AWS Organizations consola.
- `organizations:AcceptHandshake`.
- `organizations:DeclineHandshake`.
- `iam:CreateServiceLinkedRole`— Solo se requiere cuando la aceptación de la invitación requiere la creación de un rol vinculado al servicio en la cuenta del miembro para permitir la integración con otros AWS servicios. Para obtener más información, consulte AWS Organizations y roles vinculados al servicio.

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 correo electrónico de invitación, siga las instrucciones indicadas en el correo electrónico de invitación o vaya a la consola AWS Organizations con el navegador y luego elija Invitations (Invitaciones), o vaya directo a la página de member account's Invitation (Invitación de la cuenta miembro).
2. Si se le solicita, inicie sesión en la cuenta invitada como usuario de IAM, asuma un rol de IAM o inicie sesión como usuario raíz de la cuenta (no se recomienda).
3. La página de Invitación de la cuenta de miembro muestra las invitaciones abiertas de su cuenta para unirse a organizaciones.

   Elija Aceptar o Rechazar invitación según corresponda.

   - Si selecciona Aceptar invitación en el paso anterior, la consola le redirige a la página de Información general de la organización con detalles sobre la organización de la que su cuenta es ahora 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 un rol vinculado al servicio en la cuenta del nuevo miembro para facilitar la integración entre y AWS Organizations otros servicios. AWS Para obtener más información, consulte AWS Organizations y roles vinculados al servicio.

     AWS envía un mensaje de correo electrónico al propietario de la cuenta de administración de la organización en el que se indica que has 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 elige Rechazar en el paso anterior, la cuenta permanece en la página Invitación de la cuenta miembro, que muestra todas las demás invitaciones pendientes.

AWS envía un mensaje de correo electrónico al propietario de la cuenta de administración de la organización en el que se indica que has 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: accept-handshake, decline-handshake

  El siguiente ejemplo 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"
    }
}
```

El siguiente ejemplo muestra cómo rechazar una invitación para unirse a una organización.

- AWS SDK: AcceptHandshake, DeclineHandshake

Creación de una cuenta miembro en su organización

Esta página describe cómo crear Cuentas de AWS dentro de su organización en AWS Organizations. Para obtener más información acerca de cómo comenzar a utilizar AWS y crear una sola Cuenta de AWS, consulte el Centro de recursos introductorios.

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

- Crear una Cuenta de AWS que forme parte de la organización
- Acceso a una cuenta miembro con un rol de acceso a la cuenta de administración

Important

- Cuando se crea una cuenta de miembro en la organización, AWS Organizations crea automáticamente un rol de AWS Identity and Access Management (IAM) `OrganizationAccountAccessRole` en la cuenta de miembro, que permite que los usuarios y roles de la cuenta de administración puedan ejercer pleno control administrativo sobre la cuenta de miembro. Esta función está sujeta a las políticas de control de servicios (SCP) que se aplican a la cuenta miembro.

  AWS Organizations también agrega automáticamente una política administrada con el rol `OrganizationAccountAccessRole` a la cuenta del miembro. Esto permite un control centralizado, de modo que toda cuenta adicional asociada a la misma política administrada se actualice automáticamente cada vez que se actualice la política. Anteriormente, las cuentas nuevas creadas dentro de una organización recibían una política insertada que solo se aplicaba a esa única cuenta. Para obtener más información acerca de las políticas administradas, consulte Políticas administradas y políticas insertadas en la Guía del usuario de IAM.

  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.
- Si esta organización se administra con AWS Control Tower, a continuación, cree sus cuentas mediante Account Factory AWS Control Tower en la consola AWS Control Tower o API. Si crea una cuenta en Organizations, esa cuenta no está inscrita en AWS Control Tower. Para obtener más información, consulte Referencia del tipo de recurso fuera deAWS Control Tower en la Guía del usuarioAWS Control Tower.

Note

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

Crear una Cuenta de AWS que forme parte de la organización

Luego de iniciar sesión en la cuenta de administración de la organización, puede crear cuentas que se conviertan automáticamente en cuentas miembro de su organización. Al crear una cuenta utilizando el siguiente procedimiento, AWS Organizations copia automáticamente la siguiente información del contacto principal de la cuenta de administración a la cuenta miembro nueva:

- Número de teléfono
- Nombre de la empresa
- URL de sitio web
- Dirección

También copia el idioma de comunicación y la información de Marketplace (el proveedor de la cuenta en algunas Regiones de AWS) de la cuenta de administración.

> **Note**
>
> AWS no recopila automáticamente toda la información necesaria para que una cuenta miembro opere como cuenta independiente. Si alguna vez necesita eliminar la cuenta miembro de la organización y convertirla en cuenta independiente, debe proporcionar la información solicitada para la cuenta antes de poder eliminarla. Para obtener más información, consulte Abandonar una organización desde su cuenta de miembro.

> **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 una Cuenta de AWS que forme parte automáticamente de su organización

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, elija Agregar un Cuenta de AWS.
3. En la página Agregar una Cuenta de AWS, elija Crear una Cuenta de AWS (se elige de forma predeterminada).
4. En la página Crear una Cuenta de AWS, para Nombre de Cuenta de AWS ingrese el nombre que desee 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. Para Dirección de correo electrónico del propietario de la cuenta, ingrese la dirección de correo electrónico del propietario de la cuenta. Esta dirección de correo electrónico no se puede asociar ya con 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 el 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 sus cuentas para mayor coherencia.

   > **Important**
   >
   > Recuerde este nombre de rol. Lo necesitará más adelante para conceder acceso a la nueva cuenta a los usuarios y roles de la cuenta de administración.

7. (Opcional) En la sección Etiquetas, agregue una o varias etiquetas con Agregar etiqueta y 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.
8. Seleccione Crear Cuenta de AWS.

- Si aparece un error que indica que ha superado la cuota de cuenta de la organización, consulte Obtengo un mensaje de "cuota superada" cuando intento agregar una cuenta a mi organización.
- 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.
- Si el error persiste, póngase en contacto con AWS Support.

La página Cuentas de AWS aparece, con su cuenta nueva 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 de Acceso a las cuentas miembro de la organización.

> **Note**
>
> Al crear una cuenta, AWS Organizations asigna inicialmente una contraseña larga (64 caracteres), compleja y aleatoria 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.

AWS CLI & AWS SDKs

Para crear una Cuenta de AWS que forme parte automáticamente de su organización

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 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"
  }
}
```

- SDK de AWS: CreateAccount

Acceso a las cuentas miembro de la organización

Al crear una cuenta en la organización, además del usuario raíz, AWS Organizations crea automáticamente un rol de IAM con el nombre predeterminado `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 Organizations no crea ningún otro usuario o rol. Para tener acceso a las cuentas de su organización, debe utilizar uno de los siguientes métodos:

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

de usuario raíz en la Guía del usuario de IAM. Para obtener recomendaciones de seguridad adicionales para los usuarios raíz, consulte Mejores prácticas para los usuarios raízCuenta de AWS.

- Si crea una cuenta usando las herramientas proporcionadas como parte de AWS Organizations, puede tener acceso a la cuenta usando un rol preconfigurado denominado `OrganizationAccountAccessRole` que existe en todas las cuentas nuevas que usted crea de esta forma. Para obtener más información, consulte Acceso a una cuenta miembro con un rol de acceso a la cuenta de administración.
- Si invita a una cuenta existente a que se una a su organización y la cuenta acepta la invitación, puede elegir crear un rol 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 Crear la OrganizationAccountAccessRole cuenta en un miembro invitado. 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.
- Utilice AWS IAM Identity Center y habilite el acceso de confianza para IAM Identity Center con AWS Organizations. Los usuarios pueden iniciar sesión en el portal de acceso de AWS con sus credenciales corporativas y acceder a recursos en sus cuentas de administración o de miembro asignadas.

  Para obtener más información, consulte Multi-account permissions (Permisos de varias cuentas) en la Guía del usuario de AWS IAM Identity Center. Para obtener más información acerca de cómo configurar el acceso de confianza para IAM Identity Center, consulte AWS IAM Identity Center y AWS Organizations.

> **Permisos mínimos**
>
> Para tener acceso a una Cuenta de AWS desde cualquier otra cuenta de su organización, debe contar con el permiso siguiente:
>
> - `sts:AssumeRole` - El elemento `Resource` 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. Para obtener más información, consulte He olvidado la contraseña de mi usuario root Cuenta de AWS en la Guía del usuario de AWS inicio de sesión.

Notas

- 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 habilite 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. Póngase en contacto con AWS Billing and Support para obtener ayuda.

Crear la OrganizationAccountAccessRole cuenta en un miembro invitado

De forma predeterminada, si crea una cuenta miembro como parte de su organización, AWS crea automáticamente un rol en la cuenta que concede permisos de administrador a los usuarios de IAM en la cuenta maestra. 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.

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.

AWS Management Console

Para crear un rol de administrador de AWS Organizations 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de miembro. El usuario o el rol deben tener permiso para crear roles y políticas de IAM.
2. En la consola de IAM, vaya a Funciones y, a continuación, seleccione Crear función.
3. Elija y Cuenta de AWS, a continuación, seleccione Otro Cuenta de AWS.
4. Introduzca el número de ID de cuenta de 12 dígitos de la cuenta de administración a la que desea conceder acceso de administrador. En Opciones, ten en cuenta lo siguiente:
   - Para este rol, dado que las cuentas son internas a su empresa, no debe seleccionar Require external ID. Para obtener más información sobre la opción de ID externa, consulta ¿Cuándo debo usar una ID externa? en la Guía del usuario de IAM.
   - Si ha habilitado y configurado MFA, puede elegir que se requiera autenticación mediante un dispositivo MFA. Para obtener más información sobre la MFA, consulte Uso de la autenticación multifactor (MFA) AWS en la Guía del usuario de IAM.
5. Elija Siguiente.
6. En la página Añadir permisos, elija el nombre de la política AWS gestionada **`AdministratorAccess`** y, a continuación, seleccione Siguiente.
7. En la página Nombre, revisión y creación, especifique un nombre de 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.
8. Su nuevo rol aparecerá en la lista de roles disponibles. Seleccione el nombre del nuevo rol para ver los 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.
9. 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.
10. Vaya a Políticas y, a continuación, seleccione Crear política.
11. En Service, seleccione STS.

12. En Actions (Acciones), comience a escribir **`AssumeRole`** en el cuadro Filter (Filtro) y marque la casilla cuando aparezca.
13. En Recursos, asegúrese de que esté seleccionada la opción Específico y, a continuación, elija Agregar ARN.
14. Escriba su número de ID de cuenta miembro de AWS y, a continuación, el nombre del rol que haya creado anteriormente en los pasos 1-8. Seleccione Agregar ARN.
15. Si está concediendo un permiso para asumir la función en varias cuentas miembro, repita los pasos 14 y 15 para cada cuenta.
16. Elija Siguiente.
17. En la página Revisar y crear, introduzca un nombre para la nueva política y, a continuación, elija Crear política para guardar los cambios.
18. Elija Grupos de usuarios en el panel de navegación y, a continuación, elija el nombre del grupo (no la casilla de verificación) que desee usar para delegar la administración de la cuenta del miembro.
19. Elija la pestaña Permisos.
20. Elija Agregar permisos, elija Adjuntar políticas y, a continuación, seleccione la política que creó en los pasos 11 a 18.

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.

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

Cuando crea una cuenta miembro con la consola de AWS Organizations, AWS Organizations crea automáticamente un rol de IAM denominado `OrganizationAccountAccessRole` en la cuenta. Este rol tiene permisos administrativos completos en la cuenta miembro. El ámbito de acceso de este rol incluye todas las entidades principales de la cuenta de administración, de modo que el rol esté configurado para conceder ese 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

Crear la OrganizationAccountAccessRole cuenta en un miembro invitado. Para utilizar este rol para tener acceso a la cuenta miembro, debe iniciar sesión como usuario de la cuenta de administración con 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.

AWS Management 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 en https://console.aws.amazon.com/iam/ con un usuario que tenga 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 ???.

   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, escribe **`assume`** en el cuadro de búsqueda para filtrar la lista y, a continuación, selecciona la AssumeRoleopción.
5. En la sección Recursos, elija Específico, elija Agregar ARN y, a continuación, escriba el número de cuenta del miembro y el nombre del rol que creó en la sección anterior (se recomienda asignarle un nombre`OrganizationAccountAccessRole`).
6. Seleccione Añadir ARN 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 Siguiente.
9. En la página Revisar y crear, introduzca un nombre para la nueva política. Por ejemplo: **`GrantAccessToOrganizationAccountAccessRole`**. También puede agregar 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 Grupos de usuarios y, a continuación, elija el nombre del grupo (no de la casilla de verificación) cuyos miembros desee que puedan asumir el rol en la cuenta del miembro. Si es necesario, puede crear un grupo nuevo.

12. Elija la pestaña Permisos, elija Agregar permisos y luego, Asociar políticas.
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 mediante Step 10. También puede filtrar todas las políticas AWS gestionadas seleccionando Todos los tipos y, a continuación, gestionadas por el cliente.
14. Marca la casilla situada junto a tu póliza y, a continuación, selecciona Adjuntar políticas.

Los usuarios de IAM que sean miembros del grupo ahora tendrán permisos para cambiar el nuevo rol en la consola de AWS Organizations siguiendo el procedimiento que se detalla a continuación.

AWS Management Console

Para cambiar al rol 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. En la esquina superior derecha de la consola de AWS Organizations, elija el enlace que contiene el nombre de inicio de sesión y, a continuación, elija Switch Role (Cambiar rol).
2. Escriba el número de ID de la cuenta y el nombre del rol 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 original hasta que cambie otra vez a este rol.
5. Cuando haya terminado de realizar acciones que requieran los permisos del rol, puede volver a su usuario de IAM normal. Elige el nombre del rol en la esquina superior derecha (el que hayas especificado como nombre para mostrar) y, a continuación, selecciona Volver a. *UserName*

Recursos adicionales

- Para obtener más información sobre la concesión de permisos para cambiar de rol, consulte Otorgar permisos a un usuario para cambiar de rol en la Guía del usuario de IAM.
- Para obtener más información sobre el uso de un rol para el que se le han otorgado permisos, consulte Cambiar a un rol (consola) en la Guía del usuario de IAM.
- Para ver un tutorial sobre el uso de roles para el acceso entre cuentas, consulte el Tutorial: Delegar el acceso a través del Cuentas de AWS uso de roles de IAM en la Guía del usuario de IAM.
- Para obtener más información acerca de cómo cerrar Cuentas de AWS, consulte Cierre de una cuenta miembro de la organización.

Exportación de los detalles de las Cuenta de AWS de su organización

Con AWS Organizations, los usuarios de cuentas de administración y los administradores delegados de una organización pueden exportar un archivo .csv con los detalles de todas las cuentas de una organización. Como resultado, los administradores de la organización pueden ver las cuentas fácilmente y filtrar por estado: `ACTIVE`, `SUSPENDED` o `PENDING`. Si su organización tiene muchas cuentas, la opción de descargar el archivo .csv ofrece una forma sencilla de ver y ordenar los detalles de las cuentas en una hoja de cálculo.

Antes, la única forma de ver las cuentas era mirar la jerarquía de cuentas o la visualización de listas en la consola de AWS Organizations.

> **Note**
>
> Solo las entidades principales de la cuenta de administración pueden descargar la lista de cuentas.

Exportación de una lista de todas las Cuentas de AWS de su organización

Cuando se inicia sesión en la cuenta de administración de la organización, se puede obtener una lista de todas las cuentas que forman parte de la organización en forma de archivo .csv. La

lista contiene los detalles de las cuentas individuales; no obstante, no especifica a qué unidad organizativa (OU) pertenece cada cuenta.

El archivo .csv contiene la siguiente información sobre cada cuenta:

- Account ID (ID de cuenta): identificador de cuenta numérico. Por ejemplo: 123456789012
- ARN (ARN): nombre de recurso de Amazon de la cuenta. Por ejemplo: `arn:aws:organizations::123456789012account/o-o1gb0d1234/123456789012`
- Email (Correo electrónico): dirección de correo electrónico asociada a la cuenta. Por ejemplo: marymajor@example.com
- Name (Nombre): nombre de la cuenta proporcionado por el creador de la cuenta. Por ejemplo: cuenta de pruebas de fase
- Status (Estado): estado de la cuenta dentro de la organización. El valor puede ser `PENDING`, `ACTIVE` o `SUSPENDED`.
- Joined method (Método de unión): especifica cómo se creó la cuenta. El valor puede ser `INVITED`, o `CREATED`.
- Joined timestamp (Marca de tiempo de unión): fecha y hora en que la cuenta se unió a la organización.

> **Permisos mínimos**
>
> Para exportar un archivo .csv con todas las cuentas miembro de su organización, debe contar con los permisos siguientes:
>
> - `organizations:DescribeOrganization`
> - `organizations:ListAccounts`

AWS Management Console

Para exportar un archivo .csv de todas las Cuentas de AWS de su organización

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

2. Elija Actions (Accciones), y luego, para Cuenta de AWS, elija Export account list (Exportar lista de cuentas). El banner azul de la parte superior de la página indica "Export is in progress!" (La exportación está en curso)
3. Cuando el archivo esté listo, el banner se vuelve verde e indica "Download is ready!" (La descarga está lista) Elija Download CSV (Descargar CSV). El archivo `Organization_accounts_information.csv` se descarga en su dispositivo.

AWS CLI & AWS SDKs

La única forma de exportar el archivo .csv con los detalles de las cuenta es mediante la AWS Management Console. No se puede exportar el archivo .csv de la lista de cuentas mediante la AWS CLI.

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. Al eliminar una cuenta de miembro, no se cierra la cuenta, sino que se elimina la cuenta de miembro de la organización. La cuenta de miembro anterior pasa a ser una Cuenta de AWS independiente que AWS Organizations ya no administra. Posteriormente, la cuenta ya no estará sujeta a ninguna política y será responsable del pago de sus propias facturas. A la cuenta de administración de la organización ya no se le cobrará ningún gasto acumulado en la cuenta una vez que se haya retirado de la organización.

Para obtener información acerca de cómo eliminar la cuenta de administración, consulte Eliminar una organización.

Temas

- Consideraciones antes de eliminar una cuenta de una organización
- Eliminar una cuenta de miembro de su organización
- Abandonar una organización desde su cuenta de miembro

Consideraciones antes de eliminar una cuenta de una organización

Antes de eliminar una cuenta, es importante que tenga en cuenta 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 AWS Organizations , la API o los comandos de AWS CLI, no se recopila automáticamente toda la información necesaria para las cuentas independientes. Por 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. AWS utiliza el método de pago para cobrar cualquier actividad de AWS facturable (no AWS del nivel gratuito) que se produzca mientras la cuenta no esté asociada a una organización. Para eliminar una cuenta que aún no cuenta con esta información, siga los pasos que se indican en Abandonar una organización desde su cuenta de miembro.
- 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 todos los nuevos costos AWS 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 cualquier servicio AWS habilitado 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 deshabilitar o cambiar la cuenta de administrador delegado para un servicio de AWS, consulte la documentación correspondiente a dicho servicio.
- Incluso después de eliminadas las cuentas creadas mediante la consola AWS Organizations o la API de `CreateAccount` desde una organización, (i) dichas cuentas se rigen por los términos del acuerdo con nosotros de la cuenta de administración que las haya creado, y (ii) la cuenta de administración 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 AWS.
- 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.

- Cuando elimina una cuenta miembro de la organización, no se eliminan automáticamente los roles de IAM que se hayan creado para permitir el acceso de la cuenta de administración de la organización. Si desea eliminar este acceso desde la cuenta de administración anterior de la organización, debe eliminar manualmente el rol de IAM. Para obtener información acerca de cómo eliminar un rol, consulte Eliminación de roles o perfiles de instancia en la Guía del usuario de IAM.

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.
- Las entidades principales de la cuenta ya no se verán afectadas por ninguna política que se aplique en la organización. Esto significa que las restricciones impuestas por esas SCP ya no existen, y que los usuarios y los roles de la cuenta podrían tener más permisos que antes. Otros tipos de políticas de organización ya no se pueden aplicar ni procesar.
- Si utiliza la clave de condición `aws:PrincipalOrgID` en cualquier política para restringir el acceso solo a usuarios y roles de Cuentas de AWS en su organización, luego debe revisar y posiblemente actualizar estas política antes de eliminar la cuenta de miembro. Si no actualiza las políticas, 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 una AWS, los usuarios de esa cuenta ya no podrán utilizar dicho servicio.

Eliminar una cuenta de miembro de su organización

Cuando inicie 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. Este procedimiento se aplica únicamente a las cuentas de miembro. Para eliminar la cuenta de administración, debe eliminar la organización.

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 la consola AWS Artifact en la página Acuerdos de Organization AWS Artifact.

Permisos mínimos

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

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

Si decidió iniciar sesión como usuario o rol en una cuenta de miembro en el paso 5, ese usuario o rol debe tener los siguientes permisos:

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de 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 información de pago faltante, el usuario debe tener permisos de `aws-portal:ModifyBilling` y de `aws-portal:ModifyPaymentMethods` (si la cuenta aún no ha migrado a permisos específicos) O permisos de `payments:CreatePaymentInstrument` y de `payments:UpdatePaymentPreferences` (si la cuenta ha migrado a permisos específicos). Además, la cuenta miembro debe tener habilitado el acceso del usuario de IAM a la facturación. Si no está habilitado, consulte Activación del acceso a la consola Billing and Cost Management en la Guía del usuario de AWS Billing.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la pestaña Cuentas de AWS, busque y marque la casilla
junto a cada cuenta miembro que desea eliminar de su organización. Puede navegar por la jerarquía de unidades organizativas o habilitar Ver solo Cuentas de AWS para ver una lista plana de cuentas sin la estructura de unidad organizativa. Si tiene muchas cuentas, puede que tenga que elegir Cargar más cuentas en 'Nombre de OU' en la parte inferior de la lista para encontrar todas las que desea 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. Seleccionar Acciones y, a continuación, en Cuenta de AWS, elija Eliminar de la organización.
4. En el navegador ¿Eliminar cuenta 'Nombre de la cuenta' (#account-id) de la organización?, elija Eliminar la cuenta.
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 la cuenta 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.

d. Elimine de la organización los roles de IAM que conceden acceso a su cuenta.

> **Important**
>
> Si la cuenta se creó en la organización, Organizations creó 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, entonces Organizations no creó 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 acerca de cómo eliminar un rol, consulte Eliminación de roles o perfiles de instancia en la Guía del usuario de IAM.

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 si se realiza correctamente.

- SDK de AWS: RemoveAccountFromOrganization

Una vez que se haya eliminado de la organización la cuenta de miembro, asegúrese de eliminar de la organización los roles de IAM que dan acceso a su cuenta.

> **Important**
>
> Si la cuenta se creó en la organización, Organizations creó 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, entonces Organizations no creó 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 acerca de cómo eliminar un rol, consulte Eliminación de roles o perfiles de instancia en la Guía del usuario de IAM.

En su lugar, las cuentas de los miembros pueden eliminarse a sí mismas con el comando leave-organization. Para obtener más información, consulte Abandonar una organización desde su cuenta de miembro.

Abandonar una organización desde su cuenta de miembro

Cuando inicia sesión en una cuenta miembro, puede eliminar esa cuenta de su organización. Para ello, complete el procedimiento siguiente. Este procedimiento se aplica únicamente a las cuentas de miembro. La cuenta de administración no puede abandonar la organización mediante esta técnica. Para eliminar la cuenta de administración, debe eliminar la organización.

> **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.

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 los acuerdos de la organización en la consola AWS Artifact en la página Acuerdos de Organization AWS Artifact. 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.

Permisos mínimos

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

- `organizations:DescribeOrganization`: solo se requiere cuando se utiliza la consola de 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 información de pago faltante, el usuario debe tener permisos de `aws-portal:ModifyBilling` y de `aws-portal:ModifyPaymentMethods` (si la cuenta aún no ha migrado a permisos específicos) O permisos de `payments:CreatePaymentInstrument` y de `payments:UpdatePaymentPreferences` (si la cuenta ha migrado a permisos específicos). Además, la cuenta miembro debe tener habilitado el acceso del usuario de IAM a la facturación. Si no está habilitado, consulte Activación del acceso a la consola Billing and Cost Management en la Guía del usuario de AWS Billing.

AWS Management Console

Para abandonar una organización desde su cuenta de miembro

1. Inicie sesión en la consola de AWS Organizations en consola AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en una cuenta de 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.
2. En la página Panel de Organizations, seleccione Abandonar esta organización.
3. En el cuadro de diálogo ¿Confirmar el abandono de la organización?, elija Abandonar organización. Cuando se le indique, confirme su elección para eliminar la cuenta. Una vez confirmado, será redirigido 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 aparece el mensaje Todavía no puede abandonar la organización, significa que su cuenta no tiene toda la información necesaria para funcionar como una cuenta independiente. En tal caso, continúe en el paso siguiente.
4. Si el cuadro de diálogo ¿Confirmar el abandono de la organización? muestra el mensaje Todavía no puede abandonar la organización, seleccione el enlace Completar los pasos de inscripción de la cuenta.
5. En la página Inscribirse a AWS, introduzca toda la información solicitada para que la cuenta se convierta en una cuenta independiente. Puede incluir los siguientes tipos de información:

   - Nombre y dirección de contacto
   - Método de pago válido
   - Verificación de número de teléfono
   - Opciones de planes de soporte
6. Cuando vea el cuadro de diálogo que le avisa de que el proceso de inscripción se ha completado, seleccione Leave organization.

   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.

7. Elimine de la organización los roles de IAM que conceden acceso a su cuenta.

> **Important**
>
> Si la cuenta se creó en la organización, Organizations creó 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, entonces Organizations no creó 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 acerca de cómo eliminar un rol, consulte Eliminación de roles o perfiles de instancia en la Guía del usuario de IAM.

AWS CLI & AWS SDKs

Para abandonar una organización como cuenta miembro

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

- AWS CLI: leave-organization

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

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

  Este comando no genera ninguna salida si se realiza correctamente.
- SDK de AWS: LeaveOrganization

Una vez que la cuenta del miembro haya dejado la organización, asegúrese de eliminar de la organización los roles de IAM que dan acceso a su cuenta.

> **Important**
>
> Si la cuenta se creó en la organización, Organizations creó 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, entonces Organizations no creó 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 acerca de cómo eliminar un rol, consulte Eliminación de roles o perfiles de instancia en la Guía del usuario de IAM.

En su lugar, un usuario también puede eliminar las cuentas de los miembros de la cuenta de administración con el comando remove-account-from-organization. Para obtener más información, consulte Eliminar una cuenta de miembro de su organización.

Cierre de una cuenta miembro de la organización

Si ya no necesitas una cuenta de miembro en tu organización, puedes cerrarla desde la AWS Organizations consola siguiendo las instrucciones de esta sección. Solo puedes cerrar una cuenta de miembro mediante la AWS Organizations consola si tu organización está en el modo Todas las funciones.

También puedes cerrar una Cuenta de AWS directamente desde la página de la cuenta AWS Management Console después de iniciar sesión como usuario root. Para step-by-step obtener instrucciones, consulta Cerrar un Cuenta de AWS en la Guía de administración deAWS cuentas.

Para cerrar una cuenta de administración, consulteCerrar una cuenta de administración en su organización.

Cómo cerrar una cuenta miembro

Cuando inicia sesión en la cuenta de administración de la organización, puede cerrar las cuentas de miembro que pertenecen a su organización. Para ello, siga los pasos que se describen a continuación.

> **Important**
>
> Antes de cerrar su cuenta de miembro, le recomendamos encarecidamente que revise las consideraciones y comprenda el impacto de cerrar una cuenta. Para obtener más información, consulte Lo que debe saber antes de cerrar su cuenta y Qué esperar después de cerrar su cuenta en la Guía de administración deAWS cuentas.

AWS Management Console

Para cerrar la cuenta de un miembro desde la AWS Organizations consola

1. Inicie sesión en la consola deAWS Organizations.
2. En la página Cuentas de AWS, busque y elija el nombre de la cuenta de miembro que desea cerrar. Puede navegar por la jerarquía de unidades organizativas o ver una lista plana de cuentas sin la estructura de unidad organizativa.
3. Elija Close (Cerrar) junto al nombre de la cuenta en la parte superior de la página. Las organizaciones que estén en el modo de facturación unificada no podrán ver el botón Cerrar en la consola. Para cerrar una cuenta en el modo de facturación unificada, sigue los pasos de la pestaña Cuenta independiente de Cómo cerrar tu cuenta en la Guía de administración deAWS cuentas.
4. Seleccione cada casilla de verificación para confirmar todos las instrucciones de cierre de cuenta obligatorias.
5. Introduce el ID de la cuenta del miembro y, a continuación, selecciona Cerrar cuenta.

> **Note**
>
> Cualquier cuenta de miembro que cierre mostrará una `SUSPENDED` etiqueta junto al nombre de la cuenta en la AWS Organizations consola.

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

Si lo desea, puede cerrar la cuenta de un AWS miembro directamente desde la página de cuentas del AWS Management Console. Para obtener step-by-step orientación, sigue las instrucciones de Cerrar y de Cuenta de AWS la Guía de administración deAWS cuentas.

AWS CLI & AWS SDKs

Para cerrar una Cuenta de AWS

Puede utilizar uno de los siguientes comandos para cerrar una cuenta de AWS :

- AWS CLI: close-account

```
$ aws organizations close-account \
    --account-id 123456789012
```

Este comando no genera ninguna salida si se realiza correctamente.

- AWS SDK: CloseAccount

Protección de cuentas miembro contra el cierre

Si desea proteger una cuenta miembro de un cierre accidental, puede crear una política de IAM para especificar qué cuentas están exentas de cierre. No se puede cerrar ninguna cuenta de miembro que esté protegida con estas políticas. Esto no se puede lograr con una SCP, porque no afecta a las entidades principales en la cuenta de administración.

Puede crear una política de IAM que niegue el cierre de cuentas de dos formas:

- Haga una lista explícita de cada cuenta que desea proteger en la política mediante la inclusión del `arn` en el elemento `Resource`. Para ver un ejemplo, consulte Evitar que las cuentas miembro enumeradas en esta política se cierren.
- Etiquete cuentas individuales para evitar que se cierren. Utilice la clave de condición global de etiqueta `aws:ResourceTag` en la política para evitar que se cierre cualquier cuenta con esta etiqueta. Para obtener información sobre cómo etiquetar una cuenta, consulte Etiquetado de los recursos de Organizations. Para ver un ejemplo, consulte Evitar que las cuentas miembro con etiquetas se cierren .

Ejemplos de políticas de IAM que impiden los cierres de las cuentas miembro

Los siguientes ejemplos de código muestran dos métodos diferentes que puede utilizar para impedir que las cuentas de los miembros cierren sus cuentas.

Evitar que las cuentas miembro con etiquetas se cierren

Puede adjuntar la siguiente política a una identidad en su cuenta de administración. Esta política impide que las entidades principales de la cuenta de administración cierren cualquier cuenta de miembro etiquetada con la clave de condición global de etiqueta `aws:ResourceTag`, la clave `AccountType` y el valor de etiqueta `Critical`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventCloseAccountForTaggedAccts",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/AccountType": "Critical"}
            }
        }
    ]
}
```

Evitar que las cuentas miembro enumeradas en esta política se cierren

Puede adjuntar la siguiente política a una identidad en su cuenta de administración. Esta política impide que las entidades principales de la cuenta de administración cierren las cuentas miembro especificadas de forma explícita en el elemento `Resource`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PreventCloseAccount",
            "Effect": "Deny",
            "Action": "organizations:CloseAccount",
            "Resource": [
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789012",
                "arn:aws:organizations::555555555555:account/
o-12345abcdef/123456789014"
            ]
        }
```

```
    ]
}
```

Cerrar una cuenta de administración en su organización

Para cerrar la cuenta de administración de su organización, primero debe cerrar o eliminar todas las cuentas de los miembros de la organización. Al cerrar la cuenta de administración, también se eliminan la instancia AWS Organizations y las políticas que haya creado dentro de esa organización una vez transcurrido el período posterior al cierre.

¿Cómo cerrar una cuenta de administración

Use el siguiente procedimiento para cerrar una cuenta de administración.

> **Important**
>
> Antes de cerrar su cuenta de administración, le recomendamos encarecidamente que revise las consideraciones y comprenda el impacto de cerrar una cuenta. Para obtener más información, consulte Lo que debe saber antes de cerrar su cuenta y Qué esperar después de cerrar su cuenta en la Guía de administración de AWS cuentas.

AWS Management Console

Para cerrar una cuenta de administración desde la página de cuentas

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

1. Inicie sesión AWS Management Console como usuario raíz de la cuenta de administración que desee cerrar. No puedes cerrar una cuenta si has iniciado sesión como usuario o rol de IAM.
2. Compruebe que no queden cuentas de miembros activas en su organización. Para ello, ve a la AWS Organizationsconsola y asegúrate de que todas las cuentas de los miembros aparezcan `Suspended` junto a sus nombres de cuenta. Si tienes una cuenta de miembro que

sigue activa, tendrás que seguir las instrucciones que se proporcionan Cierre de una cuenta miembro de la organización antes de pasar al siguiente paso.

3. En la barra de navegación de la esquina superior derecha, elige el nombre o número de tu cuenta y, a continuación, selecciona Cuenta.
4. En la página Cuenta, desplázate hasta la parte inferior de la página hasta la sección Cerrar cuenta. Lee y asegúrate de entender el proceso de cierre de la cuenta.
5. Pulse el botón Cerrar cuenta para iniciar el proceso de cierre de la cuenta.
6. En unos minutos, recibirás un correo electrónico de confirmación de que tu cuenta se ha cerrado.

AWS CLI & AWS SDKs

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

Actualización de contactos alternativos de su organización

Puede actualizar contactos alternativos para cuentas de su organización mediante la Consola de AWS Organizations o mediante programación utilizando AWS CLI o AWS SDK. Para obtener información sobre cómo actualizar contactos alternativos, consulte Acceso o actualización de los contactos alternativos en la AWS Referencia de administración de cuentas de.

Actualización de la información de contacto principal de su organización

Puede actualizar la información de contacto principal de las cuentas de su organización mediante la consola de AWS Organizations o mediante programación con la AWS CLI o los AWS SDK. Para obtener información sobre cómo actualizar la información de contacto principal, consulte Acceso o actualización del contacto principal de la cuenta en la Referencia de administración de cuentas de AWS.

Actualización de Regiones de AWS habilitada en su organización

Puede actualizar las Regiones de AWS habilitadas para las cuentas de su organización mediante la consola de AWS Organizations. Para saber cómo actualizar las Regiones de AWS habilitadas,

consulte Specifying which Regiones de AWS your account can use (Especificación de las Regiones de AWS que puede utilizar su cuenta) en la AWS Account Management Reference (Referencia de gestión de cuentas de AWS).

Administración de políticas en AWS Organizations

Las políticas de AWS Organizations le permiten aplicar tipos adicionales de administración a las Cuentas de AWS de su organización. Puede utilizar políticas cuando todas las características están habilitadas 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

Organizations ofrece tipos de política en las dos categorías generales siguientes:

Políticas de autorización

Las políticas de autorización le ayudan a administrar de forma centralizada la seguridad de las Cuentas de AWS de 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.

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 los servicios de inteligencia artificial (IA)le permiten controlar la recopilación de datos para Servicios de IA AWS para todas las cuentas de su organización.
- Las políticas de copia de seguridad 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 le ayudan a estandarizar las etiquetas asociadas a los recursos de AWS de las cuentas de su organización.

En la siguiente tabla se resumen algunas características de cada tipo de política. Para conocer las características adicionales de estos tipos de políticas, consulte Cuotas para AWS Organizations.

Tipo de política	Afecta a la administración de la cuenta	Número máximo que se puede asociar a un nodo raíz, unidad organizativa o cuenta	Tamaño máximo	Admite la visualización efectiva de la política para la unidad organizativa o cuenta
SCP	No	5	5120 caracteres	No
Política de exclusión de servicios de IA	Sí	5	2500 caracteres	Sí
Política de copia de seguridad	Sí	10	10,000 caracteres	Sí
Política de etiquetas	Sí	10	10,000 caracteres	Sí

Uso de políticas en su organización

- Habilitar y deshabilitar tipos de política
- Obtener información sobre las políticas de su organización
- Administrador delegado para AWS Organizations

- Políticas de administración
- Políticas de control de servicios (SCP)

Habilitar y deshabilitar tipos de política

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 de Organizations
- `organizations:ListRoots`: solo se requiere cuando se utiliza la consola de 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas, elija elegir nombre del tipo de política que desea habilitar.
3. En la página de tipo de política, elija Habilitar ***tipo de política***.

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

AWS CLI & AWS SDKs

Para habilitar un tipo de política

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

- AWS CLI: Tipo de política sencilla

  En el siguiente ejemplo, se muestra cómo habilitar políticas de copia de seguridad para la organización. Tenga en cuenta que debe especificar el ID del nodo 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"
            }
        ]
    }
}
```

  La lista de `PolicyTypes` en la salida ahora incluye el tipo de política especificado con el `Status` de `ENABLED`.

- SDK de AWS: 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 políticas de control de servicios) Si vuelve a habilitar el tipo de política SCP más adelante, inicialmente todas las entidades del nodo raíz de la organización se adjuntan solo al SCP `FullAWSAccess` predeterminado. Los archivos adjuntos de las SCP a entidades se pierden cuando las SCP están deshabilitadas en la organización. Si posteriormente desea volver a habilitar SCP, debe volver a adjuntarlos al nodo 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 de Organizations
- `organizations:ListRoots`: solo se requiere cuando se utiliza la consola de 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas, elija el nombre del tipo de política que desea desactivar.
3. En la página de tipo de política, elija Desactivar ***tipo de política***.
4. En el cuadro de diálogo de confirmación, ingrese la palabra **`disable`**, y luego elija Desactivar.

   La lista de políticas 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: disable-policy-type

  En el siguiente ejemplo, se muestra cómo desactivar las políticas de copia de seguridad para la organización. Tenga en cuenta que debe especificar el ID del nodo 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": []
    }
}
```

  La lista de `PolicyTypes` en la salida ya no incluye el tipo de política especificado.

- SDK de AWS: 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 políticas de su organización en el AWS Management Console o mediante un comando AWS Command Line Interface (AWS CLI) o una operación SDK AWS.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas, elija la política que desea enumerar.

   Si el tipo de política especificado está habilitado, la consola muestra una lista de todas las políticas de ese tipo que están disponibles actualmente en la organización.
3. Vuelva a la página de Políticas y repita para cada tipo de política.

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 política que desea ver. Repetir 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
        }
```

```
    ]
}
```

- SDK de AWS:ListPolicies

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

> **Permisos mínimos**
>
> Para mostrar las políticas que están asociadas a un nodo raíz, unidad organizativa (OU) o cuenta de su organización, debe contar con el permiso siguiente:
>
> - `organizations:ListPoliciesForTarget` con un elemento `Resource` en la misma instrucción de política que incluye el Nombre de recurso de Amazon (ARN) de el objetivo especificado (o "*")

AWS Management Console

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

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, elija el nombre del nodo 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 del nodo raíz, unidad organizativa o cuenta, elija la pestaña Políticas.

   La pestaña Políticas muestra todas las políticas asociadas a ese nodo raíz, unidad organizativa o cuenta, agrupadas por tipo de política.

AWS CLI & AWS SDKs

Para mostrar todas las políticas que están asociadas directamente a un nodo 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 políticas de control de servicios asociadas a la unidad organizativa especificada. Debe especificar tanto el ID del nodo raíz, la unidad organizativa o la cuenta como el tipo de política 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
        }
    ]
}
```

- SDK de AWS: 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 mostrar todos los 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas, elija el tipo de política y, a continuación, elija el nombre de la política cuyos datos adjuntos desea examinar.
3. Elija la pestaña Objetivos, para mostrar una tabla de cada nodo raíz, unidad organizativa y cuenta a la que está asociada la política.

AWS CLI & AWS SDKs

Para mostrar todos los 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 al nodo raíz, unidades organizativas y cuentas de la política 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"
        }
    ]
}
```

- SDK de AWS: 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas, elija el tipo de política de la política que desea examinar y, a continuación, elija el nombre de la política.

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

   - La pestaña de Contenidos muestra el contenido actual de la política en formato JSON.
   - La pestaña de Objetivos muestra una lista de las nodos raíz, unidades organizativas y cuentas a los que la política está adjunta.
   - La pestaña Etiquetas muestra las etiquetas adjuntas a la política. Nota: la pestaña Etiquetas no está disponible para AWS políticas administradas.

   Para editar la política, elija Edit policy (Editar política). Dado que cada tipo de política tiene requisitos de edición diferentes, consulte las instrucciones para crear y actualizar políticas de su tipo de política 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}"
    }
}
```

- SDK de AWS: DescribePolicy

Administrador delegado para AWS Organizations

Le recomendamos que utilice la cuenta de administración de AWS Organizations y sus usuarios y roles únicamente para las tareas que deba realizar dicha cuenta. También le recomendamos que almacene sus recursos de AWS en otras cuentas de miembros de la organización y los mantenga fuera de la cuenta de administración. Esto se debe a que las características de seguridad, como las políticas de control de servicios (SCP) de las organizaciones, no restringen ni los usuarios ni los roles de la cuenta de administración.

Desde la cuenta de administración de la organización, puede delegar la administración de políticas para las organizaciones en cuentas de miembro especificadas para realizar acciones de políticas que, de forma predeterminada, solo están disponibles para la cuenta de administración.

Creación o actualización de una política de delegación basada en recursos

Desde la cuenta de administración, cree o actualice una política de delegación basada en recursos para su organización y agregue una declaración que especifique qué cuenta miembro puede realizar acciones en las políticas. Puede agregar varias declaraciones en la política para denotar distintos conjuntos de permisos para las cuentas de los miembros.

> **Permisos mínimos**
>
> Para crear o actualizar una política de delegación basada en recursos, necesita permisos para ejecutar las siguientes acciones:

- `organizations:PutResourcePolicy`
- `organizations:DescribeResourcePolicy`

Además, debe conceder a los roles y usuarios de la cuenta de administrador delegado los permisos de IAM correspondientes a las acciones requeridas. Si no dispone de los permisos de IAM, se considera que la entidad de seguridad principal que realiza la llamada no dispone de los permisos necesarios para administrar las políticas deAWS Organizations.

AWS Management Console

Agregue declaraciones a la política de delegación basada en recursos en la AWS Management Console utilizando uno de los siguientes métodos:

- Política JSON: pegue y personalice un una política de delegación basada en recursos de ejemplo para usarlo en su cuenta, o escriba su propio documento de política de JSON en el editor de JSON.
- Editor visual: cree una nueva política de delegación en el editor visual, que le guiará en la creación de una política de delegación sin tener que escribir la sintaxis JSON.

Utilice el editor de políticas JSON para crear o actualizar una política de delegación

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Elija Settings.
3. En la sección Administrador delegado para AWS Organizations, elija Delegar para crear la política de delegación de las organizaciones. Para actualizar una política de delegación existente, seleccione Edit (Editar).
4. Escriba o pegue un documento de política de JSON. Para obtener más información sobre el lenguaje de la política de IAM, consulte Referencia de políticas JSON de IAM.
5. Resuelva cualquier advertencia de seguridad, error o advertencia general generada durante la validación de la política y, a continuación, elija Create policy (Crear política) para guardar su trabajo.

Utilice el editor visual para crear o actualizar una política de delegación

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Elija Settings.
3. En la sección Administrador delegado para AWS Organizations, elija Delegar para crear la política de delegación de las organizaciones. Para actualizar una política de delegación existente, seleccione Edit (Editar).
4. En la página Crear política de delegación, elija Add new statement (Agregar nueva declaración).
5. Establezca Effect (Efecto) en `Allow`.
6. Agregue `Principal` para definir las cuentas de miembros en las que desea delegar. Para obtener más detalles acerca de la sintaxis, consulte los Ejemplo de políticas de delegación basadas en recursos.
7. En la lista de Acciones, elija las acciones que quiera delegar. Puede utilizar Filtrar acciones para limitar las opciones.
8. Para especificar si la cuenta de miembro delegado puede adjuntar políticas a la raíz de la organización o a las unidades organizativas (OU), establezca `Resources`. También debe seleccionar `policy` como tipo de recurso. Para obtener más información, consulte los Ejemplo de políticas de delegación basadas en recursos. Puede especificar recursos de las siguientes maneras:

   - Seleccione Add a resource (Agregar un recurso) y cree el Nombre de recurso de Amazon (ARN) siguiendo las instrucciones del cuadro de diálogo.
   - Enumere manualmente los ARN de recursos en el editor. Para obtener más información acerca de la sintaxis de ARN, consulte Amazon Resource Names (ARN) (Nombre de recurso de Amazon (ARN)) en la Guía de referencia general de AWS. Para obtener información sobre el uso de ARN en el elemento resource de una política, consulte Elementos de política JSON de IAM: Resource.
9. Elija Add a condition (Agregar una condición) para especificar otras condiciones, incluido el tipo de política que desea delegar. Elija la Condition key (Clave de condición), Tag key (Clave de etiqueta) Qualifier (Calificador) y Operator (Operador) de la condición y, a continuación, escriba un **`Value`**. Para obtener más información, consulte Ejemplo de políticas de delegación basadas en recursos. Cuando haya terminado elija Add condition (Añadir

condición). Para obtener más información sobre el elemento Condición, consulte Elementos de política JSON de IAM: Condition.

10. Para añadir más bloques de permisos, elija Add new statement (Añadir nueva declaración). Para cada bloque, repita los pasos 5 a 9.
11. Resuelva cualquier advertencia de seguridad, error o advertencia general generada durante la validación de la política y, a continuación, elija Crear política para guardar su trabajo.

AWS CLI & AWS SDKs

Creación o actualización de una política de delegación

Puede utilizar el siguiente comando para crear o actualizar una política de delegación:

- AWS CLI: put-resource-policy

  En el siguiente ejemplo se crea o actualiza la política de delegación.

```
$ aws organizations put-resource-policy --content
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Fully_manage_backup_policies",
            "Effect": "Allow",
            "Principal": {
                "AWS": "135791357913"
            }
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:CreatePolicy",
                "organizations:DescribePolicy",
                "organizations:UpdatePolicy",
                "organizations:DeletePolicy",
                "organizations:AttachPolicy",
                "organizations:DetachPolicy"
            ],
            "Resource": [
                "arn:aws:organizations::246802468024:root/o-abcdef/r-pqrstu",
                "arn:aws:organizations::246802468024:ou/o-abcdef/*",
                "arn:aws:organizations::246802468024:account/o-abcdef/*",
```

```
                "arn:aws:organizations::246802468024:organization/policy/
backup_policy/*",
            ],
            "Condition": {
                "StringLikeIfExists": {
                    "organizations:PolicyType": [
                        "BACKUP_POLICY"
                    ]
                }
            }
        }
    ]
}
```

- AWS SDK: PutResourcePolicy

Acciones de política de delegación admitidas

Se admiten las siguientes acciones para políticas de delegación:

- `AttachPolicy`
- `CreatePolicy`
- `DeletePolicy`
- `DescribeAccount`
- `DescribeCreateAccountStatus`
- `DescribeEffectivePolicy`
- `DescribeHandshake`
- `DescribeOrganization`
- `DescribeOrganizationalUnit`
- `DescribePolicy`
- `DescribeResourcePolicy`
- `DetachPolicy`
- `DisablePolicyType`
- `EnablePolicyType`
- `ListAccounts`

- `ListAccountsForParent`
- `ListAWSServiceAccessForOrganization`
- `ListChildren`
- `ListCreateAccountStatus`
- `ListDelegatedAdministrators`
- `ListDelegatedServicesForAccount`
- `ListHandshakesForAccount`
- `ListHandshakesForOrganization`
- `ListOrganizationalUnitsForParent`
- `ListParents`
- `ListPolicies`
- `ListPoliciesForTarget`
- `ListRoots`
- `ListTagsForResource`
- `ListTargetsForPolicy`
- `TagResource`
- `UntagResource`
- `UpdatePolicy`

Ver una política de delegación basada en recursos

Desde la cuenta de administración, vea la política de delegación basada en recursos de su organización para saber qué administradores delegados tienen acceso a la administración de qué tipos de políticas.

> **Permisos mínimos**
>
> Para ver una política de delegación basada en recursos, necesita permisos para ejecutar la siguiente acción: `organizations:DescribeResourcePolicy`.

AWS Management Console

Para ver una política de delegación

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Elija Settings.
3. En la sección Administrador delegado para AWS Organizations, desplácese hacia abajo para ver la política de delegación completa.

AWS CLI & AWS SDKs

Visualización de una política de delegación

Puede utilizar el siguiente comando para ver una política de delegación:

- AWS CLI: describe-resource-policy

  En el siguiente ejemplo se recupera la política.

  ```
  $ aws organizations describe-resource-policy
  ```

- AWS SDK: DescribeResourcePolicy

Eliminar una política de delegación basada en recursos

Cuando ya no necesite delegar la administración de políticas en su organización, puede eliminar la política de delegación basada en recursos de la cuenta de administración de la organización.

> **Important**
>
> Si elimina la política de delegación basada en recursos, no podrá recuperarla.

> **Permisos mínimos**
>
> Para eliminar la política de delegación basada en recursos, necesita permisos para ejecutar la siguiente acción:`organizations:DeleteResourcePolicy`.

AWS Management Console

Para eliminar una política de delegación

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Elija Settings.
3. En la sección Administrador delegado para AWS Organizations, elija Eliminar.
4. En el cuadro de diálogo de confirmación Delete policy (Eliminar política), escriba **`delete`**. A continuación, elija Delete policy (Eliminar política).

AWS CLI & AWS SDKs

Eliminación de una política de delegación

Puede utilizar el siguiente comando para eliminar una política de delegación:

- AWS CLI: delete-resource-policy

  En el siguiente ejemplo se elimina la política especificada.

  ```
  $ aws organizations delete-resource-policy
  ```

- AWS SDK: DeleteResourcePolicy

Ejemplo de políticas de delegación basadas en recursos

Los siguientes ejemplos de código muestran cómo se pueden utilizar las políticas de delegación basadas en recursos.

Ejemplos

- Ejemplo: ver la organización, las unidades organizativas, las cuentas y las políticas
- Ejemplo: permisos consolidados para administrar las políticas de copia de seguridad de una organización

Ejemplo: ver la organización, las unidades organizativas, las cuentas y las políticas

Antes de delegar la administración de las políticas, debe delegar los permisos para navegar por la estructura de una organización y ver las unidades organizativas (OU), las cuentas y las políticas asociadas a ellas.

En este ejemplo se muestra cómo podría incluir estos permisos en su política de delegación basada en recursos para la cuenta de miembro, *AccountId*.

> **Important**
>
> Es aconsejable que incluya permisos solo para las acciones mínimas requeridas como se muestra en el ejemplo, aunque es posible delegar cualquier acción de solo lectura de Organizaciones utilizando esta política.

En este ejemplo de política de delegación se conceden los permisos necesarios para completar acciones mediante programación desde la API de AWS o la AWS CLI. Para utilizar esta política, sustituya el texto del marcador de posición de AWS para *AccountId* por su propia información. A continuación, siga las instrucciones indicadas en Administrador delegado para AWS Organizations.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
```

```
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}
```

Ejemplo: permisos consolidados para administrar las políticas de copia de seguridad de una organización

En este ejemplo se muestra cómo se puede crear una política de delegación basada en recursos que permita a la cuenta de administración delegar todos los permisos necesarios para administrar las políticas de copia de seguridad dentro de la organización, incluidas `create`, `read`, `update` y acciones `delete`, así como acciones de `attach` y `detach` política. Para comprender el significado de cada acción, recurso y condición, consulte Ejemplo de políticas de delegación basadas en recursos.

> **Important**
>
> Esta política permite que los administradores delegados realicen las acciones especificadas en las políticas creadas por cualquier cuenta de la organización, incluida la cuenta de administración.

En este ejemplo de política de delegación se conceden los permisos necesarios para completar acciones mediante programación desde la API de AWS o la AWS CLI. Para utilizar esta política de delegación, sustituya el texto del marcador de posición de AWS para *`MemberAccountId`*, *`ManagementAccountI`*d, *`OrganizationId`* y *`RootId`* por su propia información. A continuación, siga las instrucciones indicadas en Administrador delegado para AWS Organizations.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DelegatingNecessaryDescribeListActions",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribePolicy",
        "organizations:DescribeEffectivePolicy",
        "organizations:ListRoots",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListParents",
        "organizations:ListChildren",
        "organizations:ListAccounts",
        "organizations:ListAccountsForParent",
        "organizations:ListPolicies",
        "organizations:ListPoliciesForTarget",
        "organizations:ListTargetsForPolicy",
        "organizations:ListTagsForResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringLikeIfExists": {
          "organizations:PolicyType": "BACKUP_POLICY"
        }
      }
    },
    {
      "Sid": "DelegatingAllActionsForBackupPolicies",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::MemberAccountId:root"
      },
      "Action": [
        "organizations:CreatePolicy",
        "organizations:UpdatePolicy",
        "organizations:DeletePolicy",
```

```
        "organizations:AttachPolicy",
        "organizations:DetachPolicy",
        "organizations:EnablePolicyType",
        "organizations:DisablePolicyType"
      ],
      "Resource": [
        "arn:aws:organizations::ManagementAccountId:root/o-OrganizationId/r-RootId",
        "arn:aws:organizations::ManagementAccountId:ou/o-OrganizationId/*",
        "arn:aws:organizations::ManagementAccountId:account/o-OrganizationId/*",
        "arn:aws:organizations::ManagementAccountId:policy/o-OrganizationId/
backup_policy/*"
      ]
    }
  ]
}
```

Políticas de administración

Las políticas de administración le permiten configurar y administrar de forma centralizada los servicios de AWS y sus características. Cómo afectan las políticas a las unidades organizativas y a las cuentas que las heredan depende del tipo de política de administración que aplica en AWS Organizations. Revise los temas en esta sección para comprender los términos y conceptos pertinentes sobre las políticas de administración.

Temas

- Descripción de la herencia de políticas de administración
- Políticas de exclusión de servicios de IA
- Políticas de copia de seguridad
- Políticas de etiquetas

Descripción de la herencia de políticas de administración

> **Note**
>
> La información de esta sección no se aplica a las SCP porque estas gestionan tanto la autorización como la denegación de las acciones de IAM. Si bien las SCP están asociados a la raíz, a las unidades organizativas y a las cuentas, es necesario incluir una declaración `allow` explícita en las SCP en todos los niveles, desde la raíz hasta cada

unidad organizativa en la ruta directa a la cuenta (incluida la propia cuenta de destino). Para obtener más información acerca de cómo las SCP se comportan en una jerarquía de AWS Organizations, consulte Evaluación de SCP.

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

- Cuando se asocia una política de administración a la raíz de la organización, todas las unidades organizativas y cuentas de la organización heredan esa política.
- Cuando asocia una política de administración 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 de administración a una cuenta específica, solo afecta a esa cuenta.

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

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

Temas

- Terminología de herencia
- Sintaxis de política y herencia para tipos de políticas de administración
- Operadores de herencia
- Ejemplos de herencia

Terminología de herencia

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

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 de administración 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 de administración heredan esa política.

Por ejemplo, cuando se asocian las políticas de administración 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 de administración 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.

Operadores de herencia

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. Para obtener más información, consulte Operadores de herencia.

Sintaxis de política y herencia para tipos de políticas de administración

Cómo afectan las políticas exactamente a las unidades organizativas y a las cuentas que las heredan depende del tipo de política de administración que selecciona: Los tipos de políticas de administración incluyen:

- Políticas de exclusión de servicios de inteligencia artificial (IA)
- Políticas de copia de seguridad
- Políticas de etiquetas

La sintaxis de estos tipos de política de administración incluye Operadores de herencia, que permiten especificar con precisión qué elementos de las políticas principales se aplican y qué elementos pueden invalidar o modificar cuando 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 de reglas final 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.

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` – Sobreescribe cualquier configuración de política 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` – Agrega la configuración especificada (sin quitar ninguna) 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` – Elimina las configuraciones heredadas especificadas de la política efectiva, si existen. 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.

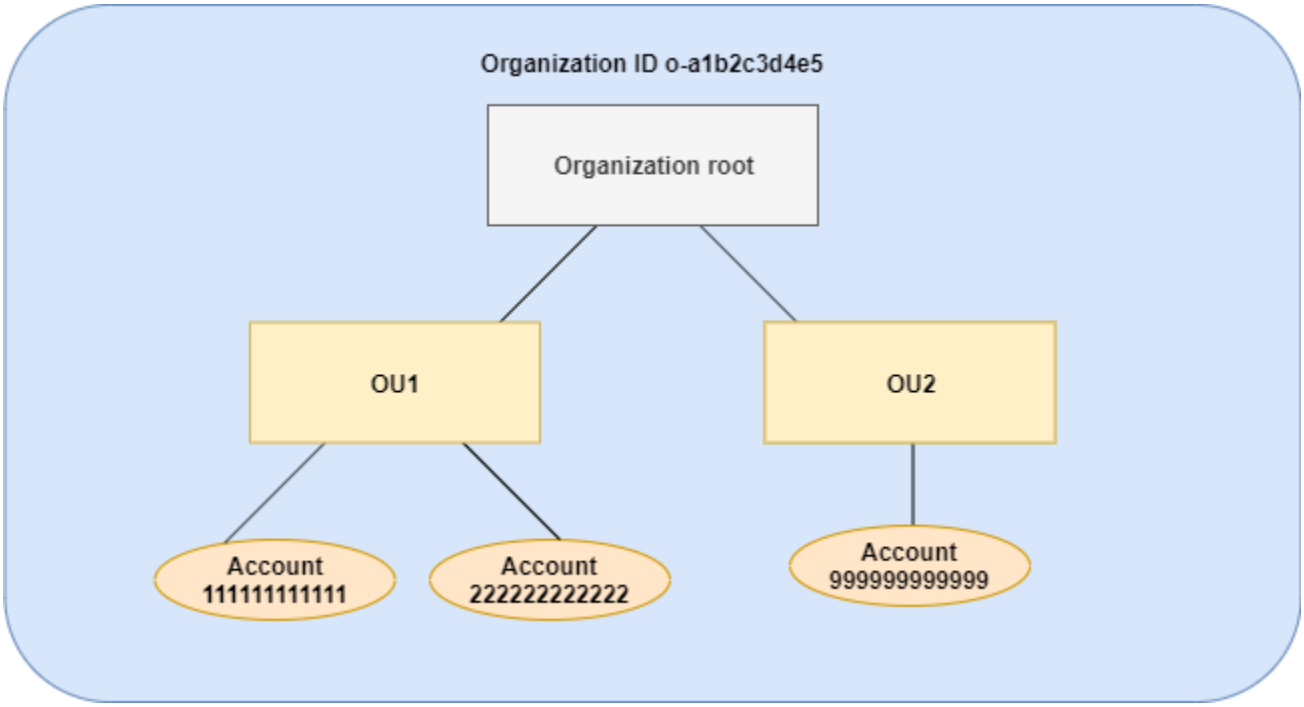
- `"@@operators_allowed_for_child_policies":["@@assign", "@@append", "@@remove"]` - Las unidades organizativas secundarias y las cuentas solo pueden utilizar los operadores especificados en las políticas secundarias. Puede especificar uno o más operadores de configuración de valores en este operador de control secundario.
- `"@@operators_allowed_for_child_policies":["@@none"]` — Las unidades organizativas secundarias y las cuentas no pueden utilizar operadores en las políticas. 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

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 sobrescriban solo valores de etiquetas
- Ejemplo 2: Agregar nuevos valores a las etiquetas heredadas
- Ejemplo 3: Eliminar los valores de etiquetas heredadas
- Ejemplo 4: Restringir los cambios en las políticas secundarias
- Ejemplo 5: Conflictos con los operadores de control secundarios
- Ejemplo 6: Conflictos al anexar valores en el mismo nivel de jerarquía

Ejemplo 1: Permitir que las políticas secundarias sobrescriban solo valores 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.

Política A: política 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.

Política 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 etiqueta `CostCenter` debe 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 política efectiva mostrada como contenido de una nueva política. La sintaxis no incluye los operadores necesarios para controlar la fusión con otras políticas secundarias y primarias. La presentación de una política eficaz solo 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.

Política A: política 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`.

Política 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 etiqueta `CostCenter` se debe utilizar como valor de etiquetas especificado en todos los recursos de Amazon Redshift y 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 política efectiva mostrada como contenido de una nueva política. La sintaxis no incluye los operadores necesarios para controlar la fusión con otras políticas secundarias y primarias. La presentación de una política eficaz solo 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: Eliminar los 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.

Política A: política 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.

Política D: política de etiqueta de la cuenta 999999999999 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 política efectiva mostrada como contenido de una nueva política. La sintaxis no incluye los operadores necesarios para controlar la fusión con otras políticas secundarias y primarias. La presentación de una política eficaz solo 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 secundarias

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.

Política E: política de etiqueta raíz de la organización para restringir los cambios en las políticas 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.

Política F: política 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 política efectiva mostrada como contenido de una nueva política. La sintaxis no incluye los operadores necesarios para controlar la fusión con otras políticas secundarias y primarias. La presentación de una política eficaz solo 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.

Política G: política de etiqueta raíz de la organización 1

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

```
        }
    }
}
```

Política H: política de etiqueta raíz de la organización 2

```
{
    "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 al anexar valores 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.

Política J: primera política de etiquetas adjunta al nodo raíz de la organización

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

```
            },
            "tag_value": {
                "@@append": ["Maintenance"]
            }
        }
    }
}
```

Política K: segunda política de etiquetas adjunta al nodo 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 política efectiva mostrada como contenido de una nueva política. La sintaxis no incluye los operadores necesarios para controlar la fusión con otras políticas secundarias y primarias. La presentación de una política eficaz solo tiene por objeto comprender los resultados de la fusión.

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

```
            ]
        }
    }
}
```

Políticas de exclusión de servicios de IA

Los servicios de inteligencia artificial (IA) de AWS, tales como Amazon Rekognition, Amazon CodeWhisperer, Amazon Transcribe y Contact Lens for Amazon Connect, pueden almacenar y utilizar contenido de clientes procesado por dichos servicios para el desarrollo y la mejora continua de otros servicios de AWS. Como cliente AWS, puede optar por no tener su contenido almacenado o utilizado para mejorar el servicio.

> **Note**
>
> Es posible que los servicios de inteligencia artificial (IA) de AWS necesiten almacenar su contenido para proporcionar los servicios, incluso si opta por no permitir que AWS utilice sus datos para mejorar el servicio. Para obtener más información, consulte la documentación del servicios de IA que utilice.

En lugar de configurar esta configuración individualmente para cada Cuenta de AWS que utiliza su organización, puede configurar una política 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 un Región de AWS se replica a todas las demás regiones.
> - Cuando se opta por no utilizar el contenido por parte de un servicio de IA AWS, ese servicio elimina todo el contenido histórico asociado que se compartió con AWS antes de establecer la opción. Esta eliminación debe limitarse a los datos almacenados que no son necesarios para proporcionar funciones de servicio.

Introducción a las políticas de exclusión de servicios de IA

Siga estos pasos para empezar a utilizar las políticas de exclusión de servicios de Inteligencia Artificial (IA).

1. Habilitar políticas de exclusión de servicios de IA para su organización.
2. Crear una política de exclusión de servicios de IA.
3. Asocie la política de exclusión de servicios de IA al nodo raíz, unidad organizativa o cuenta de su organización.
4. Vea la política de exclusión de servicios de IA en vigor combinada que se aplica a una cuenta.

Para todos estos pasos, debe iniciar sesión como usuario de AWS Identity and Access Management (IAM), asumir un rol de IAM o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

Información adicional

- Conozca la sintaxis de políticas para las políticas de exclusión de servicios de IA y vea ejemplos de políticas

Crear, actualizar y eliminar políticas de exclusión de servicios de IA

En este tema:

- Después de habilitar las políticas de exclusión de IA de su organización, puede crear una política.
- Cuando cambien sus requisitos de exclusión, puede actualizar una política existente.
- Cuando ya no necesite una política y después de desconectarla de todas las unidades organizativas (OU) y cuentas, puede eliminarla.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de exclusión de servicios de IA, seleccione Create policy (Crear política).
3. En la página Crear nueva política de exclusión de servicios de IA, introduzca un Nombre de política y una Descripción opcional para la política.
4. (Opcional) Puede agregar una o varias etiquetas a la política seleccionando Agregar etiqueta y a 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 .
5. Ingrese o pegue el texto de la política en la pestaña JSON. Para obtener información acerca de la sintaxis de política de exclusión de servicios de IA, consulte Sintaxis y ejemplos de políticas de exclusión de servicios de IA. Para ver las políticas de ejemplo que puede utilizar como punto de partida, consulte Ejemplos de políticas de exclusión de servicios de IA.
6. Cuando haya terminado de editar la política, elija Crear política en 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 minúsculas.

```
{
    "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 nueva política 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"
        }
    }
}
```

- SDK de AWS: CreatePolicy

Qué hacer a continuación

Cuando haya creado una política de exclusión de los servicios de IA, puede poner en práctica sus opciones de exclusión. Para ello, puede asociar la política al nodo raíz de la organización, las unidades organizativas (OU), Cuentas de AWS de la organización o una combinación de todo ello.

Actualización de una política de exclusión de servicios de IA

> **Permisos mínimos**
>
> Para actualizar una política de exclusión 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 elemento `Resource` en la misma instrucción 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de exclusión de servicios de IA, elija el nombre de la política que desea actualizar.
3. En la página de detalles de la política, elija Editar política.
4. Puede introducir un nuevo Nombre de la política, Descripción de la política o editar el texto de la política JSON. Para obtener información acerca de la sintaxis de política de exclusión de servicios de IA, consulte Sintaxis y ejemplos de políticas de exclusión de servicios de IA. Para ver las políticas de ejemplo que puede utilizar como punto de partida, consulte Ejemplos de políticas de exclusión de servicios de IA.
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 ejemplo siguiente se cambia el documento de política JSON adjunto a una política de exclusión de servicio de IA. En este ejemplo, el contenido se toma de un archivo llamado `policy.json` con el siguiente texto:

```
{
    "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"}
}
```

- SDK de AWS: UpdatePolicy

Edición de etiquetas adjuntas a una política de exclusión de servicios de IA

Cuando inicie sesión en la cuenta de administración de su organización, puede agregar o quitar las etiquetas adjuntas a una política de exclusión de servicios de IA. Para obtener más información acerca del etiquetado, consulte Etiquetado de recursos de AWS Organizations.

Permisos mínimos

Para editar las etiquetas asociadas a una política de exclusión de servicios de IA en su organización de AWS, 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 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración 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 elegida de la política, elija la opción Etiquetas y, a continuación, elija Administrar 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 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 eligiendo Eliminar.
   - Agregue una nueva clave de etiqueta y valore el par. Seleccione Agregar etiqueta y, a continuación, introduzca el nuevo nombre de clave y el valor opcional en los cuadros proporcionados. Si deja el Valor en blanco, el valor es una cadena vacía; no es `null`.
5. Seleccione Guardar los cambios después 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 siguientes comandos para editar las etiquetas asociadas a una política de exclusión de servicios de IA:

- AWS CLI: tag-resource y untag-resource
- SDK de AWS:TagResource y UntagResource

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 desconectarla de todas las entidades asociadas.

Permisos mínimos

Para eliminar una política, debe tener permiso para ejecutar la siguiente acción:

- `organizations:DescribePolicy` (solo consola: para navegar a la política)
- `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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de exclusión de servicios de IA, elija el nombre de la política que desea eliminar.
3. Primero debe desconectar la política que desea eliminar de todos los nodos raíz, unidades organizativas y cuentas. Elija el icono Implementación, elija el botón de opción situado junto a cada nodo raíz, OU o cuenta que se muestra en la lista Implementación y, a continuación, elija Desconectar. En el cuadro de diálogo de confirmación, elija Desconectar. Repita hasta que elimine todos los destinos.
4. En la parte superior de la página, elija Eliminar.
5. En el cuadro de diálogo de confirmación, escriba el nombre de la política y, a continuación, elija Eliminar.

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. Solo funciona si la política no está asociada a ningún nodo raíz, unidad organizativa o cuenta.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- SDK de AWS: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:

- Cuando asocia una política de exclusión de servicios de IA al nodo raíz de su organización, la política se aplica a todas las cuentas y unidades organizativas de los miembros del nodo raíz.
- Cuando asocia una política de exclusión de servicios de IA a una unidad organizativa, esa política se aplica a las cuentas que pertenecen a la OU o a cualquiera de sus OU secundarias. Esas cuentas también están sujetas a cualquier política de copia de seguridad asociada a la raíz de la organización.
- Cuando asocia una política de exclusión de servicios de IA a una cuenta, esa política se aplica únicamente 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 OU raíz y principales, así como de cualquier política directamente asociada a la cuenta, es la política en vigor. Para obtener información sobre cómo se fusionan las políticas con la política en vigor, consulte Descripción de la herencia de políticas de administración.

> **Permisos mínimos**
>
> Para asociar una política de exclusión de IA, debe tener permiso para ejecutar la siguiente acción:
>
> - `organizations:AttachPolicy`

AWS Management Console

Puede asociar una política de exclusión de servicios de IA navegando hasta la política o el nodo raíz, unidad organizativa o cuenta a la que desee adjuntar la política.

Para asociar una política de exclusión de servicios de IA navegando hasta el nodo raíz, unidad organizativa o cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, busque y seleccione el nombre del nodo 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.
3. En la pestaña Políticas, en la entrada de Políticas de exclusión de servicios de IA, elija Adjuntar.
4. Busque la política que desea y elija Asociar política.

   La lista de políticas de exclusión de los servicios de IA adjuntas en la pestaña Políticas se actualiza para incluir la nueva adición. El cambio en la política surtirá efecto de inmediato.

Para adjuntar una política de exclusión de servicios de IA navegando hasta la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de exclusión de servicios de IA, elija el nombre de la política que desea adjuntar.
3. En la pestaña Objetivos, seleccione Adjuntar.
4. Elija el botón de opción situado junto al nodo 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 Asociar política.

   La lista de políticas de exclusión de los servicios de IA adjuntas en la pestaña Objetivos se actualiza para incluir la nueva adición. El cambio en la política surtirá efecto de inmediato.

AWS CLI & AWS SDKs

Para asociar una política de exclusión de servicios de IA al nodo raíz de la organización, la unidad organizativa o la cuenta

Puede utilizar uno de los siguientes elementos para asociar una política de exclusión de servicios de IA:

- AWS CLI: attach-policy

  En el siguiente ejemplo se adjunta una política a una OU.

  ```
  $ aws organizations attach-policy \
      --target-id ou-a1b2-f6g7h222 \
      --policy-id p-i9j8k7l6m5
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- SDK de AWS:AttachPolicy

El cambio en la 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 desconectar una política de exclusión de servicios de IA del nodo raíz de la organización, unidad organizativa o cuenta a la que está asociada. Después de desconectar 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 desconectada. Para desasociar una política, siga los pasos que se describen a continuación.

Permisos mínimos

Para desconectar una política de exclusión de servicios de IA del nodo raíz de una organización, unidad organizativa o cuenta, debe tener permiso para ejecutar la siguiente acción:

- `organizations:DetachPolicy`

AWS Management Console

Puede desconectar una política de exclusión de servicios de IA navegando hasta la política o el nodo raíz, unidad organizativa o cuenta de la que desee desconectar la política.

Para desconectar una política de exclusión de servicios de IA navegando hasta el nodo raíz, unidad organizativa o cuenta a la que está adjunta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS desplácese hasta el nodo raíz, unidad organizativa o cuenta de la que desea desconectar 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 del nodo raíz, unidad organizativa o cuenta.
3. En la página Políticas, elija el botón de opción situado junto a la política de exclusión de servicios de IA que desea desconectar y, a continuación, elija Desconectar.
4. En el cuadro de diálogo de confirmación, elija Desconectar política.

   Se actualiza la lista de políticas de exclusión de servicios de IA adjuntas. El cambio en la política surtirá efecto de inmediato.

Para separar una política de exclusión de servicios de IA navegando a la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de exclusión de servicios de IA, elija el nombre de la política que desea desconectar de un nodo raíz, unidad organizativa o cuenta.
3. En la pestaña de Objetivos, elija el botón de opción situado junto al nodo raíz, unidad organizativa o cuenta de la que desea desconectar 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, elija Desconectar.

   Se actualiza la lista de políticas de exclusión de servicios de IA adjuntas. El cambio en la política surtirá efecto de inmediato.

AWS CLI & AWS SDKs

Para desconectar una política de exclusión de servicios de IA del nodo raíz de la organización, la unidad organizativa o la cuenta

Puede utilizar uno de los comandos siguientes para desconectar una política de exclusión de servicios desconectar IA:

- AWS CLI:detach-policy

  En el ejemplo siguiente se desconecta una política de una unidad organizativa.

  ```
  $ aws organizations detach-policy \
      --target-id ou-a1b2-f6g7h222 \
      --policy-id p-i9j8k7l6m5
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- SDK de AWS:DetachPolicy

El cambio en la política surtirá efecto de inmediato.

Visualización de políticas efectivas de exclusión de servicios de IA

Determine la política de exclusión de servicios de Inteligencia artificial (IA) en vigor de una cuenta en su organización.

¿Cuál es la política de exclusión de los servicios de IA en vigor?

La política de exclusión efectiva de servicios de IA especifica las reglas finales que se aplican a un Cuenta de AWS. Es la agregación de cualquier política de exclusión de servicios de IA que hereda la cuenta, además de cualquier política de exclusión de servicios de IA asociada directamente a la cuenta. Cuando se asocia una política de exclusión de servicios de IA al nodo 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 OU. Cuando se asocia una política directamente a una cuenta, solo se aplica a esa Cuenta de AWS.

Por ejemplo, la política de exclusión de los servicios de IA adjunta al nodo raíz de la organización podría especificar que todas las cuentas de la organización se excluyan del uso de contenidos por parte de todos los servicios de aprendizaje automático AWS. Una política de exclusión de servicios de IA independiente 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 todos los servicios AWS, 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, consulte Descripción de la herencia de políticas de administración.

¿Cómo ver la política de exclusión de los servicios de IA en vigor?

Puede ver la política de exclusión de servicios de IA 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 exclusión de servicios de IA 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 de exclusión de servicios de IA en vigor de una cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, elija el nombre de la cuenta para la que desea ver la política 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 pestaña Políticas, en la sección Políticas de exclusión de servicios de IA, elija Ver la política de IA efectiva para este Cuenta de AWS.

   La consola muestra la política 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. Todos los documentos de la política de exclusión de servicios de IA deben incluir los operadores de herencia que especifican cómo se fusiona cada configuración en la política en vigor final.

AWS CLI & AWS SDKs

Para ver la política de exclusión de servicios de IA en vigor de una cuenta

Puede utilizar una de las siguientes opciones para ver la política de exclusión de servicios de IA en vigor:

- 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"
    }
}
```

- SDK de AWS: 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 (IA) 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 que se estructura de acuerdo con las reglas de JSON. La sintaxis de las políticas de exclusión de servicios de IA sigue la sintaxis de los tipos de políticas de administración. Para obtener una explicación completa de esa sintaxis, consulte Descripción de la herencia de políticas de administración. Este tema se centra en aplicar esa sintaxis general a los requisitos específicos del tipo de política de exclusión de servicios de IA.

> **Important**
>
> En esta sección son importantes las mayúsculas de los valores. Introduzca los valores con letras mayúsculas y minúsculas como se muestra en este tema. Las políticas no funcionan si utiliza mayúsculas inesperadas.

La siguiente política muestra la sintaxis básica de política de exclusión de servicios de IA. Si este ejemplo se asociara directamente a una cuenta, esa cuenta se excluiría explícitamente de un servicio y se optaría por otra. Otras políticas heredadas de niveles superiores (OU o políticas raíz) podrían optar por o excluir otros servicios.

```
{
    "services": {
        "rekognition": {
            "opt_out_policy": {
                "@@assign": "optOut"
            }
        },
        "lex": {
            "opt_out_policy": {
                "@@assign": "optIn"
            }
```

```
        }
    }
}
```

Imagine la siguiente política de ejemplo asociada al nodo raíz de la organización. Establece el valor predeterminado para que la organización opte por la exclusión de todos los servicios de IA. Esto incluye automáticamente todos los servicios de IA que no estén explícitamente exentos de otra manera, incluidos los servicios de IA que AWS podría implementar 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 reemplace. 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 política permite que las política 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:

- El elemento `services`. 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 el elemento `services`. Cada sentencia contiene los siguientes elementos:

- Una clave de nombre de servicio que identifica un servicio de IA AWS. Los siguientes nombres clave son valores válidos para este campo:
  - **`default`**: representa todos los servicios de IA que actualmente están disponibles e incluye implícita y automáticamente cualquier servicio de IA que se pueda agregar en el futuro.
  - `awssupplychain`
  - `chimesdkvoiceanalytics`
  - `cloudwatch`
  - `codeguruprofiler`
  - `codewhisperer`
  - `comprehend`
  - `connectamd`
  - `connectoptimization`
  - `contactlens`
  - `datazone`
  - `frauddetector`
  - `guardduty`
  - `lex`
  - `polly`
  - `q`
  - `quicksightq`
  - `rekognition`
  - `securitylake`
  - `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.

  El `opt_out_policy` clave puede contener solo el operador `@@assign` 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.

  > **Notas**
  >
  > - No puede usar la opción `@@append` y operadores `@@remove` de herencia en las políticas de exclusión de servicios de IA.
  > - No puede usar los operadores `@@enforced_for` de herencia 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 políticas secundarias pueden hacer para anular la configuración impuesta por las políticas principales. Puede especificar uno de los siguientes valores:

  - `@@assign`: las políticas secundarias de esta política pueden utilizar el operador `@@assign` para anular el valor heredado con un valor diferente.
  - `@@none`: las políticas secundarias de esta política no pueden cambiar el valor.

  El comportamiento del `@@operators_allowed_for_child_policies` depende de dónde lo coloque. Puede usar las siguientes ubicaciones:

  - En la clave `services`: controla si una política secundaria puede agregar o cambiar la lista de servicios de la política efectiva.
  - En la clave para un servicio de IA específico o en la clave `default`: controla si una política secundaria puede agregar o cambiar la lista de claves bajo esta entrada específica.
  - En la clave `opt_out_policies` para un servicio específico: controla si una política secundaria puede cambiar solo 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: Excluir todos los servicios de IA para todas las cuentas de la organización

En el siguiente ejemplo se muestra una política que puede adjuntar al nodo raíz de su organización para excluir 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 política 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 políticas secundarias agreguen secciones nuevas que no sean `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 la configuración `optOut` o que agreguen cualquier configuración adicional.

Ejemplo 2: Establecer una configuración predeterminada de la organización para todos los servicios, pero permitir que las políticas secundarias anulen la configuración de los servicios individuales

En el siguiente ejemplo de política se establece un valor predeterminado para toda la organización para todos los servicios de IA. El valor para `default` impide que una política secundaria cambie el valor `optOut` para el servicio `default`, el marcador de posición para todos los servicios de IA. Si esta política se aplica como política principal adjuntándola al nodo raíz o a una unidad organizativa, las políticas secundarias pueden cambiar la configuración de exclusión de servicios individuales, como se muestra en la segunda política.

- Porque no hay `"@@operators_allowed_for_child_policies": ["@@none"]` en la clave `services`, las políticas secundarias pueden agregar nuevas secciones para servicios individuales.
- El `"@@operators_allowed_for_child_policies": ["@@none"]` que está en `default` impide que las políticas secundarias agreguen secciones nuevas que no sean `opt_out_policy` que ya está allí.
- El `"@@operators_allowed_for_child_policies": ["@@none"]` que está en `opt_out_policy` evita que las políticas secundarias cambien el valor de la configuración `optOut` o que agreguen cualquier configuración adicional.

Política principal de exclusión de servicios de IA de usuario 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 política de ejemplo se supone que la política del ejemplo anterior está asociada al nodo raíz de la organización o a una unidad organizativa principal y que se adjunta este ejemplo a una cuenta afectada por la política principal. Anula la configuración predeterminada de exclusión y opta explícitamente solo por el servicio Amazon Lex.

Política secundaria de exclusión 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 todos los demás servicios de IA AWS debido a la configuración heredada `default` de exclusión de la política 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 una configuración `optOut` para un único servicio de IA. Si esta política está adjunta al nodo raíz de la organización, impide que cualquier política secundaria anule la configuración `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

AWS Backup le permite crear planes de copias de seguridad que definen cómo realizar copias de seguridad de sus recursos de 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, Región de AWS que contiene los recursos para realizar la copia de seguridad y el almacén en el que se va a almacenar 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 un rol de AWS Identity and Access Management (IAM) que conceda permiso a AWS Backup para 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 el nodo raíz, las unidades organizativas (OU) y las cuentas individuales. Organizations aplica reglas de herencia para combinar las políticas del nodo 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 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 al nodo 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 adjuntar estas políticas a diferentes partes del árbol de la organización, como el nodo raíz o una unidad organizativa principal, con la intención de que las unidades organizativas y cuentas de nivel inferior hereden esas políticas parciales. Cuando Organizations combina 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 Backup considera 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 de una cuenta está incompleta, se producirán errores o habrá 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.

El plan de copia de seguridad en vigor para cada Cuenta de AWS de la organización aparece en la consola de AWS Backup como 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 a servicios de confianza con AWS 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, consulte Cómo habilitar la administración entre cuentas en la Guía para desarrolladores AWS Backup.

Introducción a las políticas de copia de seguridad

Siga estos pasos para empezar a utilizar las políticas de copia de seguridad.

1. Obtenga información sobre los permisos que debe tener para realizar tareas de políticas de copia de seguridad
2. Obtenga más información sobre algunas prácticas que recomendamos al utilizar políticas de copia de seguridad.
3. Habilite políticas de copia de seguridad para su organización.
4. Crear una política de copias de seguridad.
5. Asocie la política de copia de seguridad a la raíz, unidad organizativa o cuenta de su organización.
6. Vea la política de copia de seguridad en vigor combinada que se aplica a una cuenta.

Para todos estos pasos, debe iniciar sesión como usuario de IAM, asumir un rol de IAM o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

Información adicional

- Aprenda la sintaxis de las políticas de copia de seguridad y vea ejemplos de políticas

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 en AWS Organizations.

Temas

- Requisitos previos para administrar políticas de copia de seguridad
- Permisos para administrar políticas de copia de seguridad

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.
- Debe haber iniciado sesión en la cuenta de administración de su organización.
- Su usuario o rol de AWS Identity and Access Management (IAM) debe tener 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 sobre las políticas y permisos de IAM, consulte la Guía del usuario de IAM.

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 valores

de políticas predeterminados 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.

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 o mediante la operación de la API GetEffectivePolicy o una de sus variantes de AWS SDK o AWS CLI. 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 abordaje 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 y cuentas de la organización

Para mejorar su posición de recuperación de 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. Use la sección `copy_actions` de la política 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 la variable `$account` cuando especifique el ARN del almacén de copia de seguridad en el que se almacenará la copia de la copia de seguridad. La variable `$account` se reemplaza automáticamente en tiempo de ejecución con el ID de cuenta en el que se está ejecutando la política 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. Use la sección `copy_actions` de la política 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 usando el número de ID real de la cuenta cuando especifique el ARN del almacén de copia de seguridad en el que se almacenará 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 abordaje ayuda a mantener los problemas con un plan aislados en una política y evita que esos problemas compliquen la resolución de problemas con otras políticas y sus planes.

Utilice stack sets para crear los almacenes de copias de seguridad y los roles de IAM necesarios

Utilice la integración de los stack sets de AWS CloudFormation con Organizations para crear automáticamente los almacenes de copias de seguridad y los roles de AWS Identity and Access Management (IAM) necesarios 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 todas las Cuenta de AWS de su organización. Este abordaje le permite ejecutar sus planes de copia de seguridad con la seguridad de que las dependencias ya se cumplen. Para obtener más información, consulte Crear un Stack Set con permisos autoadministrados en la Guía del usuario AWS CloudFormation.

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 que AWS Backup interprete sus políticas e implemente los planes de copias de seguridad de la manera que pretendía.

Crear, actualizar y eliminar políticas de copia de seguridad

En este tema:

- Después de habilitar las políticas de copia de seguridad de su organización, puede crear una política.
- Cuando cambien sus requisitos de copia de seguridad, puede actualizar una política existente.

- Cuando ya no necesite una política y después de desconectarla de todas las unidades organizativas (OU) y cuentas, puede eliminarla.

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 solo el operador de configuración de valores @@assign y no proporciona ningún acceso a los operadores de control secundarios. Solo puede agregar los operadores de control infantil 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Backup policies (Políticas de copia de seguridad), seleccione Create policy (Crear política).

3. En la página Create policy (Crear política), introduzca un Policy name (Nombre de política) y una Description (Descripción) opcional para la política.
4. (Opcional) Puede agregar una o varias etiquetas a la política seleccionando Agregar etiqueta y a 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.
5. Puede crear la política mediante el Visual editor (Editor visual) como se describe en este procedimiento. También puede ingresar o pegar texto de política en la pestaña JSON. Para obtener información acerca de la sintaxis de las políticas de copia de seguridad, consulte Ejemplos y sintaxis de políticas de copia de seguridad.

   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 acerca de estos elementos del plan de copia de seguridad, consulte Crear un plan de copia de seguridad y Asignar recursos en la Guía del desarrollador AWS Backup.

   a. Detalles generales del plan de copia de seguridad
      - El nombre del plan de copia de seguridad puede 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 las Regiones de AWS seleccionadas.

   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) Una o varias reglas Copy to region (Copiar en región) para copiar también las copias de seguridad en almacenes de otras 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.

Seleccionar Agregar regla para agregar cada regla que necesite al plan.

Para obtener más información sobre las reglas de copia de seguridad, consulte las Reglas de copia de seguridad en la Guía para desarrolladores AWS Backup.

c. Una asignación de recursos que especifica los recursos de los que AWS Backup debe realizar una copia de seguridad con este plan. La asignación se realiza especificando pares de etiquetas que AWS Backup utiliza para buscar y hacer coincidir recursos

- El nombre de la asignación de recursos puede constar únicamente de caracteres alfanuméricos, guiones y guiones bajos.
- Especifique el rol de IAM que AWS Backup utilizará para 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` o `service-role`, y se separan 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**
  >
  > El rol de IAM especificado 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 más Clave de etiqueta de recursos y Valores de etiquetas para identificar los recursos de los que desea realizar una copia de seguridad. Si hay más de un valor de etiqueta, sepárelos con comas.

Seleccionar Agregar una asignación para agregar cada asignación de recursos configurada al plan de copia de seguridad.

Para obtener más información, consulte Asignar recursos a un plan de copia de seguridad en la Guía para desarrolladores AWS Backup.

6. Cuando haya terminado de crear la política, elija Create policy (Crear 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, consulte Ejemplos y sintaxis de políticas de copia de seguridad.

```
{
    "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 que la copia de seguridad AWS debe realizar resguardar todos los recursos de Cuentas de AWS afectados que se encuentran en las Regiones de AWS especificadas y que tienen la etiqueta `dataType` con un valor de `PII`.

A continuación, importe el archivo de política JSON del plan de copia de seguridad 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...",
    }
}
```

- SDK de AWS: CreatePolicy

Qué hacer a continuación

Cuando haya creado una política de copia de seguridad, puede hacerla efectiva. Para ello, puede adjuntar la política al nodo raíz de la organización, las unidades organizativas (OU), las Cuentas de AWS de la organización o una combinación de todo ello.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Backup policies (Políticas de copia de seguridad), elija el nombre de la política que desea actualizar.
3. Elija Edit policy (Editar política).

4. Puede introducir un nuevo Nombre de la política, Descripción de la política. Puede cambiar el contenido de la política mediante el Visual editor (Editor visual) o editando directamente el JSON.
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 comandos siguientes para actualizar una política de copia de seguridad:

- AWS CLI: update-policy

  En el siguiente ejemplo se 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 política JSON adjunto a una política de copia de seguridad. En este ejemplo, el contenido se toma de un archivo llamado `policy.json` con el siguiente texto:

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

- SDK de AWS: UpdatePolicy

Edición de etiquetas adjuntas a una política de copia de seguridad

Cuando inicie sesión en la cuenta de administración de su organización, puede agregar o eliminar las etiquetas asociadas a una política de copia de seguridad. Para obtener más información acerca del etiquetado, consulte Etiquetado de recursos de AWS Organizations.

Permisos mínimos

Para editar las etiquetas adjuntas a una política de copia de seguridad en su organización AWS, debe contar con los siguientes permisos:

- `organizations:DescribeOrganization` (solo consola: para navegar a la política)
- `organizations:DescribePolicy` (solo consola: para navegar a la política)
- `organizations:TagResource`
- `organizations:UntagResource`

AWS Management Console

Para editar las etiquetas adjuntas a una política de copia de seguridad

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Página de Políticas de copia de seguridad
3. Elija el nombre de la política que tenga las etiquetas que quiere modificar.

   Aparece la página de detalles de la 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 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 eligiendo Eliminar.
   - Agregue una nueva clave de etiqueta y valore el par. Seleccione Agregar etiqueta y, a continuación, introduzca el nuevo nombre de clave y el valor opcional en los cuadros proporcionados. Si deja el Valor en blanco, el valor es una cadena vacía; no es `null`.
6. Seleccione Guardar los cambios después 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 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-resource y untag-resource
- SDK de AWS:TagResource y UntagResource

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 desconectarla 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Tag policies (Políticas de copia de seguridad), elija el nombre de la política de copia de seguridad que desea eliminar.
3. Primero debe desconectar la política de copia de seguridad que desea eliminar de todos los nodos raíz, unidades organizativas y cuentas. Elija el icono Implementación, elija el botón de opción situado junto a cada nodo raíz, OU o cuenta que se muestra en la lista Implementación y, a continuación, elija Desconectar. En el cuadro de diálogo de confirmación, elija Desconectar. Repita hasta que elimine todos los destinos.

4. En la parte superior de la página, elija Eliminar.
5. En el cuadro de diálogo de confirmación, escriba el nombre de la política y, a continuación, elija Eliminar.

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 siguiente ejemplo se elimina la política especificada. Solo funciona si la política no está asociada a ningún nodo raíz, unidad organizativa o cuenta.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- SDK de AWS: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 asocia una política de copia de seguridad a una cuenta, esa política se aplica únicamente 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 herede la cuenta de las unidades organizativas raíz y principales, así como de cualquier política directamente asociada a la cuenta, es la política en vigor. Para obtener información sobre cómo se fusionan las políticas con la política en vigor, consulte Descripción de la herencia de políticas de administración.

Asociar una política de copia de seguridad

Cuando inicia sesión en la cuenta de administración de la organización, puede asociar una política de copia de seguridad al nodo raíz de la organización, la 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 el nodo raíz, unidad organizativa o cuenta a la que desee adjuntar la política.

Para asociar una política de copia de seguridad navegando hasta el nodo raíz, unidad organizativa o cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, busque y seleccione el nombre del nodo 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.
3. En la pestaña Políticas, en la entrada de Políticas de copia de seguridad, elija Adjuntar.
4. Busque la política que desea y elija Asociar política.

La lista de políticas de copia de seguridad asociadas en la pestaña Políticas se actualiza para incluir la nueva adición. El cambio en la política surtirá efecto de inmediato.

Para adjuntar una política de copia de seguridad navegando a la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de copia de seguridad elija el nombre de la política que desea adjuntar.
3. En la pestaña Objetivos, seleccione Adjuntar.
4. Elija el botón de opción situado junto al nodo 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 Asociar política.

   La lista de políticas de copia de seguridad asociadas en la pestaña Objetivos se actualiza para incluir la nueva adición. El cambio en la política surtirá efecto de inmediato.

AWS CLI & AWS SDKs

Para asociar una política de copia de seguridad al nodo raíz de la organización, la OU o la cuenta

Puede utilizar uno de los comandos siguientes para adjuntar una política de copia de seguridad:

- AWS CLI: attach-policy

```
$ aws organizations attach-policy \
    --target-id 123456789012 \
    --policy-id p-i9j8k7l6m5
```

- SDK de AWS:AttachPolicy

El cambio en la política surtirá efecto de inmediato.

Desasociar una política de copia de seguridad

Cuando inicia sesión en la cuenta de administración de su organización, puede desconectar una política de copia de seguridad del nodo 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 desconectar una política de copia de seguridad navegando hasta la política o el nodo raíz, unidad organizativa o cuenta de la que desee desconectar la política.

Para desconectar una política de copia de seguridad navegando hasta el nodo raíz, unidad organizativa o cuenta a la que está adjunta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS desplácese hasta el nodo raíz, unidad organizativa o cuenta de la que desea desconectar 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 del nodo raíz, unidad organizativa o cuenta.
3. En la pestaña Políticas elija el botón de opción situado junto a la política de copia de seguridad que desea desconectar y, a continuación, elija Desconectar.
4. En el cuadro de diálogo de confirmación, elija Desconectar política.

   La lista de políticas de copia de seguridad asociadas se actualiza. El cambio en la política surtirá efecto de inmediato.

Para desconectar una política de copia de seguridad navegando hasta la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de copia de seguridad elija el nombre de la política que desea desconectar de un nodo raíz, unidad organizativa o cuenta.
3. En la pestaña de Objetivos, elija el botón de opción situado junto al nodo raíz, unidad organizativa o cuenta de la que desea desconectar 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, elija Desconectar.

   La lista de políticas de copia de seguridad asociadas se actualiza. El cambio en la política surtirá efecto de inmediato.

AWS CLI & AWS SDKs

Para desconectar una política de copia de seguridad de nodo raíz de la organización, la unidad organizativa o la cuenta

Puede utilizar uno de los comandos siguientes para desconectar una política de copia de seguridad:

- AWS CLI:detach-policy

  En el ejemplo siguiente se desconecta una política de una unidad organizativa.

```
$ aws organizations detach-policy \
    --target-id ou-a1b2-f6g7h222 \
    --policy-id p-i9j8k7l6m5
```

  Este comando no genera ninguna salida si se realiza correctamente.

- SDK de AWS:DetachPolicy

El cambio en la 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 Management Console AWS, API AWS, o interfaz de línea de comandos AWS. En la siguiente sección se proporciona una breve información general de la política de copia de seguridad en vigor, incluido un ejemplo.

¿Cuál es la política de copia de seguridad en vigor?

La política de copia de seguridad en vigor especifica la configuración final del plan de copia de seguridad que se aplica a una 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 se asocia una política de copia de seguridad al nodo 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. Cuando se asocia una política directamente a una cuenta, solo se aplica a esa 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 realizan una copia de seguridad de sus tablas de DynamoDB una vez a la 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, consulte Descripción de la herencia de políticas de administración.

Ver la política de copia de seguridad en vigor

Puede ver la política de copia de seguridad en vigor de una cuenta usando la AWS Management Console, la API de AWS o AWS 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 de copia de seguridad en vigor de una cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En 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 pestaña Políticas, en la sección Políticas de copia de seguridad, elija Ver la política de copia de seguridad en vigor de este Cuenta de AWS.

   La consola muestra la política 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 políticas de copia de seguridad deben incluir los Operadores de herencia que especifican cómo se fusiona cada configuración en la política en vigor final.

AWS CLI & AWS SDKs

Para ver la política de copia de seguridad 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 siguiente ejemplo 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\"
}}}}}}}"
    }
}
```

- SDK de AWS: DescribeEffectivePolicy

Uso de eventos de AWS CloudTrail para monitorear las políticas de respaldo en su organización

Puede usar los eventos de AWS CloudTrail para monitorear cuándo se crean, actualizan o eliminan las políticas de respaldo de cualquier cuenta de su organización de AWS, o cuando hay un plan de respaldo organizacional no válido. Para obtener más información, consulte Cómo registrar eventos de administración entre cuentas en la Guía para desarrolladores AWS Backup.

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.

El bloque de una política de copia de seguridad es el plan de copia de seguridad y sus reglas. La sintaxis del plan de respaldo dentro de una política de AWS Organizations respaldo es estructuralmente idéntica a la sintaxis utilizada por AWS Backup, pero los nombres de las claves son diferentes. En las descripciones de los nombres clave de la política que aparecen a continuación, cada uno incluye el nombre de clave del AWS Backup plan equivalente. Para obtener más información sobre AWS Backup los planes, consulte CreateBackupPlanla Guía paraAWS Backup desarrolladores.

> **Note**
>
> Al usar JSON, se rechazarán los nombres de clave duplicados. Si desea incluir varios planes, reglas o selecciones en una sola política, asegúrese de que el nombre de cada clave sea único.

Para ser completa y funcional, una política de copia de seguridad en vigor debe incluir algo más que un plan de copia de seguridad con su programación y sus reglas. La política también debe identificar los recursos de Regiones de AWS los que se va a realizar la copia de seguridad, así como la función AWS Identity and Access Management (de IAM) que AWS Backup se puede 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 adjuntara directamente a una cuenta, se AWS Backup haría una copia de seguridad de todos los recursos de esa cuenta en las `eu-north-1` regiones `us-`

east-1 y regiones que tienen la etiqueta dataType con un valor de PII oRED. 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. Las dos bóvedas se encuentran en la misma cuenta que el recurso. También almacena una copia de la copia de seguridad en la My_Tertiary_Vault en una cuenta diferente, explícitamente especificada. Las bóvedas deben existir ya en cada una de las áreas especificadas Regiones de AWS para cada una de las Cuenta de AWS que reciben la política vigente. Si alguno de los recursos respaldados son instancias 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:

- Variables `$account`: en ciertas cadenas de texto de las políticas, puede usar la función `$account` para representar la Cuenta de AWSactual. Cuando AWS Backup ejecuta un plan en la política efectiva, reemplaza automáticamente esta variable por la actual Cuenta de AWS en la que se ejecutan la política efectiva y sus planes.

  > **Important**
  >
  > Solo puede utilizar la variable `$account` 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 haya un depósito con el nombre `My_Vault` en cada uno de los lugares a los Cuenta de AWS que se aplique la política.

  ```
  arn:aws:backup:us-west-2:$account:vault:My_Vault"
  ```

  Le recomendamos que utilice conjuntos de AWS CloudFormation pilas y su integración con Organizations para crear y configurar automáticamente bóvedas de respaldo y funciones de IAM para cada cuenta de miembro de la organización. Para obtener más información, consulte Crear un conjunto de pilas con permisos autoadministrados en la Guía del usuarioAWS CloudFormation .

- Operadores de herencia: las políticas de copia de seguridad pueden utilizar tanto la herencia de Operadores de configuración de valores como los Operadores de control secundarios.

- `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 propias `rules`, `regions`, `selections`, y `tags`.

  El nombre clave de este plan de respaldo en una política de respaldo se corresponde con el valor de la `BackupPlanName` clave en un plan. AWS Backup

  Cada plan puede contener los siguientes elementos:

  - `rules`— 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 los elementos `selections` y `regions` de la política de copia de seguridad en vigor.
  - `regions`— Esta clave contiene una lista de matrices de Regiones de AWS cuyos recursos se pueden respaldar mediante esta política.
  - `selections`— Esta clave contiene una o más colecciones de recursos (dentro de la `regions` específica) que se hace una copia de seguridad en `rules`.
  - `advanced_backup_settings`— Esta clave contiene la configuración específica de las copias de seguridad que se ejecutan en determinados recursos.
  - `backup_plan_tags`: Esto especifica etiquetas adjuntas al plan de copia de seguridad en sí.
- `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`— La clave de esta política se corresponde con la `ScheduleExpression` clave de un AWS Backup plan.

    Especifica la hora de inicio de la copia de seguridad. Esta clave contiene el operador de valor `@@assign` heredado y un valor de cadena con una expresión CRON que especifica cuándo AWS Backup se debe iniciar 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 relaciona con la `TargetBackupVaultName` clave de un AWS Backup plan.

  Especifica el nombre del almacén de copia de seguridad en el que se almacenará la copia de seguridad. El valor se crea mediante el uso de AWS Backup. Esta clave contiene el operador de valor heredado de `@@assign` 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. Le recomendamos que utilice conjuntos de AWS CloudFormation pilas y su integración con Organizations para crear y configurar automáticamente bóvedas de respaldo y funciones de IAM para cada cuenta de miembro de la organización. Para obtener más información, consulte Crear un conjunto de pilas con permisos autoadministrados en la Guía del usuarioAWS CloudFormation .

- `start_backup_window_minutes`— Esta clave de política se corresponde con la `StartWindowMinutes` clave de un plan. AWS Backup

  (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` y un valor con un número entero de minutos.

- `complete_backup_window_minutes` – Esta clave de política se asigna a la clave `CompletionWindowMinutes` de un plan de AWS Backup

  (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 AWS Backuplo cancele. Esta clave contiene el operador de valor heredado de `@@assign` y un valor con un número entero de minutos.

- `enable_continuous_backup`— La clave de esta política se corresponde con la `EnableContinuousBackup` clave de un AWS Backup plan.

  (Opcional) Especifica si AWS Backup crea copias de seguridad continuas. `True`hace AWS Backup que se creen copias de seguridad continuas con capacidad de point-in-time restauración (PITR). `False`(o no especificado) provoca AWS Backup la creación de copias de seguridad 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 especificar un valor si establece una de las siguientes opciones:
>
> - Defina `delete_after_days` en un valor mayor de 35.
> - Establezca `move_to_cold_storage_after_days` en cualquier valor.

Para obtener más información sobre las copias de seguridad continuas, consulte la oint-in-time recuperación de P en la Guía paraAWS Backup desarrolladores.

- `lifecycle`— La clave de esta política se corresponde con la `Lifecycle` clave de un AWS Backup plan.

  (Opcional) Especifica cuándo AWS Backup pasa esta copia de seguridad a almacenamiento en frío y cuándo caduca.

  - `move_to_cold_storage_after_days` — La clave de esta política se corresponde con la `MoveToColdStorageAfterDays` clave de un AWS Backup plan.

    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` y un valor con un número entero de días.

  - `delete_after_days`— La clave de esta política se corresponde con la `DeleteAfterDays` clave de un AWS Backup plan.

    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` 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`— La clave de esta política se corresponde con la `CopyActions` clave de un AWS Backup plan.

(Opcional) Especifica que se 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 clave `DestinationBackupVaultArn` de un plan de AWS Backup

    (Opcional) Especifica el almacén en el que se AWS Backup almacena una copia adicional de la copia de seguridad. El valor de esta clave contiene el Operador de valores de herencia `@@assign` y el ARN de la bóveda.
    - Para hacer referencia a un almacén en el Cuenta de AWS que se ejecuta la política de copias de seguridad, utilice la `$account` variable del ARN en lugar del número de ID de la cuenta. Cuando AWS Backup ejecuta el plan de respaldo, reemplaza automáticamente la variable por el número de ID de cuenta Cuenta de AWS en la que se ejecuta la política. Esto permite que la copia de seguridad se ejecute correctamente cuando la política 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 diferente 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 esta razón, le recomendamos que proporcione siempre esta clave y valor.
    > - El almacén de copia de seguridad que quiere copiar a la copia de seguridad ya debe existir la primera vez que inicie el plan de copia de seguridad. Se recomienda utilizar conjuntos de pilas de stack sets AWS CloudFormation y 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, consulte Crear un conjunto de pilas con permisos autoadministrados en la Guía del usuarioAWS CloudFormation .

- `lifecycle`— La clave de esta política se asigna a la `Lifecycle` clave situada debajo de la `CopyAction` clave de un AWS Backup plan.

  (Opcional) Especifica cuándo se hace la AWS Backup transición de esta copia de una copia de seguridad a un almacenamiento en frío y cuándo caduca.

  - `move_to_cold_storage_after_days` – Esta clave de política se asigna a la clave `MoveToColdStorageAfterDays` de un plan de AWS Backup .

    Especifica el número de días transcurridos desde la realización de la copia de seguridad antes de que el punto de recuperación AWS Backup se traslade al almacenamiento en frío. Esta clave contiene el operador de valores de herencia de`@@assign` y un valor con un número entero de días.

  - `delete_after_days` – Esta clave de política se asigna a la clave `DeleteAfterDays` de un plan de AWS Backup

    Especifica el número de días transcurridos desde la realización de la copia de seguridad antes de AWS Backup eliminar el punto de recuperación. Esta clave contiene el operador de valores de herencia de`@@assign` 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 corresponde con la `RecoveryPointTags` clave de un AWS Backup plan.

  (Opcional) Especifica las etiquetas que se AWS Backup adjuntan 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 `0wner`. 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` y un valor de cadena. El 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 y uno o más valores para reemplazar, adjuntar o quitar de la política en vigor. Estos valores distinguen entre mayúsculas y minúsculas.

- `regions`

  La clave `regions` de política especifica qué Regiones de AWS recursos AWS Backup busca para encontrar los recursos que cumplen las condiciones de la `selections` clave. Esta clave contiene cualquiera de los operadores de valores heredados y uno o más valores de cadena para los 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 aproximadamente al BackupSelectionobjeto en 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 la Regiones de AWS especificada por la clave `regions`. Este valor contiene el operador del valor de `@@assign` herencia y un valor de cadena que contiene el ARN del rol. AWS Backup utiliza este rol para buscar 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 se ejecuta el plan de respaldo AWS Backup, reemplaza automáticamente la variable por el número de ID de cuenta real de la cuenta Cuenta de AWS en la que se ejecuta la política.

> **Important**
>
> El rol ya debe existir cuando inicie el plan de copia de seguridad la primera vez. Le recomendamos que utilice conjuntos de AWS CloudFormation pilas y su integración con Organizations para crear y configurar automáticamente bóvedas de respaldo y funciones de IAM para cada cuenta de miembro de la organización. Para obtener más información, consulte Crear un conjunto de pilas con permisos autoadministrados en la Guía del usuarioAWS CloudFormation .

- `tag_key` — Especifica el nombre de clave de etiqueta que se va a buscar. Esta clave contiene el operador de valor heredado de `@@assign` y un valor de cadena. El valor distingue entre mayúsculas y minúsculas.
- `tag_value`— Especifica el valor que debe asociarse a un nombre de clave que coincida. `tag_key` AWS Backup incluye el recurso en la copia de seguridad solo si ambos `tag_value` coinciden. `tag_key` Esta clave contiene cualquiera de los operadores de valor heredado 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 tipo de recurso `"ec2"` 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 copia de seguridad de Windows habilitada para VSS en la Guía para desarrolladoresAWS Backup .

```
"advanced_backup_settings": {
    "ec2": {
        "windows_vss": {
```

```
            "@@assign": "enabled"
        }
    }
}
```

- `backup_plan_tags`: Especifica etiquetas adjuntas al plan de copia de seguridad en sí. 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` 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` y un valor de cadena. Este valor distingue entre mayúsculas y minúsculas.

Ejemplos de políticas de copia de seguridad

Los ejemplos de 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 política se puede asociar al nodo raíz de la organización o a cualquier unidad organizativa que sea primaria 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 hereda ni se adjunta ninguna otra política a las cuentas, la política vigente que se muestra en cada una de las aplicables es la Cuenta de AWS que se muestra en el siguiente ejemplo. 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 siguiente ejemplo, una política principal heredada y una política secundaria se heredan o se asocian directamente a una Cuenta de AWS fusión para formar la política efectiva.

Política principal: esta política se puede asociar al nodo 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 secundaria: esta política puede estar asociada directamente a la cuenta o a una unidad organizativa en cualquier nivel por debajo del nivel al que está asociada.

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

Resultado de políticas 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 para aplicar toda la configuración y evita que una política secundaria los modifique.

Política principal: esta política se puede asociar al nodo 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"]
                    }
                }
            }
        }
    }
}
```

Resultado de políticas en vigor: si existe alguna política de copia de seguridad secundaria, se ignora y la política principal se convierte en la política 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 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 política se puede asociar al nodo 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 secundaria: esta política puede estar asociada directamente a la cuenta o a una unidad organizativa en cualquier nivel por debajo del nivel al que está asociada. Esta política secundaria define un nuevo plan.

Las secciones del plan se truncan para mayor claridad.

```
{
    "plans": {
        "MonthlyBackupPlan": {
            "regions": { ... },
            "rules": { ... },
            "selections": { … }
        }
    }
}
```

Resultado de políticas en vigor — La política en vigor 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 utiliza operadores de establecimiento de valores para anular algunas de las configuraciones heredadas de una política principal.

Política principal: esta política se puede asociar al nodo 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 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 secundaria: la política secundaria incluye solo la configuración que debe ser diferente de la política 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 no válido que 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"}
                    }
```

```
                }
            }
        }
    }
}
```

Resultado de políticas en vigor: la política en vigor incluye la configuración de ambas políticas, con la configuración proporcionada por la política secundaria anulando la configuración heredada de la principal. 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 secundaria.
- AWS Backup actúa cada dos horas en lugar de cada hora.
- AWS Backup deja transcurrir 80 minutos para que comience la copia de seguridad en lugar de 60 minutos.
- AWS Backup utiliza la `Default` bóveda 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

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 utilizar 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 información general sobre el etiquetado, incluidas las convenciones de denominación y uso, consulte la Guía del usuario de Tagging AWS Resources.
- Para obtener una lista de los servicios que admiten el uso de etiquetas, consulte Referencia de la API de etiquetado de Resource Groups Tagging API Reference.
- Para obtener información sobre el uso de etiquetas para categorizar los recursos, consulte el documento técnico sobre las prácticas recomendadas para AWS etiquetar los recursos.
- Para obtener información acerca del etiquetado de recursos de Organizations, consulte Etiquetado de recursos de AWS Organizations.
- Para obtener información sobre cómo etiquetar los recursos en otros AWS servicios, consulte la documentación de ese servicio.

¿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 se inicia sesión en la cuenta de administración de la organización, se utiliza Organizations para habilitar la característica de políticas de etiquetas. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización. 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 se inicia sesión en una cuenta de la organización, se 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 la organización, puede ver la información de conformidad de todas las cuentas de la organización.

Las políticas de etiquetas solo están disponibles en las organizaciones que tienen todas las características habilitadas. Para obtener más información acerca de qué se necesita para utilizar políticas de etiquetas, consulte Requisitos previos y permisos para administrar políticas de etiquetas.

> **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 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 la página Introducción a las políticas de etiquetas también ofrecen 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
- Permisos para administrar políticas de etiquetas

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.
- 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.

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

La política de IAM de ejemplo siguiente 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 sobre las políticas y permisos de IAM, consulte la Guía del usuario de IAM.

Prácticas recomendadas para utilizar políticas de etiquetas

AWS recomienda 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.

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. Consulte también los flujos de trabajo que se describen en Introducción a las políticas de etiquetas.

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. Para saber si un servicio de AWS es soportado por el control del acceso mediante etiquetas, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM. 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 varios servicios de AWS. 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
- Prácticas recomendadas para utilizar políticas de etiquetas

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 etiquetado de su organización.	Esta es la cuenta de administración de la organización.	AWS Organizations
Paso 2: cree una política de etiquetas. 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.	Esta es la cuenta de administración de la organización.	AWS Organizations
Paso 3: asocie una política de etiquetas a la cuenta de un solo miembro que pueda utilizar para las pruebas. Tendrá que iniciar sesión en esta cuenta en el siguiente paso.	Esta es la cuenta de administración de la organización.	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

Tarea	Cuenta en la que iniciar sesión	Consola de servicio de AWS que utilizar
		secretos de conformidad y no conformes.
Paso 5: vea 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.	Resource Groups y el servicio de AWS en el que 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.	Resource Groups y el servicio de AWS en el que se creó el recurso.
En cualquier momento, puede evaluar el cumplimiento en toda la organización.	Esta es la cuenta de administración de la organización.	Grupos de recursos

[1] Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

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. 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 de administración y Sintaxis de la política de etiquetas para crear políticas de etiquetas más detalladas.	Esta es la cuenta de administración de la organización.	AWS Organizations
Asocie políticas de etiquetas a cuentas o unidades organizativas adicionales. Compruebe la política de etiquetas en vigor de una cuenta después de asociar más políticas a ella o a cualquier unidad organizativa de la que la cuenta sea miembro.	Esta es la cuenta de administración de la organización.	AWS Organizations
Cree una SCP para precisar etiquetas cuando alguien cree nuevos recursos. Para ver un	Esta es la cuenta de administración de la organización.	AWS Organizations

Tarea avanzada	Cuenta en la que iniciar sesión	Consola de servicio de AWS que utilizar
ejemplo, consulte Requerir una etiqueta en los recursos creados especificados.		
Continúe evaluando el estado de cumplimiento de la cuenta con la política de etiquetas en vigor a medida que cambia. Corrija las etiquetas no conformes.	Una cuenta de miembro con una política de etiquetas efectiva.	Resource Groups y el servicio de AWS en el que se creó el recurso.
Evalúe el cumplimiento en toda la organización.	Esta es la cuenta de administración de la organización.	Grupos de recursos

[1] Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

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.

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. 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.	Esta es la cuenta de administración de la organización.	AWS Organizations
Paso 2: asocie una política de etiquetas a una única cuenta de prueba.	Esta es la cuenta de administración de la organización.	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 en un recurso 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.

Tareas de aplicación de políticas	Cuenta en la que iniciar sesión	Consola de servicio de AWS que utilizar
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 el servicio de AWS en el que 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.	Resource Groups y el servicio de AWS en el que se creó el recurso.
En cualquier momento, puede evaluar el cumplimiento en toda la organización.	Esta es la cuenta de administración de la organización.	Grupos de recursos

[1] Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

Crear, actualizar y eliminar políticas de etiqueta

En este tema:

- Después de habilitar las políticas de etiquetas de su organización, puede crear una política.
- Cuando cambien sus requisitos de etiquetado, puede actualizar una política existente.
- Cuando ya no necesite una política y después de desconectarla de todas las unidades organizativas (OU) y cuentas, puede eliminarla.

> **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 etiqueta 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 solo el operador de configuración de valores @@assign y no proporciona ningún acceso a los operadores de control secundarios. Solo puede agregar los operadores de control infantil 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Tag policies (Políticas de etiquetas), seleccione Create policy (Crear política).
3. En la página Create policy (Crear política), introduzca un Policy name (Nombre de política) y una Description (Descripción) opcional para la política.
4. (Opcional) Puede agregar una o varias etiquetas al objeto de la política en sí. Estas etiquetas no forman parte de la política. Para ello, elija Agregar etiqueta y, a continuación, ingrese 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.

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 información acerca de la sintaxis de políticas de etiquetas, consulte Sintaxis de la política de etiquetas.

   En Nueva clave de etiqueta 1, especifique el nombre de la clave de etiqueta que desea agregar.

6. En Tag key capitalization compliance (Conformidad del uso de mayúsculas en la clave de etiqueta), deje esta opción desactivada (la opción predeterminada) para especificar que la política de etiquetas principal heredada, si existiera, debe definir el tratamiento de las mayúsculas y minúsculas en la clave de etiqueta.

   Habilite esta opción si desea asignar un uso específico de las mayúsculas en la clave de etiqueta mediante esta política. Si selecciona esta opción, el uso de mayúsculas que haya especificado en Tag Key (Clave de etiqueta) anula el tratamiento de las mayúsculas y minúsculas especificado en una política principal heredada.

   Si no existe ninguna política principal y no se habilita esta opción, solo las claves de etiqueta con todos los caracteres en minúscula se consideran conformes. Para obtener más información acerca de la herencia de políticas principales, consulte Descripción de la herencia de políticas de administración.

   > **Tip**
   >
   > Tenga en cuenta el uso de la política de etiquetas de ejemplo que se muestra en Ejemplo 1: Definir las mayúsculas y minúsculas de la clave de etiquetas en toda la organización 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. Para Cumplimiento de valor de etiquetas, habilite esta opción si desea agregar valores permitidos a 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 esos valores definidos y heredados de una política principal. Si no

existe ninguna política principal y no especifica valores de etiqueta, entonces cualquier valor (incluso la ausencia de valores) se considera conforme.

Para actualizar la lista de valores de etiqueta aceptables, seleccione Specify allowed values for this tag key (Especificar los valores permitidos en esta clave de etiqueta) y, a continuación, elija Specify values (Especificar valores). Cuando se le soliciten, introduzca los nuevos valores (un valor por casillero) y elija Save changes (Guardar cambios).

8. En Prevent noncompliant operations for this tag (Evitar operaciones no conformes en esta etiqueta), 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 en Descripción de la aplicación de políticas y evaluar minuciosamente. 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 los tipos de recursos. Cuando se le solicite, seleccione los tipos de recursos que desea incluir en la política. 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 solo si la operación da como resultado etiquetas que cumplan con la política.

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 6-9 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 información acerca de la sintaxis de políticas de etiquetas, consulte Sintaxis de la política de etiquetas.

Para crear una política de etiquetas

1. Cree una política de etiquetas en un archivo de texto que tenga un aspecto similar a la 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 política que contenga el contenido de la política 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"
    }
}
```

- SDK de AWS: CreatePolicy

Qué hacer a continuación

Después de crear una política de etiquetas, puede poner las reglas de etiquetado en vigor. Para ello, asocie la política a la raíz de la organización, las unidades organizativas (OU), las Cuentas de AWS 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Tag policies (Políticas de etiquetas), elija la política de etiquetas que desea actualizar.

3. Elija Edit policy (Editar política).
4. Puede introducir un nuevo Nombre de la política, Descripción de la política. Puede cambiar el contenido de la política mediante el Editor visual o editando el JSON.
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 siguiente ejemplo 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\n"
    }
}
```

  En el siguiente ejemplo 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\n"
    }
}
```

En el ejemplo siguiente se cambia el documento de política JSON adjunto a una política de exclusión de servicio 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\"]}}}}"
}
```

- SDK de AWS: UpdatePolicy

Edición de etiquetas adjuntas a una política de etiquetas

Cuando inicie sesión en la cuenta de administración de su organización, puede agregar o quitar 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 política de etiquetas en su organización AWS, debe contar con los siguientes permisos:

- `organizations:DescribeOrganization` (solo consola: para navegar a la política)
- `organizations:DescribePolicy` (solo consola: para navegar a la política)
- `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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de etiquetas, elija elegir nombre de la política con las etiquetas que desea editar.

3. En la página de detalles elegida de la política, elija la opción Etiquetas y, a continuación, elija Administrar 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 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 eligiendo Eliminar.
   - Agregue una nueva clave de etiqueta y valore el par. Seleccione Agregar etiqueta y, a continuación, introduzca el nuevo nombre de clave y el valor opcional en los cuadros proporcionados. Si deja el Valor en blanco, el valor es una cadena vacía; no es `null`.
5. Seleccione Guardar los cambios después 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 comandos siguientes para editar las etiquetas adjuntas a una política de etiquetas:

- AWS CLI: tag-resource y untag-resource
- SDK de AWS:TagResource y UntagResource

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 desconectarla 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2.
3. En la página Políticas de etiquetas, elija la política que desea eliminar.
4. Primero debe desconectar la política que desea eliminar de todos los nodos raíz, unidades organizativas y cuentas. Elija la pestaña Objetivos, elija el botón de opción situado junto a cada nodo raíz, unidad organizativa o cuenta que se muestra en la lista de Objetivos y, a continuación, elija Desconectar. En el cuadro de diálogo de confirmación, elija Desconectar.
5. En la parte superior de la página, elija Eliminar.
6. En el cuadro de diálogo de confirmación, escriba el nombre de la política y, a continuación, elija Eliminar.

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 siguiente ejemplo se elimina la política especificada. Solo funciona si la política no está asociada a ningún nodo raíz, unidad organizativa o cuenta.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- SDK de AWS:DeletePolicy

Conectar 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. Para obtener más información, consulte Descripción de la herencia de políticas de administración.

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 asociar una política de etiquetas navegando hasta la política o el nodo raíz, unidad organizativa o cuenta a la que desee adjuntar la política.

Para asociar una política de etiquetas navegando hasta el nodo raíz, unidad organizativa o cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

2. En la página Cuentas de AWS, busque y seleccione el nombre del nodo 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.
3. En la pestaña Políticas, en la entrada de Políticas de etiquetas, elija Adjuntar.
4. Busque la política que desea y elija Asociar política.

   La lista de políticas de etiquetas asociadas en la pestaña Políticas se actualiza para incluir la nueva adición. El cambio en la política surtirá efecto de inmediato.

Para adjuntar una política de etiquetas navegando a la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de etiquetas, elija el nombre de la política que desea adjuntar.
3. En la pestaña Objetivos, seleccione Adjuntar.
4. Elija el botón de opción situado junto al nodo 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 Asociar política.

   La lista de políticas de etiquetas asociadas en la pestaña Objetivos se actualiza para incluir la nueva adición. El cambio en la política surtirá efecto de inmediato.

AWS CLI & AWS SDKs

Para asociar una política de etiquetas a la raíz de la organización, la OU 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.

- SDK de AWS:AttachPolicy

El cambio en la política surtirá efecto de inmediato.

Qué hacer a continuación

Después de asociar una política de etiquetas, puede averiguar la conformidad de sus 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 desconectar una política de etiquetas del nodo 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 desconectar una política de etiquetas navegando hasta la política o el nodo raíz, unidad organizativa o cuenta de la que desee desconectar la política.

Para desconectar una política de etiqueta navegando hasta el nodo raíz, unidad organizativa o cuenta a la que está adjunta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS desplácese hasta el nodo raíz, unidad organizativa o cuenta de la que desea desconectar 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 del nodo raíz, unidad organizativa o cuenta.
3. En la pestaña Políticas, elija el botón de opción situado junto a la política de etiquetas que desea desconectar y, a continuación, elija Desconectar.
4. En el cuadro de diálogo de confirmación, elija Desconectar política.

   Actualización de la lista de políticas de etiquetas asociadas. El cambio en la política surtirá efecto de inmediato.

Para desconectar una política de etiquetas navegando hasta la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de etiquetas, elija el nombre de la política que desea desconectar de un nodo raíz, unidad organizativa o cuenta.
3. En la pestaña de Objetivos, elija el botón de opción situado junto al nodo raíz, unidad organizativa o cuenta de la que desea desconectar 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, elija Desconectar.

   Actualización de la lista de políticas de etiquetas asociadas. El cambio en la política surtirá efecto de inmediato.

AWS CLI & AWS SDKs

Para desconectar una política de etiquetas de la raíz de la organización, la unidad organizativa o la cuenta

Puede utilizar uno de los siguientes elementos para desconectar una política de etiquetas:

- AWS CLI:detach-policy
- SDK de AWS:DetachPolicy

El cambio en la 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 etiqueta `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 de administración.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, elija 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 pestaña Políticas, en la sección Políticas de etiquetas, elija Ver la política de etiquetas en vigor de este Cuenta de AWS.

   La consola muestra la política 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 la política de etiquetas

deben incluir los operadores de herencia que especifican 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 asocian a una cuenta, ejecute la siguiente acción desde la cuenta y guarde el resultado 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 y al nodo raíz o a cualquier OU, la combinación de todas las políticas heredadas define la política de etiquetas en vigor de la cuenta. En estos casos, ejecutar `describe-effective-policy` desde la cuenta devuelve el contenido combinado de todas las políticas de etiquetas en la jerarquía de la cuenta.

- SDK de AWS: DescribeEffectivePolicy

Uso de Amazon EventBridge para supervisar etiquetas no conformes

Puede utilizar Amazon EventBridge, antes Eventos de Amazon CloudWatch, 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 más información de EventBridge, consulte la Guía del usuario de Amazon EventBridge.

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:

- En la pestaña Visual editor (Editor visual), seleccione Prevent noncompliant operations for this tag (Evitar las operaciones no conformes en esta etiqueta).
- 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.

Siga estas prácticas recomendadas para ejecutar la conformidad con las políticas de etiquetas:

- Actúe con precaución al ejecutar la conformidad. Asegúrese de que conoce los efectos del uso de políticas de etiquetas y siga los flujos de trabajo recomendados que se describen en Introducción a las políticas de etiquetas. 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 la conformidad de las política de etiquetas en tipos de recursos admitidos. 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— Algunos AWS tienen 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 grupos de Amazon EC2 Auto Scaling y los clústeres de Amazon EMR se pueden propagar automáticamente a las instancias de Amazon EC2 contenidas. Puede contar con políticas de etiquetas para Amazon EC2 que sean 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 que utiliza la política de etiqueta, 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 etiquetado de la API o la consola del servicio AWS que tiene los recursos no conformes.
- Usar los AWS Resource Groups TagResources y UntagResources para agregar 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 importa que estén en conformidad 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 las Cuentas de AWS de la 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 la organización en la región `us-east-1`, dado que tiene acceso a un bucket de Amazon S3. El bucket debe tener una política de bucket asociada como se muestra en Política de bucket de Amazon S3 para almacenar informes. 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 devuelva `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 • Operaciones de la API REST • Escenarios	• `"apigateway:apikeys"` • `"apigateway:domainnames"` • `"apigateway:restapis"` • `"apigateway:restapis/stages"`
AWS Amplify	• Componente • Tema	• `"amplifyuibuilder:app/environment/components"` • `"amplifyuibuilder:app/environment/themes"`
AWS AppConfig	• Aplicación • Perfil de configuración • Implementación	• `"appconfig:application"` • `"appconfig:application/configurationprofile"` • `"appconfig:application/environment/deployment"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
	• Estrategia de implementación • Entorno	• `"appconfig:deploymentstrategy"` • `"appconfig:application/environment"`
AWS App Mesh	• Todos • Puerta de enlace de entrada • Malla • Ruta • Puerta de enlace virtual • Nodo virtual • Enrutador virtual • Servicio virtual	• `"appmesh:*"` • `"appmesh:mesh/virtualGateway/gatewayRoute"` • `"appmesh:mesh"` • `"appmesh:mesh/virtualRouter/route"` • `"appmesh:mesh/virtualGateway"` • `"appmesh:mesh/virtualNode"` • `"appmesh:mesh/virtualRouter"` • `"appmesh:mesh/virtualService"`
Amazon Athena	• Todos • Grupo de trabajo	• `"athena:*"` • `"athena:workgroup"`
AWS Audit Manager	• Evaluación • Marco de evaluación • Controlar	• `"auditmanager:assessment  "` • `"auditmanager:assessmentFramework "` • `"auditmanager:control  "`
AWS Backup	• Plan de copias de seguridad • Almacén • Puerta de enlace • Hipervisor • VM	• `"backup:backup-plan"` • `"backup:backup-vault"` • `"backup-gateway:gateway"` • `"backup-gateway:hypervisor"` • `"backup-gateway:vm"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
AWS Batch	• Trabajo • Definición de trabajo • Cola de trabajos	• `"batch:job"` • `"batch:job-definition"` • `"batch:job-queue"`
AWS BugBust	• Evento	• `"bugbust:event"`
AWS Certificate Manager	• Todos • Certificados • Private Certificate Authority	• `"acm:*"` • `"acm:certificate"` • `"acm-pca:certificate-authority"`
Amazon Chime	• Instancia de aplicación • Canal • Canalización de medios • Reunión • Aplicaciones multimedia SIP • Instancia de aplicación de usuario • Conector de voz	• `"chime:app-instance"` • `"chime:app-instance/channel"` • `"chime:media-pipeline"` • `"chime:meeting"` • `"chime:sma"` • `"chime:app-instance/user"` • `"chime:vc"`
AWS Clean Rooms	• Colaboración • Tabla configurada • Pertenencia • Asociación de tablas configurada	• `"cleanrooms:collaboration"` • `"cleanrooms:configuredtable"` • `"cleanrooms:membership"` • `"cleanrooms:membership/configuredtableassociation"`
AWS Cloud9	• Entorno	• `"cloud9:environment"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon CloudFront	• Todos • Distribución • Distribución de streaming	• `"cloudfront:*"` • `"cloudfront:distribution"` • `"cloudfront:streaming-distribution"`
AWS CloudTrail	• Todos • Trail	• `"cloudtrail:*"` • `"cloudtrail:trail"`
Amazon CloudWatch	• Todos • Alarma • Reglas de Contributor Insights • Flujos métricos	• `"cloudwatch:*"` • `"cloudwatch:alarm"` • `"cloudwatch:insight-rule"` • `"cloudwatch:metric-stream"`
Amazon CloudWatch Internet Monitor	• Monitorizar	• `"internetmonitor:monitor"`
Amazon CloudWatch Logs	• Grupo de registros	• `"logs:log-group"`
Administrador de acceso a Amazon CloudWatch Observability	• Enlace • Sink	• `"oam:link"` • `"oam:sink"`
AWS CodeBuild	• Todos • Proyecto	• `"codebuild:*"` • `"codebuild:project"`
Amazon CodeCatalyst	• Conexiones	• `"codecatalyst:connections"`
AWS CodeCommit	• Todos • Repositorio	• `"codecommit:*"` • `"codecommit:repository"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
AWS CodePipeline	• Todos • Tipo de acción • Canalización • Webhook	• `"codepipeline:*"` • `"codepipeline:actiontype"` • `"codepipeline:pipeline"` • `"codepipeline:webhook"`
Amazon Cognito Identity	• Todos • Grupo de identidades	• `"cognito-identity:*"` • `"cognito-identity:identitypool"`
Grupos de usuarios de Amazon Cognito	• 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 Config • Regla de Config	• `"config:*"` • `"config:aggregation-authorization"` • `"config:config-aggregator"` • `"config:config-rule"`
CodeGuru Revisor de Amazon	• Asociación	• `"codeguru-reviewer:association"`
CodeGuru Seguridad de Amazon	• Examen	• `"codeguru-security:scans"`
CodeConnections	• Connection • Host	• `"codestar-connections:connection"` • `"codestar-connections:host"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon Connect	• Flujo de contacto • Asociación de integración • Queue • Quick Connect • Perfil de enrutamiento • Usuario	• `"connect:instance/contact-flow"` • `"connect:instance/integration-association"` • `"connect:instance/queue"` • `"connect:instance/transfer-destination"` • `"connect:instance/routing-profile"` • `"connect:instance/agent"`
Amazon Connect Wisdom	• Asistente • Asociación • Contenidos • Base de conocimientos • Sesión	• `"wisdom:assistant"` • `"wisdom:association"` • `"wisdom:content"` • `"wisdom:knowledge-base"` • `"wisdom:session"`
AWS Database Migration Service	• Todos • Punto de conexión • ES • Rep. • Subgrp • Tarea	• `"dms:*"` • `"dms:endpoint"` • `"dms:es"` • `"dms:rep"` • `"dms:subgrp"` • `"dms:task"`
Amazon Data Lifecycle Manager	• Política	• `"dlm:policy"`
AWS Direct Connect	• Todos • Dxcon • Dxlag • Dxvif	• `"directconnect:*"` • `"directconnect:dxcon"` • `"directconnect:dxlag"` • `"directconnect:dxvif"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon DynamoDB	• Todos • Tabla	• `"dynamodb:*"` • `"dynamodb:table"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon EC2	• Reserva de capacidad • Punto de conexión de Client VPN • Puerta de enlace de cliente • Opciones de DHCP • Elastic IP • Flota • Imagen FPGA • Reserva de host • Imagen • instancia • Puerta de enlace de Internet • Plantilla de inicializ ación • Puerta de enlace de NAT • ACL de red • Interfaz de red • instancias reservadas • Tabla de enrutamie nto • Grupo de seguridad • Instantánea • Solicitud de instancias de spot • Subred	• `"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-instances-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"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
	• 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 conexión de VPC • Interconexión de VPC • Conexión de VPN • Puerta de enlace de VPN	• `"ec2:vpn-connection"` • `"ec2:vpn-gateway"`
Papelera de reciclaje Amazon EC2	• Regla	• `"rbin:rule"`
Amazon Elastic Container Registry	• Repositorio	• `"ecr:repository"`
AWS Elastic Beanstalk	• Aplicación • Versión de la aplicación • Plantilla de configuración • Plataforma	• `"elasticbeanstalk:application"` • `"elasticbeanstalk:applicationversion"` • `"elasticbeanstalk:configurationtemplate"` • `"elasticbeanstalk:platform"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
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 Elastic Inference	• Acelerador	• `"elastic-inference:elastic-inference-accelerator"`
Amazon Elastic Kubernetes Service	• Clúster	• `"eks:cluster"`
Amazon Elastic Search	• Dominio	• `"es:domain"`
Amazon EMR	• Clúster • Editor	• `"elasticmapreduce:cluster"` • `"elasticmapreduce:editor"`
Amazon EMR sin servidor	• Aplicación	• `"emr-serverless:applications"`
AWS Resolución de la entidad	• Flujo de trabajo de coincidencias • Mapeo de esquemas	• `"entityresolution:matchingworkflow"` • `"entityresolution:schemamapping"`
Amazon ElastiCache	• Clúster	• `"elasticache:cluster"`
Amazon EventBridge	• Todos • Event bus • Regla	• `"events:*"` • `"events:event-bus"` • `"events:rule"`
Amazon EventBridge Pipes	• Canalización	• `"pipes:pipe"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon EventBridge Scheduler	• Grupo de horarios	• `"scheduler:schedule-group"`
Amazon Fraud Detector	• Detector • Versión de detector • Modelo • Regla • Variable	• `"frauddetector:detector"` • `"frauddetector:detector-version"` • `"frauddetector:model"` • `"frauddetector:rule"` • `"frauddetector:variable"`
Amazon Global Accelerator	• Acelerador	• `"globalaccelerator:accelerator"`
Elastic Load Balancing	• Todos • Equilibrador de carga • Grupo de destino	• `"elasticloadbalancing:*"` • `"elasticloadbalancing:loadbalancer"` • `"elasticloadbalancing:targetgroup"`
Amazon FSx	• Todos • Copia de seguridad • Sistema de archivos	• `"fsx:*"` • `"fsx:backup"` • `"fsx:file-system"`
Amazon GuardDuty	• Detector • Filtro • Conjunto de IP • Conjunto de inteligencia sobre amenazas	• `"guardduty:detector"` • `"guardduty:detector/filter"` • `"guardduty:detector/ipset"` • `"guardduty:detector/threatintelset"`
AWS HealthLake	• Almacén de datos	• `"healthlake:datastore  "`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
AWS HealthOmics	• Almacén de anotaciones • Versión del almacén de anotaciones • Tienda de referencia • Referencia • Ejecute • Grupo de ejecución • Tienda de secuencias • Conjunto de lectura • Tienda de variantes • Flujo de trabajo	• `"omics:annotationStore"` • `"omics:annotationStore/version"` • `"omics:referenceStore"` • `"omics:referenceStore/reference"` • `"omics:run"` • `"omics:runGroup"` • `"omics:sequenceStore"` • `"omics:sequenceStore/readSet"` • `"omics:variantStore"` • `"omics:workflow"`
Amazon Inspector	• Filtro	• `"inspector2:filter "`
AWS Identity and Access Management	• Perfil de instancia • MFA • Proveedor OIDC • Política • Proveedor SAML • Certificado de servidor	• `"iam:instance-profile"` • `"iam:mfa"` • `"iam:oidc-provider"` • `"iam:policy"` • `"iam:saml-provider"` • `"iam:server-certificate"`
AWS IoT Analytics	• Todos • Canal • Conjunto de datos • Almacén de datos • Canalización	• `"iotanalytics:*"` • `"iotanalytics:channel"` • `"iotanalytics:dataset"` • `"iotanalytics:datastore"` • `"iotanalytics:pipeline"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
AWS IoT Events	• Todos • Modelo de detector • Entrada	• `"iotevents:*"` • `"iotevents:detectorModel"` • `"iotevents:input"`
AWS IoT Fleet Hub	• Aplicación	• `"iotfleethub:application"`
AWS IoT SiteWise	• activo • Modelo de recurso	• `"iotsitewise:asset"` • `"iotsitewise:asset-model  "`
AWS IoT Greengrass	• Implementación masiva • Definición del conector • Definición del núcleo • Definición del dispositivo • Definición de la función • Definición del registrador • Definición del recurso • Definición de la suscripción	• `"greengrass:bulk"` • `"greengrass:connectorsDefinition"` • `"greengrass:coresDefinition"` • `"greengrass:devicesDefinition"` • `"greengrass:functionsDefinition"` • `"greengrass:loggersDefinition"` • `"greengrass:resourcesDefinition"` • `"greengrass:subscriptionsDefinition"`
AWS Key Management Service	• Todos • Clave	• `"kms:*"` • `"kms:key"`
Amazon Kinesis	• Todos • Aplicación	• `"kinesisanalytics:*"` • `"kinesisanalytics:application"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon Data Firehose	• Todos • Flujo de entrega	• `"firehose:*"` • `"firehose:deliverystream"`
AWS Lambda	• Todos • Función	• `"lambda:*"` • `"lambda:function"`
Amazon Macie	• Identificador de datos personalizado	• `"macie2:custom-data-identifier"`
Amazon MediaStore	• Contenedor	• `"mediastore:container"`
Amazon MQ	• Broker • Configuración	• `"mq:broker"` • `"mq:configuration"`
Amazon Network Firewall	• Firewall • Directiva de firewall • Grupo de reglas con estado • Grupo de reglas sin estado	• `"network-firewall:firewall"` • `"network-firewall:firewall-policy"` • `"network-firewall:stateful-rulegroup"` • `"network-firewall:stateless-rulegroup"`
Amazon OpenSearch Serverless	• Recopilación	• `"aoss:collection"`
AWS Organizations	• Cuenta • Organizational Unit • Política • Raíz	• `"organizations:account"` • `"organizations:ou"` • `"organizations:policy"` • `"organizations:root"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
SMS Voice V2 de Amazon Pinpoint	• Conjunto de configuración • Lista de exclusión • Número de teléfono • Grupo • ID de remitente	• `"sms-voice:configuration-set"` • `"sms-voice:opt-out-list"` • `"sms-voice:phone-number"` • `"sms-voice:pool"` • `"sms-voice:sender-id"`
Amazon RDS	• Grupo de parámetros del clúster • Punto de conexión de clúster • Suscripción a eventos • Grupo de opciones de base de datos • DB Parameter Group (Grupo de parámetros de base de datos) • Proxy de base de datos • Punto de conexión de proxy de base de datos • Instancia de base de datos reservada • Grupo de seguridad de base de datos • Grupo de subred de base de datos • Grupo de destino	• `"rds:cluster-pg"` • `"rds:cluster-endpoint"` • `"rds:es"` • `"rds:og"` • `"rds:pg"` • `"rds:db-proxy"` • `"rds:db-proxy-endpoint"` • `"rds:ri"` • `"rds:secgrp"` • `"rds:subgrp"` • `"rds:target-group"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
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 (Grupo de subredes)	• `"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"`
Amazon Redshift sin servidor	• Espacio de nombres • Grupo de trabajo	• `"redshift-serverless:namespace"` • `"redshift-serverless:workgroup"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
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"`
Amazon S3	• Bucket • Storage Lens	• `"s3:bucket"` • `"s3:storage-lens"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon SageMaker	• Config. de imagen de aplicación • Artefacto • Context • Trabajo de entrenamiento • Trabajo de procesamiento • Grupo de paquetes de modelos • UI de tareas humanas • Paquete de modelos • Acción • Canalización • Experimento • Definición del flujo • Proyecto	• `"sagemaker:app-image-config"` • `"sagemaker:artifact"` • `"sagemaker:context"` • `"sagemaker:training-job"` • `"sagemaker:processing-job "` • `"sagemaker:model-package-group"` • `"sagemaker:human-task-ui"` • `"sagemaker:model-package"` • `"sagemaker:action"` • `"sagemaker:pipeline"` • `"sagemaker:experiment"` • `"sagemaker:flow-definition"` • `"sagemaker:project"`
AWS Secrets Manager	• Todos • secreta	• `"secretsmanager:*"` • `"secretsmanager:secret"`
AWS Lago de seguridad	• Lago de datos • Suscriptor	• `"securitylake:data-lake"` • `"securitylake:subscriber"`
AWS Service Catalog	• Aplicación • Grupo de atributos • Portfolio • Producto	• `"servicecatalog:applications"` • `"servicecatalog:attribute-groups "` • `"catalog:portfolio "` • `"catalog:product "`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon Simple Notification Service (SNS)	• Tema	• `"sns:topic"`
Amazon Simple Queue Service (SQS)	• Queue	• `"sqs:queue"`
Amazon States Language	• Todos • Actividad • State Machine (Máquina de estado)	• `"states:*"` • `"states:activity "` • `"states:stateMachine  "`
AWS Step Functions	• Actividad	• `"states:activity"`
AWS Storage Gateway	• Todos • Puerta de enlace • Share • Cinta • Volumen	• `"storagegateway:*"` • `"storagegateway:gateway"` • `"storagegateway:share"` • `"storagegateway:tape"` • `"storagegateway:gateway/volume"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
AWS Systems Manager	• Asociación • Ejecución de automatización • Documento • Maintenance Window (Período de mantenimiento) • Instancia administrada • Elemento de operaciones • Línea de base de revisiones • Sesión • Contactos	• `"ssm:association"` • `"ssm:automation-execution"` • `"ssm:document"` • `"ssm:maintenancewindow"` • `"ssm:managed-instance"` • `"ssm:opsitem"` • `"ssm:patchbaseline"` • `"ssm:session"` • `"ssm-contacts:contact"`
AWS Transfer Family	• Server • Usuario • Flujo de trabajo	• `"transfer:server"` • `"transfer:user"` • `"transfer:workflow"`
Amazon Well-Architected	• Carga de trabajo	• `"wellarchitected:workload"`
AWS Wickr	• Network	• `"wickr:network"`

Nombre del servicio	Tipo de recurso	Sintaxis JSON
Amazon WorkSpaces	• Todos • Directorio • WorkSpace • WorkSpaces paquete • WorkSpaces imagen • WorkSpaces grupo IP	• `"workspaces:*"` • `"workspaces:directory"` • `"workspaces:workspace"` • `"workspaces:workspacebundle"` • `"workspaces:workspaceimage"` • `"workspaces:workspaceipgroup"`
Amazon WorkLink	• Flota	• `"worklink:fleet"`

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 explicación completa de esa sintaxis, consulte Descripción de la herencia de políticas de administración. Este tema se centra en aplicar esa sintaxis general a los requisitos específicos del tipo de política de etiqueta.

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 política 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 política no distingue entre mayúsculas y minúsculas.

  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 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.
- - Puede utilizar el comodín `*` en los valores de etiquetas y en los campos `enforced_for`.
  - Puede utilizar solo un comodín por valor de etiquetas. 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.

    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 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 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. 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 las mayúsculas y minúsculas de la 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.

Política A: política 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.

Siguiente paso: 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`.

Política B: Política 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 de administración.

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 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. Además, la opción `enforced_for` realmente impide que las cuentas afectadas etiqueten solo tablas de Amazon DynamoDB con la etiqueta `Color`.

```
{
    "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
Región Este de EE. UU. (Norte de Virginia)[1]	**us-east-1**
Región del este de EE. UU. (Ohio)	us-east-2
Región del oeste de EE. UU. (Norte de California)	us-west-1
Región del oeste de EE. UU. (Oregón)	us-west-2
Africa (Cape Town) Region[2]	af-south-1
Región Asia Pacífico (Hong Kong)[2]	ap-east-1
Región de Asia-Pacífico (Bombay)	ap-south-1
Asia Pacífico (Hyderabad) [2]	ap-south-2
Región de Asia-Pacífico (Tokio)	ap-northeast-1
Región de Asia-Pacífico (Seúl)	ap-northeast-2
Región Asia-Pacífico (Osaka)	ap-northeast-3
Región de Asia-Pacífico (Singapur)	ap-southeast-1
Región de Asia-Pacífico (Sídney)	ap-southeast-2
Región de Asia Pacífico (Yakarta) [2]	ap-southeast-3
Asia Pacífico (Melbourne) [2]	ap-southeast-4
Canadá Oeste (Calgary) [2]	ca-west-1
Región de Canadá (centro)	ca-central-1
Región de Europa (Fráncfort)	eu-central-1
Región de Europa (Zúrich) [2]	eu-central-2
Europe (Milan) Region[2]	eu-south-1

Nombre de la región	Parámetro de la región
Europa (España) [2]	`eu-south-2`
Región de Europa (Irlanda)	`eu-west-1`
Región de Europa (Londres)	`eu-west-2`
Región de Europa (París)	`eu-west-3`
Región Europa (Estocolmo)	`eu-north-1`
Región de Medio Oriente (EAU) [2]	`me-central-1`
Middle East (Bahrain) Region[2]	`me-south-1`
Región de América del Sur (São Paulo)	`sa-east-1`
Israel (Tel Aviv) [2]	`il-central-1`

[1]Debe especificar la región **`us-east-1`** 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 región **`us-east-1`** cuando llame a las siguientes operaciones de la API de etiquetado de grupos de recursos que forman parte de la característica de políticas de etiquetas:

- DescribeReportCreation
- GetComplianceSummary
- GetResources
- StartReportCreation

> **Note**
>
> Para evaluar la conformidad de políticas de etiquetas en toda la organización, también debe tener acceso a un bucket de Amazon S3 en la región EE. UU. Este (Norte de Virginia) para el almacenamiento de informes. Para obtener más información, consulte la política de depósitos de Amazon S3 para el almacenamiento de informes en la Guía del usuario de Tagging AWS Resources.

²Estas regiones deben estar habilitadas manualmente. Para obtener más información sobre cómo habilitar y deshabilitar Regiones de AWS, consulte Especificar qué cuenta puede usar Regiones de AWS su cuenta en la Guía de referencia de administración deAWS cuentas. La consola Resource Groups no está disponible en estas regiones.

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. Los SCP ofrecen un control central sobre los permisos máximos disponibles para los usuarios de IAM y las funciones de IAM en 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. 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.

Los SCP no conceden permisos a los usuarios ni a las funciones de IAM en su organización. Una SCP no concede permisos. Un SCP define una barrera de permisos, o establece límites, a las acciones que los usuarios de IAM y las funciones de IAM de su organización pueden realizar. Para conceder los permisos, el administrador debe adjuntar políticas para controlar el acceso, como las políticas basadas en la identidad que se asocian a los usuarios y las funciones de IAM, y las políticas basadas en los recursos que se asocian a los recursos de sus cuentas. Los permisos efectivos son la intersección lógica entre lo que permite el SCP y lo que permiten las políticas basadas en la identidad y los recursos.

> **Important**
>
> Las SCP no afectan a los usuarios ni a los roles de la cuenta de administración. Afectan solo a las cuentas miembro de su organización.

Temas en esta página

- Comprobación de los efectos de las políticas SCP
- Tamaño máximo de las políticas SCP
- Adjuntar las SCP a diferentes niveles de la organización
- Efectos de las SCP en los permisos
- Uso de datos de acceso para mejorar las políticas SCP
- Tareas y entidades no restringidas por SCP
- Creación, actualización y eliminación de políticas de control de servicios
- Asociar y desasociar políticas de control de servicios
- Evaluación de SCP
- Sintaxis de SCP
- Ejemplos de políticas de control de servicios

Comprobación de los efectos de las políticas SCP

AWS recomienda encarecidamente que no asocie los SCP a la raíz de su organización sin comprobar exhaustivamente el impacto que la política tiene 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 utilizará un servicio es examinar los datos a los que tuvo acceso el servicio por última vez en IAM. Otra forma consiste en registrar el uso del servicio AWS CloudTrail a nivel de la API.

> **Note**
>
> No debes eliminar la AWSAccess política completa a menos que la modifiques o la sustituyas por una política independiente con acciones permitidas; de lo contrario, todas AWS las acciones de las cuentas de los miembros fallarán.

Tamaño máximo de las políticas SCP

Todos los caracteres de la SCP se contabilizan para calcular su tamaño máximo. 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.

Adjuntar las SCP a diferentes niveles de la organización

Para obtener una explicación detallada de cómo funcionan las SCP, consulte Evaluación de SCP

Efectos de las SCP en los permisos

Los SCP son similares a las políticas de permisos AWS Identity and Access Management (IAM) y utilizan prácticamente la misma sintaxis. Sin embargo, una SCP nunca concede permisos. En cambio, los SCP son políticas de JSON que especifican los permisos máximos para los usuarios de IAM y las funciones de IAM en su organización. Para obtener más información, consulte Lógica de evaluación de políticas en la Guía del usuario IAM.

- Las SCP solo afectan a los usuarios y roles IAM administrados por 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 que no pertenecen a la organización. La cuenta A tiene asociada una SCP. Esa SCP no se aplica a los usuarios externos de la cuenta B. La SCP 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 en las cuentas miembro, incluido el usuario raíz de la cuenta de 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.

- Las SCP afectan solo a las cuentas miembro de su organización. No tienen ningún efecto en los usuarios ni en los 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 de control de servicios correspondientes permitan todos los servicios y todas las acciones.
- Si un usuario o rol 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 rol puede realizar dicha acción.
- Si un usuario o rol 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 rol 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.
- Las SCP no afectan a cualquier rol vinculado al servicio. Los roles vinculados a los servicios permiten que otros AWS servicios se integren con los SCP AWS Organizations y no pueden restringirlos.
- Al deshabilitar el tipo de política SCP en una raíz, todos los SCP se separan automáticamente de todas las entidades de esa raíz. AWS Organizations AWS Organizations las entidades 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 (característica avanzada de IAM) como una SCP, entonces ese límite, la SCP y la política basada en identidad deberán permitir la acción.

Uso de datos de acceso para mejorar las políticas SCP

Al iniciar sesión con las credenciales de la cuenta de administración, puede ver los datos del servicio al que se accedió por última vez para una AWS Organizations entidad o política en la AWS Organizationssección de la consola de IAM. También puedes usar AWS Command Line Interface (AWS CLI) o la AWS API de IAM para recuperar los datos del servicio a los que se accedió por última

vez. Estos datos incluyen información sobre los servicios permitidos a los que los usuarios y roles de IAM de una AWS Organizations cuenta intentaron acceder por última vez 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 un SCP de lista de denegación que prohíba el acceso a tres AWS servicios. Todos los servicios que no figuren en la instrucción `Deny` de la SCP se permiten. Los datos del servicio al que se accedió por última vez en IAM indican qué AWS servicios están permitidos por el SCP pero que 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

Usted no puede utilizar SCP para restringir las siguientes tareas:

- Cualquier acción realizada por la cuenta de administración
- Cualquier acción realizada mediante permisos que adjuntos a un rol vinculado al servicio
- Registrarse en el plan Enterprise Support como usuario raíz
- Cambie el nivel AWS de soporte como usuario root
- Proporcione una funcionalidad de firmante confiable para el contenido CloudFront privado
- Configurar DNS inverso para un servidor de correo electrónico de Amazon Lightsail y una instancia de Amazon EC2 como usuario raíz
- Tareas en algunos servicios AWS relacionados:
  - Alexa Top Sites
  - Alexa Web Information Service
  - Amazon Mechanical Turk
  - API de marketing de productos de Amazon

Creación, actualización y eliminación de políticas de control de servicios

Cuando inicia sesión con la cuenta maestra de su organización, puede crear y actualizar políticas de control de servicios (SCP). 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 las SCP es usar una estrategia de "lista de bloqueos" donde todas las acciones están implícitamente permitidas excepto aquellas acciones que desea bloquear mediante la creación de sentencias que deniegan el acceso. Con las instrucciones de denegación, puede especificar recursos y condiciones para la instrucción y utilizar el elemento NotAction. 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 Evaluación de SCP.

> **Tip**
>
> Puede utilizar los datos del último acceso al servicio de IAM como punto de datos para actualizar las SCP para restringir el acceso únicamente a los servicios de AWS que necesite. Para obtener más información, consulte Visualización de los datos del último acceso al servicio de Organizations en la Guía del usuario IAM.

En este tema:

- Después de habilitar las políticas de control de servicios de su organización, puede crear una política.
- Cuando cambien sus requisitos de SCP, puede actualizar una política existente.
- Cuando ya no necesite una política y después de desconectarla de todas las unidades organizativas (OU) y cuentas, puede eliminarla.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de control de servicios, seleccione Crear política.
3. En la página Create new service control policy (Crear política de control de servicios nueva), introduzca un Policy name (Nombre de política) y una Description (Descripción) opcional para la política.
4. (Opcional) Agregue una o varias etiquetas seleccionando Añadir etiqueta y a 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.

   > **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 que deniega el acceso o lo permite. Para obtener más información, consulte Evaluación de SCP. Si usa instrucciones de `Deny`, dispone de un control adicional, ya que puede restringir el acceso a recursos específicos, definir condiciones que marcan cuándo se aplicará la SCP y utilizar el elemento NotAction. Para obtener más detalles acerca de la sintaxis, consulte Sintaxis de SCP.

   Para agregar una instrucción que deniega el acceso:

   a. En el panel derecho Edición de declaraciones del editor, en Agregar acciones, seleccione un servicio de AWS.

      A medida que elige opciones a la derecha, el editor JSON se actualiza para mostrar la política de JSON correspondiente a la izquierda.

b. Después de seleccionar un servicio, se abre una lista que contiene las acciones disponibles para ese servicio. Puede elegir Todas las acciones o elegir 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, a continuación, también vuelve y también selecciona Todas 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 agregar acciones de servicios adicionales, puede elegir Todos los servicios al principio del casillero de la Instrucción y, a continuación, repita los dos pasos anteriores según sea necesario.

d. Especifique los recursos que hay que incluir en la instrucción.

   - Junto a Agregar un recurso, elija Agregar.
   - En el navegador Add resource (Agregar recurso), elija de la lista el servicio cuyos recursos desea controlar. Puede seleccionar entre solo los servicios que ha seleccionado en el paso anterior.
   - Bajo Tipo de recurso, elija el tipo de recurso que desea controlar.
   - Por último, complete el nombre de recurso de Amazon (ARN) en ARN de recurso para 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 eligiendo Add resource (Agregar recurso). El elemento `Resource` en el JSON refleja sus adiciones o cambios. El elemento de Recurso es obligatorio.

> **Tip**
>
> Si desea especificar todos los recursos para el servicio seleccionado, elija la opción Todos los recursos en la lista, o edite la opción `Resource` directamente en el JSON para leer `"Resource":"*"`.

e. (Opcional) Para especificar las condiciones que determinan cuándo una declaración de política está en vigor, junto a Agregar condición, elija Agregar.

- Clave de condición— En la lista puede elegir cualquier clave de condición que esté disponible para todos los servicios AWS (por ejemplo,`aws:SourceIp`) o una clave específica de servicio para solo uno de los servicios que ha seleccionado para esta instrucción.
- Calificador— (Opcional) Si proporciona varios valores para la condición (dependiendo de la clave de condición especificada), puede especificar un Calificador para probar solicitudes con los valores.
  - Valor predeterminado: prueba un valor único de la solicitud con el valor de la clave de condición de la política. La condición es verdadera 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 es verdadera 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 si al menos uno de los valores de solicitud coincide con al menos uno de los valores 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 en una solicitud — Cuando la solicitud puede tener varios valores, esta opción prueba si todos de los valores de solicitud coinciden con un valor de clave de condición de 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.
- Operador — El operador especifica 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, la clave de condición global `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 la prueba `Null`, puede elegir la opción IfExists.

- 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, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

f. (Opcional) Para usar el elemento `NotAction` para denegar el acceso a todas las acciones excepto las especificadas, sustituya `Action` en el panel izquierdo con `NotAction`, justo después de `"Effect": "Deny",`. Para obtener más información, consulte Elementos de la política de JSON de IAM: NotAction en la Guía del usuario de IAM.

6. Para agregar una instrucción que permita el acceso:

a. En el editor JSON de la izquierda, cambie la línea `"Effect": "Deny"` a `"Effect": "Allow"`.

A medida que elige opciones a la derecha, el editor JSON se actualiza para mostrar la política de JSON correspondiente a la izquierda.

b. Después de seleccionar un servicio, se abre una lista que contiene las acciones disponibles para ese servicio. Puede elegir Todas las acciones o 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, a continuación, también vuelve y también selecciona Todas 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 agregar acciones de servicios adicionales, puede elegir Todos los servicios al principio del casillero de la Instrucción y, a continuación, repita los dos pasos anteriores según sea necesario.

7. (Opcional) Para agregar otra instrucción a la política, elija Add statement (Añadir instrucción) y 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.

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 ejemplo siguiente se presupone que dispone de un archivo denominado `Deny-IAM.json` con el texto de la política JSON. 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\":[\"*\"]}]}"
```

```
    }
}
```

- SDK de AWS: CreatePolicy

> **Note**
>
> Las SCP no se aplican en la cuenta de administración y en determinadas situaciones. Para obtener más información, consulte Tareas y entidades no restringidas por SCP.

Actualización de una SCP

Puede cambiar el nombre o cambiar el contenido de una política iniciando sesión en la cuenta de administración de su organización. 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de control de servicios, elija el nombre de la política que desea actualizar.
3. En la página de detalles de la política, elija Editar política.
4. Realice una de las siguientes modificaciones, o todas:

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

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: update-policy

  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 ejemplo siguiente 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 política del SCP especificando un archivo que contiene el nuevo texto de política 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\":[\"*
\"]}]}"
    }
}
```

- SDK de AWS: UpdatePolicy

Para obtener más información

Para obtener más información sobre la creación de SCP, consulte los temas siguientes:

- Ejemplos de políticas de control de servicios
- Sintaxis de SCP

Edición de etiquetas adjuntas a una SCP

Cuando inicie sesión en la cuenta de administración de su organización, puede agregar o quitar las etiquetas adjuntas a una SCP. Para obtener más información acerca del etiquetado, consulte Etiquetado de recursos de AWS Organizations.

Permisos mínimos

Para editar las etiquetas adjuntas a una SCP de su organización AWS, 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 una SCP

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de control de servicios, elija el nombre de la política con las etiquetas que desea editar.
3. En la página de detalles de la política, elija la pestaña Etiquetas y, a continuación, elija Administrar etiquetas.
4. Realice una de las siguientes modificaciones, o todas:
   - Para cambiar el valor de una etiqueta, ingrese un nuevo valor sobre el antiguo. 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 eligiendo Eliminar.
   - Agregue una nueva clave de etiqueta y valore el par. Seleccione Agregar etiqueta y, a continuación, introduzca el nuevo nombre de clave y el valor opcional en los cuadros proporcionados. Si deja el Valor en blanco, 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 una SCP

Puede utilizar uno de los comandos siguientes para editar las etiquetas adjuntas a una SCP:

- AWS CLI: tag-resource y untag-resource
- SDK de AWS:TagResource y UntagResource

Eliminación de una SCP

Cuando inicia sesión en la cuenta de administración de su organización, puede eliminar una política que ya no necesite en su organización.

Notas

- Para poder eliminar una política, primero debe desconectarla de todas las entidades asociadas.
- No puede eliminar ninguna SCP administrada por AWS, como la que se denomina `FullAWSAccess`.

Permisos mínimos

Para eliminar una SCP, necesita permiso para ejecutar la siguiente acción:

- `organizations:DeletePolicy`

AWS Management Console

Para eliminar SCP

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de control de servicios, elija el nombre de la SCP que desea eliminar.
3. Primero debe desconectar la política que desea eliminar de todos los nodos raíz, unidades organizativas y cuentas. Elija el icono Implementación, elija el botón de opción situado junto a cada nodo raíz, OU o cuenta que se muestra en la lista Implementación y, a continuación, elija Desconectar. En el cuadro de diálogo de confirmación, elija Desconectar. Repita hasta que elimine todos los destinos.
4. En la parte superior de la página, elija Eliminar.
5. En el cuadro de diálogo de confirmación, escriba el nombre de la política y, a continuación, elija Eliminar.

AWS CLI & AWS SDKs

Para eliminar SCP

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

- AWS CLI: delete-policy

  El siguiente ejemplo elimina la SCP especificada.

  ```
  $ aws organizations delete-policy \
      --policy-id p-i9j8k7l6m5
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- SDK de AWS:DeletePolicy

Asociar y desasociar 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 al nodo 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 elemento `Resource` en la misma declaración de política que incluye "*" o el Nombre de recurso de Amazon (ARN) de la política especificada y el ARN del nodo raíz, unidad organizativa o cuenta a la que desea adjuntar la política

AWS Management Console

Puede asociar una SCP navegando hasta la política o el nodo raíz, unidad organizativa o cuenta a la que desee adjuntar la política.

Para asociar una SCP navegando hasta el nodo raíz, unidad organizativa o cuenta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

2. En la página Cuentas de AWS, desplácese y luego marque la casilla de verificación situada junto al nodo raíz, unidad organizativa o cuenta a la que desea adjuntar 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 la pestaña Políticas, en la entrada de Políticas de control de servicios, elija Adjuntar.
4. Busque la política que desea y elija Asociar política.

   La lista de SCP asociadas en la pestaña Políticas se actualiza para incluir la nueva adición. El cambio en la política se hace efectivo de manera inmediata, afectando a los permisos y los roles de los usuarios IAM de la cuenta asociada o de todas las cuentas situadas bajo el nodo raíz o la unidad organizativa.

Para adjuntar una SCP navegando a la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de control de servicios elija el nombre de la política que desea adjuntar.
3. En la pestaña Objetivos, seleccione Adjuntar.
4. Elija el botón de opción situado junto al nodo 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 Asociar política.

   La lista de SCP asociadas en los Objetivos se actualiza para incluir la nueva adición. El cambio en la política se hace efectivo de manera inmediata, afectando a los permisos y los roles de los usuarios 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 el nodo raíz, unidad organizativa o cuenta

Puede utilizar uno de los comandos siguientes para asociar una SCP:

- AWS CLI: attach-policy

  En el ejemplo siguiente se adjunta una SCP a una unidad organizativa.

  ```
  $ aws organizations attach-policy \
      --policy-id p-i9j8k7l6m5 \
      --target-id ou-a1b2-f6g7h222
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS SDK: AttachPolicy

El cambio en la política se hace efectivo de manera inmediata, afectando a los permisos y los roles de los usuarios 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 desconectar una SCP del nodo raíz de la organización, unidad organizativa o cuenta a la que está asociada. Tras separar un SCP de una entidad, ese SCP ya no se aplica a los usuarios ni a las funciones de IAM que se hayan visto afectados por la entidad ahora separada. Para desasociar una SCP, siga los pasos que se describen a continuación.

> **Note**
>
> No puede separar la última SCP de una raíz, una unidad organizativa o una cuenta. Debe haber al menos una SCP adjunta a cada nodo raíz, unidad organizativa y cuenta en todo momento.

> **Permisos mínimos**
>
> Para desconectar una SCP del nodo raíz, unidad organizativa o cuenta, necesita permiso para ejecutar la siguiente acción:

- `organizations:DetachPolicy`

AWS Management Console

Puede desconectar una SCP navegando hasta la política o el nodo raíz, unidad organizativa o cuenta a la que desee desconectar la política.

Para desconectar una SCP navegando hasta el nodo raíz, unidad organizativa o cuenta a la que está adjunta

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS desplácese hasta el nodo raíz, unidad organizativa o cuenta de la que desea desconectar 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 del nodo raíz, unidad organizativa o cuenta.
3. En la pestaña Políticas, elija el botón de opción situado junto a la SCP que desea desconectar y, a continuación, elija Desconectar.
4. En el cuadro de diálogo de confirmación, elija Desconectar política.

   La lista de SCP asociadas se actualiza. El cambio de política que se origina al desconectar la 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 la cuenta o cuentas anteriormente asociadas situados bajo el nodo raíz de la organización o unidad organizativa anteriormente asociadas.

Para desconectar una SCP navegando a la política

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Políticas de control de servicios, elija el nombre de la política que desea desconectar de un nodo raíz, unidad organizativa o cuenta.

3. En la pestaña de Objetivos, elija el botón de opción situado junto al nodo raíz, unidad organizativa o cuenta de la que desea desconectar 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 Desasociar.
5. En el cuadro de diálogo de confirmación, elija Desconectar.

   La lista de SCP asociadas se actualiza. El cambio de política que se origina al desconectar la 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 la cuenta o cuentas anteriormente asociadas situados bajo el nodo raíz de la organización o unidad organizativa anteriormente asociadas.

AWS CLI & AWS SDKs

Para desconectar una SCP de un nodo raíz, una unidad organizativa o una 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
  ```

- AWS SDK: DetachPolicy

El cambio en la política se hace efectivo de manera inmediata, afectando a los permisos y los roles de los usuarios IAM de la cuenta asociada o de todas las cuentas situadas bajo el nodo raíz o la OU.

Evaluación de SCP

> **Note**
>
> La información de esta sección no se aplica a los tipos de políticas de administración, incluidas las políticas de exclusión de servicios de IA, las políticas de copia de seguridad o las políticas de etiqueta. Para obtener más información, consulte Descripción de la herencia de políticas de administración.

Dado que puede adjuntar varias políticas de control de servicios (SCP) en diferentes niveles en AWS Organizations, comprender cómo se evalúan las SCP puede ayudar a redactar SCP que produzcan el resultado correcto.

Temas

- Cómo funcionan las SCP con Allow
- ¿Cómo funcionan las SCP con denegación
- Estrategias para utilizar SCP

Cómo funcionan las SCP con Allow

Para que se conceda un permiso a una cuenta específica, debe haber una declaración **`Allow`** explícita en cada nivel, desde la raíz hasta cada unidad organizativa situada en la ruta directa a la cuenta (incluida la propia cuenta de destino). Por eso, cuando habilita las SCP, AWS Organizations adjunta una política de SCP de AWS administrada llamada FullAWSAccess que permite todos los servicios y acciones. Si esta política se elimina y no se reemplaza en ningún nivel de la organización, todas las OU y cuentas que estén por debajo de ese nivel quedarán bloqueadas y no podrán realizar acciones.

Por ejemplo, veamos la situación que se muestra en las figuras 1 y 2. Para permitir un permiso o un servicio en la cuenta B, la SCP que permita el permiso o el servicio debe estar vinculada a la raíz, a la unidad organizativa de producción y a la propia cuenta B.

La evaluación de las SCP sigue un modelo de denegación por defecto, lo que significa que se niegan todos los permisos que no estén explícitamente permitidos en las SCP. Si las SCP no contienen una declaración de autorización en ninguno de los niveles, como raíz, unidad organizativa de producción o cuenta B, se deniega el acceso.

Notas

- Una declaración de `Allow` en un SCP permite al elemento `Resource` para tener solo una entrada de `"*"`.
- Un registro `Allow` en una SCP no puede tener un elemento `Condition` en absoluto.

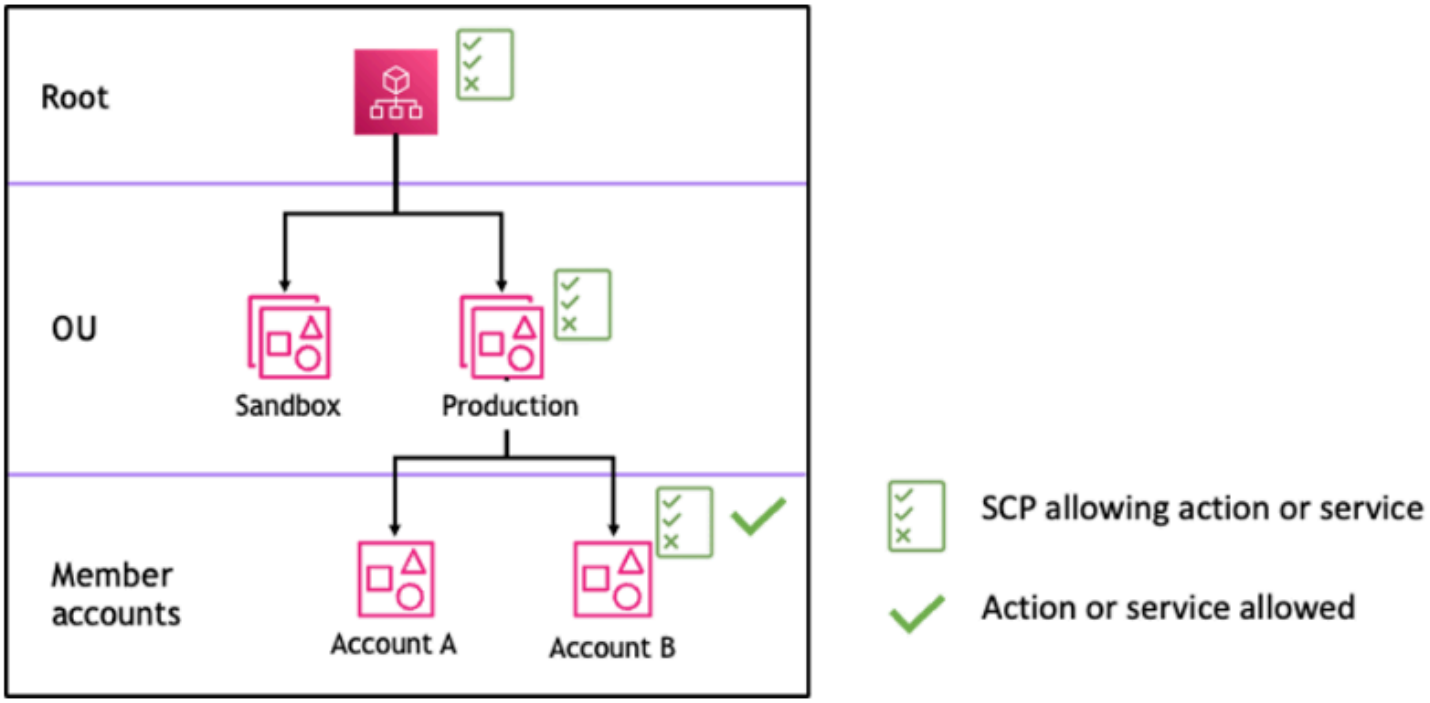


Figura 1: Ejemplo de estructura organizativa con una declaración *`Allow`* adjunta en la raíz, la OU de producción y la cuenta B

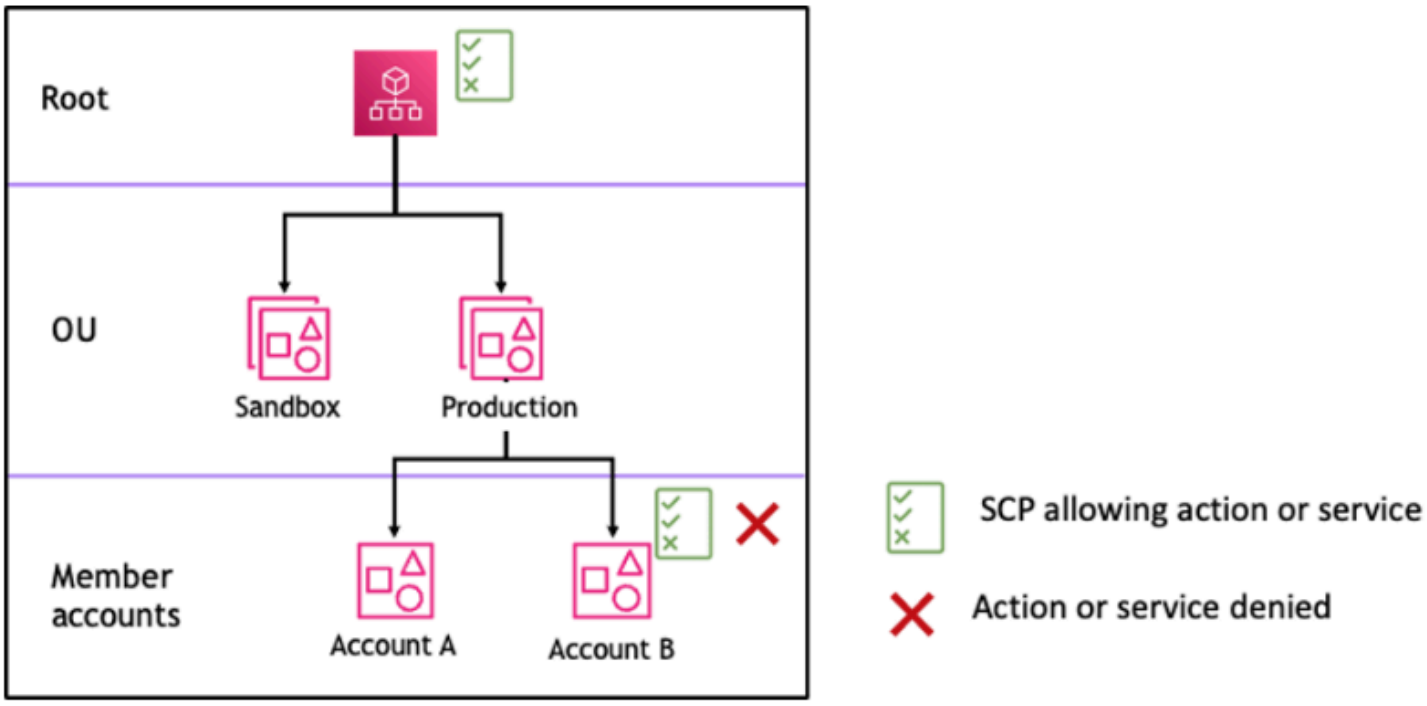


Figura 2: Ejemplo de estructura organizativa con una declaración *`Allow`* faltante en la OU de producción y su impacto en la cuenta B

¿Cómo funcionan las SCP con denegación

Si se niega un permiso para una cuenta específica, cualquier SCP desde la raíz hasta cada unidad organizativa situada en la ruta directa a la cuenta (incluida la propia cuenta de destino) puede denegar ese permiso.

Por ejemplo, supongamos que hay una SCP adjunta a la OU de producción que tiene una declaración `Deny` explícita especificada para un servicio determinado. Resulta que también hay otra SCP conectada a la raíz y a la cuenta B que permite explícitamente el acceso a ese mismo servicio, como se muestra en la figura 3. Como resultado, se negará el acceso al servicio tanto a la cuenta A como a la cuenta B, ya que se evalúa una política de denegación aplicable a cualquier nivel de la organización para todas las unidades organizativas y cuentas de los miembros que dependen de ella.

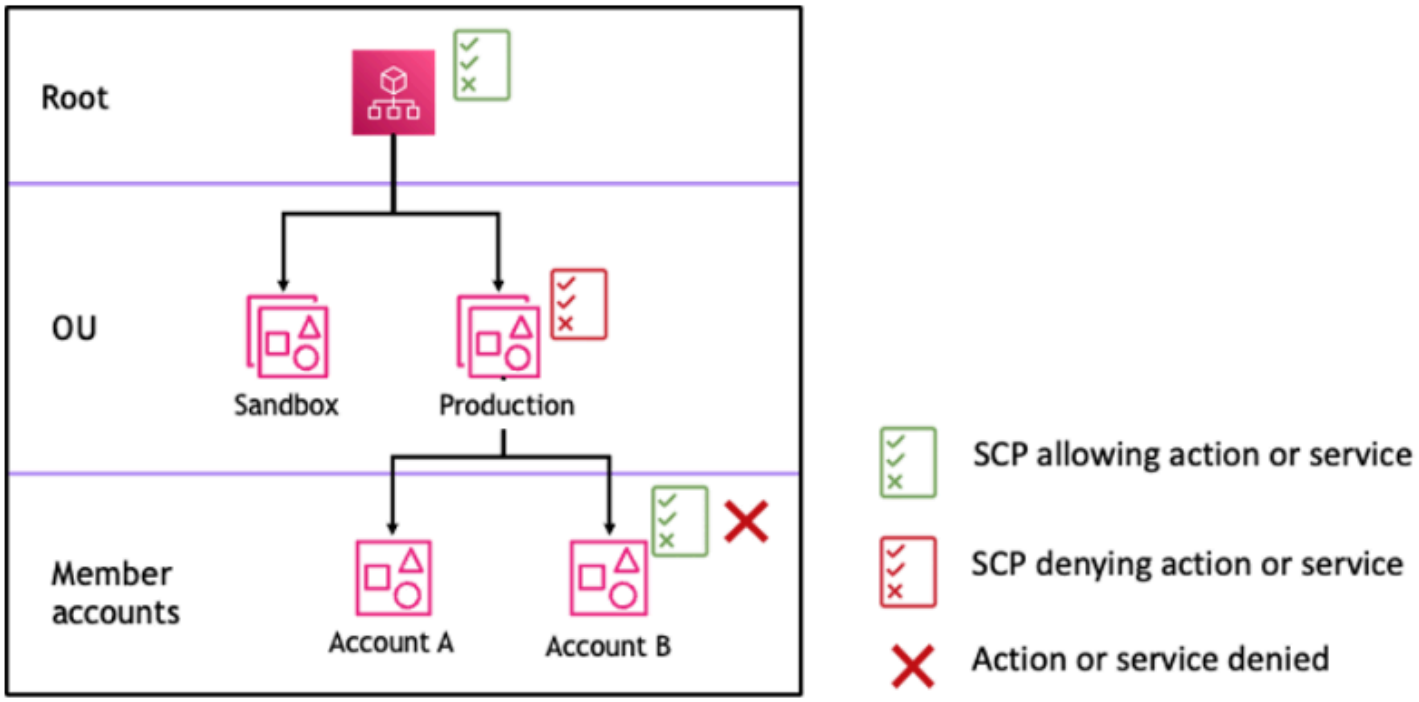


Figura 3: Ejemplo de estructura organizativa con una declaración *Deny* adjunta en la OU de producción y su impacto en la cuenta B

Estrategias para utilizar SCP

Al redactar las SCP, puede utilizar una combinación de declaraciones `Allow` y declaraciones `Deny` para permitir las acciones y servicios previstos en su organización. Las declaraciones `Deny` son una forma eficaz de implementar restricciones que deberían aplicarse a una parte más amplia de la organización o de la unidad organizativa, ya que, cuando se aplican a nivel raíz o a nivel de la unidad organizativa, afectan a todas las cuentas que dependen de ella.

Por ejemplo, puede implementar el uso de una política en Evitar que las cuentas de miembros dejen la organización. en el nivel raíz, que será efectiva para todas las cuentas de la organización. Las declaraciones de denegación también admiten un elemento de condición que puede ser útil para crear excepciones.

> **Tip**
>
> Puede utilizar los datos del último acceso al servicio de IAM para actualizar las SCP para restringir el acceso únicamente a los servicios de AWS que necesite. Para obtener más información, consulte Visualización de los datos del último acceso al servicio de Organizations en la Guía del usuario IAM.

AWS Organizations asocia una SCP administrada por AWS denominada FullAWSAccess a cada raíz, unidad organizativa y cuenta en el momento de su creación. Esta política permite todos los servicios y acciones. Puede sustituir FullAWSAccess por una política que permita solo un conjunto de servicios, de modo que no se permitan nuevos servicios de AWS a menos que se los permita explícitamente mediante la actualización de las SCP. Por ejemplo, si su organización solo quiere permitir el uso de un subconjunto de servicios en su entorno, puede usar una declaración `Allow` para permitir solo servicios específicos.

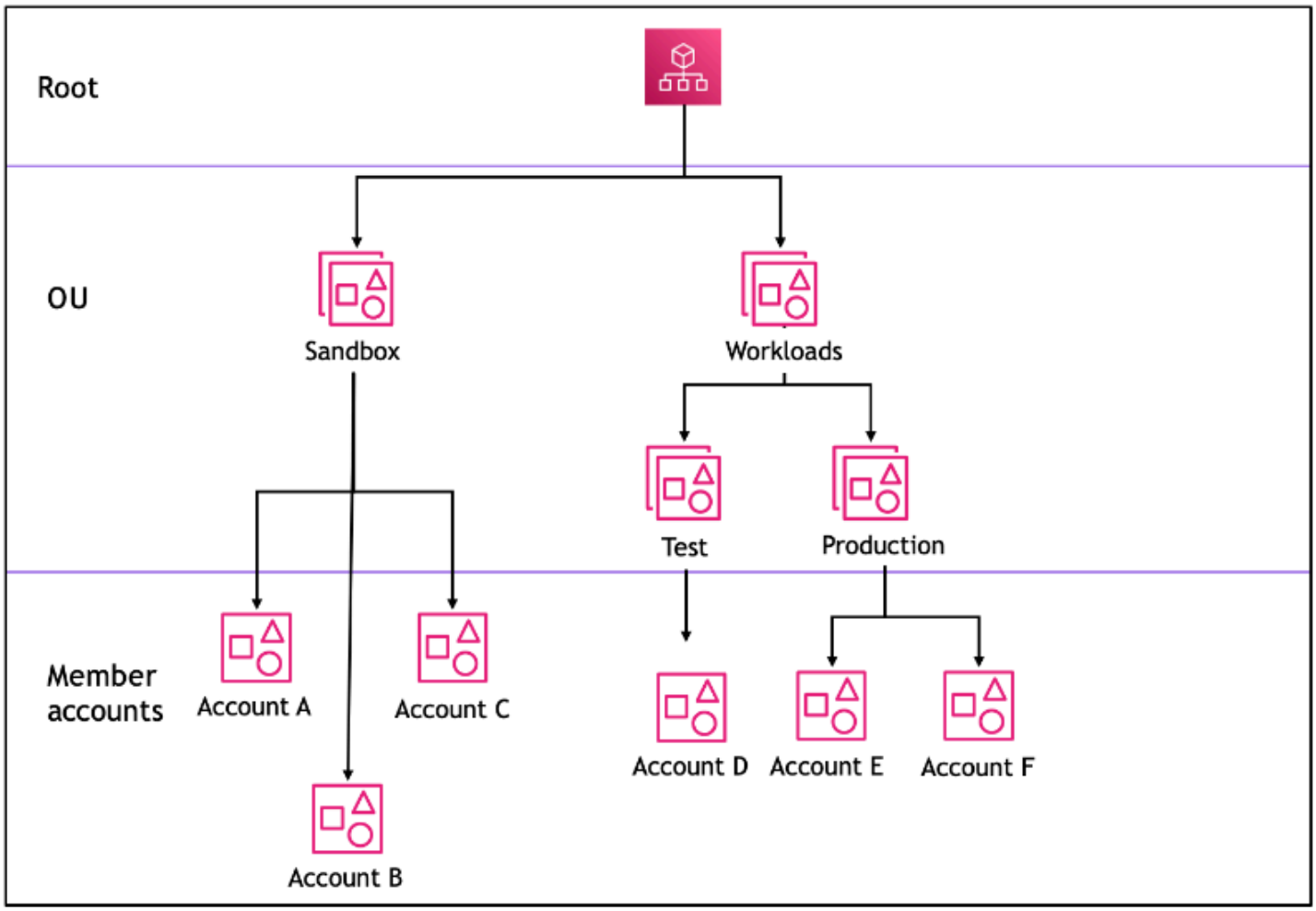
```
{
"Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        }
    ]
}
```

Una política que combine las dos declaraciones podría ser como la del ejemplo siguiente, que impide que las cuentas de los miembros salgan de la organización y permite el uso de los servicios AWS deseados. El administrador de la organización puede desasociar la política FullAWSAccess y asociar esta en su lugar.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*",
                "organizations:*"
            ],
            "Resource": "*"
        },
        {
```

```
            "Effect": "Deny",
            "Action":"organizations:LeaveOrganization",
            "Resource": "*"
        }
    ]
}
```

Ahora, analice el siguiente ejemplo de estructura organizativa para comprender cómo puede aplicar varias SCP en diferentes niveles de una organización.



En la tabla siguiente se muestran las políticas efectivas de la OU de un entorno aislado.

Escenario	SCP en la raíz	SCP en la OU de un entorno aislado	SCP en la cuenta A	Política resultante en la cuenta A	Política resultante en la cuenta B y la cuenta C
1	Acceso completo de AWS	Acceso completo de AWS + denegar el acceso a S3	Acceso completo de AWS + denegar el acceso a EC2	Sin acceso a S3 ni a EC2	Sin acceso a S3
2	Acceso completo de AWS	Permitir acceso de Amazon Elastic Compute Cloud (Amazon EC2)	Permitir el acceso a EC2	Solo permitir el acceso a EC2	Solo permitir el acceso a EC2
3	Denegar el acceso a S3	Permitir el acceso a S3	Acceso completo de AWS	Sin acceso a los servicios	Sin acceso a los servicios

En la tabla siguiente se muestran las políticas efectivas de la OU de cargas de trabajo.

Escenario	SCP en la raíz	SCP en OU de cargas de trabajo	SCP en OU de pruebas	Política resultante en la cuenta D	Políticas resultantes en OU de producción, cuenta E y cuenta F
1	Acceso completo de AWS	Acceso completo de AWS	Acceso completo de AWS + denegar el acceso a EC2	Sin acceso a EC2	Acceso completo de AWS
2	Acceso completo de AWS	Acceso completo de AWS	Permitir el acceso a EC2	Permitir el acceso a EC2	Acceso completo de AWS
3	Denegar el acceso a S3	Acceso completo de AWS	Permitir el acceso a S3	Sin acceso a los servicios	Sin acceso a los servicios

Sintaxis de SCP

Las políticas de control de servicios (SCP) utilizan una sintaxis similar a la que utilizan las políticas de permisos AWS Identity and Access Management (IAM) y las políticas basadas en recursos (como las políticas de bucket de Amazon S3). Para obtener más información sobre las políticas del IAM y su sintaxis, consulte Información general de las políticas del AM en la Guía del usuario 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. 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 (SCP).

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. En la columna Efectos admitidos se enumera los tipos de efectos que se pueden usar con cada elemento de política en las SCP.

Elemento	Finalidad	Efectos admitidos
Versión	Especifica las reglas de sintaxis del lenguaje que se utilizarán para procesar la política.	`Allow`, `Deny`
Instrucción	Sirve como contenedor de elementos de política. Una SCP puede contener varias	`Allow`, `Deny`

Elemento	Finalidad	Efectos admitidos
	instrucciones.	
Statement ID (Sid) (ID de instrucción)	(Opcional) Proporciona un nombre fácil de recordar para la instrucción.	`Allow`, `Deny`
Effect	Define si la instrucción SCP permite o deniega el acceso a los usuarios y roles IAM en una cuenta.	`Allow`, `Deny`
Action	Especifica el AWS servicio y las acciones que el SCP permite o deniega.	`Allow`, `Deny`

Elemento	Finalidad	Efectos admitidos
NotAction	Especifica el AWS servicio y las acciones que están exentos del SCP. Se utiliza en lugar del elemento `Action`.	`Deny`
Resource	Especifica los AWS recursos a los que se aplica el SCP.	`Deny`
Condición	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.

Elemento **`Version`**

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, consulte Elementos de la política de JSON de IAM: Versión en la Guía del usuario de IAM.

Elemento **`Statement`**

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 [ ]).

El siguiente ejemplo muestra una única instrucción que consta de los elementos `Effect`, `Action` y `Resource`.

```
    "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 el administrador de la cuenta puede delegar cualquier permiso, excepto los de Amazon Elastic Compute Cloud (Amazon EC2):

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "ec2:*",
            "Resource": "*"
```

```
        }
    ]
```

Para obtener más información, consulte Elementos de la política de JSON de IAM: Instrucción en la Guía 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, consulte Elementos de la política de JSON de IAM: ID en la Guía del usuario de IAM.

Elemento **`Effect`**

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, consulte Elemento de la política de JSON de IAM: Efecto en la Guía del usuario IAM.

`"Effect": "Allow"`

En el siguiente ejemplo se muestra una SCP con una instrucción que contiene un elemento `Effect` 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 usa la estrategia de permitidos (donde las políticas `FullAWSAccess` predeterminadas estén desasociadas y, por tanto, los permisos se deniegan implícitamente de forma predeterminada). El resultado es que la instrucción permite los permisos de Amazon S3 en cualquier cuenta asociada:

```
{
    "Statement": {
        "Effect": "Allow",
        "Action": "s3:*",
        "Resource": "*"
    }
}
```

Tenga en cuenta que aunque esta instrucción utiliza la misma palabra clave con el valor `Allow` que en una política de permisos de IAM, las SCP no conceden en realidad permisos de usuario. En su lugar, los SCP actúan como filtros que especifican los permisos máximos para los usuarios de IAM y las funciones de IAM en una organización. En el ejemplo anterior, aunque un usuario de la cuenta tuviera la política `AdministratorAccess` administrada asociada, esta SCP limita las acciones de todos los usuarios de la cuenta afectada a 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 Amazon EC2 si estas instancias 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.

Elementos **`Action`** y **`NotAction`**

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 `NotAction` elemento `Action` o es una lista (una matriz JSON) de cadenas que identifican AWS los servicios y las acciones que la sentencia 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 caracteres comodín tales como el asterisco (*) o el signo de interrogación de cierre (?) en una SCP:

- Utilice un asterisco (*) como carácter comodín como representación de 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".
- Utilice el carácter comodín del signo de interrogación de cierre (?) como representación de un carácter único.

> **Note**
>
> En una política SCP, el carácter comodín (*) o (?) 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 admiten en las políticas de permisos de los AWS Organizations SCP y de IAM, consulte las acciones, los recursos y las claves de condición de los AWS servicios en la Guía del usuario de IAM.

Para obtener más información, consulte Elementos de la política JSON de IAM: acción y Elementos de la política JSON de IAM: NotAction en la Guía 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. Este es un ejemplo de una lista de permitidos, y es útil cuando las políticas `Allow *` predeterminadas no se adjuntan para que, de forma predeterminada, los permisos sean denegados implícitamente. Si la política `Allow *` predeterminada sigue estando asociada al nodo raíz, unidad organizativa o cuenta a la que la siguiente política está asociada, entonces 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 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`**

El siguiente ejemplo muestra cómo se puede utilizar un `NotAction` elemento para excluir los AWS servicios 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 declaración, las cuentas afectadas se limitan a realizar las acciones especificadas Región de AWS, excepto cuando utilizan acciones de IAM.

Elemento **`Resource`**

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.

También puede utilizar caracteres comodín tales como el asterisco (*) o el signo de interrogación de cierre (?) en el elemento de recurso:

- Utilice un asterisco (*) como carácter comodín como representación de varias acciones que comparten parte de un nombre.
- Utilice el carácter comodín del signo de interrogación de cierre (?) como representación de un carácter único.

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 las cuentas de usuarios y roles IAM para que no puedan realizar cambios en un rol de IAM administrativo común creado en todas las cuentas de la organización.

Para obtener más información, consulte Elemento de la política de JSON de IAM: Resource en la Guía del usuario de IAM.

Elemento **`Condition`**

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, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

Elementos no compatibles

Los siguientes elementos no son compatibles con las SCP:

- `Principal`
- `NotPrincipal`
- `NotResource`

Ejemplos de políticas de control de servicios

Los ejemplos de políticas de control de servicios (SCP) que se muestran en este tema solo tienen fines informativos.

Antes de usar estos ejemplos

Antes de usar estos ejemplos de SCP en la organización, haga lo siguiente:

- Revise las SCP atentamente y personalícelas para ajustarlas a sus requisitos únicos.
- Pruebe a fondo las SCP en su entorno con los servicios AWS que utilice.

  Las políticas de ejemplo de esta sección demuestran la implementación y el uso de las SCP. Ellas no son destinadas a ser interpretadas como recomendaciones AWS oficiales 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 de servicios AWS a menos que agregue las excepciones necesarias a la política. 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 no deseado.
- Recuerde que una SCP afecta a todos los usuarios y roles e incluso al usuario raíz de todas las cuentas a las que se asocia.

Tip

Puede utilizar los datos del último acceso al servicio de IAM para actualizar las SCP para restringir el acceso únicamente a los servicios de AWS que necesite. Para obtener más información, consulte Visualización de los datos del último acceso al servicio de Organizations en la Guía del usuario IAM.

Cada una de las siguientes políticas es un ejemplo de una estrategia de política de lista de denegación . 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 asociando políticas de permisos de AWS Identity and Access Management (IAM) estándar adjuntar los 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
  - Denegar acceso a AWS en función de la Región de AWS solicitada
  - Evitar que los usuarios y los roles de IAM realicen determinados cambios
  - Impedir que los usuarios y roles de IAM realicen cambios especificados, con una excepción para un rol de administrador especificado
  - Requerir que MFA realice una acción de API
  - Bloquee el acceso al servicio del usuario raíz
  - Evitar que las cuentas de miembros dejen la organización.
- SCP de ejemplo para Amazon CloudWatch
  - Evitar que los usuarios deshabiliten CloudWatch o modifiquen su configuración
- SCP de ejemplo para AWS Config
  - Evitar que los usuarios deshabiliten AWS Config o cambien sus reglas
- Ejemplos de SCP para Amazon Elastic Compute Cloud (Amazon EC2)
  - Requerir que las instancias de Amazon EC2 usen un tipo específico
  - Impedir el lanzamiento de instancias de EC2 sin IMDSv2
  - Impedir la desactivación del cifrado predeterminado de Amazon EBS
- SCP de ejemplo para Amazon GuardDuty
  - Evitar que los usuarios deshabiliten GuardDuty o modifiquen su configuración
- SCP de ejemplo para AWS Resource Access Manager
  - Prevención de uso compartido externo
  - Permitir que determinadas cuentas compartan solo tipos de recursos especificados
  - Evitar compartir con organizaciones o unidades organizativas (OU)
  - Permitir el uso compartido solo con usuarios y roles de IAM especificados
- Ejemplos de SCP para el Controlador de recuperación de aplicaciones de Amazon Route 53
  - Impedir que los usuarios actualicen los estados de control de enrutamiento de Route 53 ARC

- Ejemplos de SCP para Amazon S3
  - Impedir la carga de objetos sin cifrar en Amazon S3
- Ejemplo de SCP para etiquetar recursos
  - Requerir una etiqueta en los recursos creados especificados
  - Impedir que las etiquetas se modifiquen excepto por entidades autorizadas
- Ejemplo de SCP para Amazon Virtual Private Cloud (Amazon VPC)
  - Evitar que los usuarios eliminen los registros de flujo de Amazon VPC
  - Evitar que cualquier VPC que no tenga acceso a Internet lo obtenga

Ejemplos generales

Denegar acceso a AWS en función de la Región de AWS solicitada

Este SCP deniega el acceso a cualquier operación fuera de las regiones especificadas. Reemplazar `eu-central-1` y `eu-west-1` con el 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.

> **Note**
>
> Para utilizar la SCP de denegación de región con AWS Control Tower, consulte Denegar acceso a AWS en función de la Región de AWS solicitada.

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 región `us-east-1`, deben quedar exentos de esta manera. Con una SCP estructurada 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

Es posible que este ejemplo no incluya todos los últimos servicios u operaciones globales de AWS. Sustituya la lista de servicios y operaciones por los servicios globales que las cuentas de la organización utilizan.

Sugerencia

Puede ver los últimos datos del servicio a los que se ha accedido en la consola de IAM para determinar qué servicios globales utiliza la organización. La pestaña Asesor de acceso de la página de detalles de un usuario, grupo o rol de IAM muestra los servicios de AWS que ha utilizado esa entidad, ordenados por el acceso más reciente.

Consideraciones

- AWS KMS y AWS Certificate Manager admiten puntos de enlace 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 de SCP. Un servicio global como Amazon CloudFront normalmente requiere acceso a AWS KMS y 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 STS es un servicio global y debe incluirse en la lista de exclusión de servicios globales. Sin embargo, puede habilitar AWS STS para utilizar los puntos de enlace de la 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 de SCP. Para obtener más información, consulte Administración de AWS STS en la 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:*",
                "route53-recovery-cluster:*",
                "route53-recovery-control-config:*",
                "route53-recovery-readiness:*",
                "s3:GetAccountPublic*",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints",
                "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 los roles de IAM realicen determinados cambios

Esta SCP restringe a las cuentas de usuarios y roles IAM para que no puedan realizar cambios en un rol de IAM especificado que ha creado 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 administrativo común de IAM creado en todas las cuentas de la organización, excepto para los administradores que utilizan un rol específico.

```
{
  "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 que MFA realice una acción de API

Utilice una SCP similar a la siguiente para requerir que la autenticación multifactor (MFA) esté habilitada antes de que un usuario o rol de IAM puedan realizar una acción. En este ejemplo, la acción consiste en detener una instancia de Amazon EC2.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyStopAndTerminateWhenMFAIsNotPresent",
      "Effect": "Deny",
      "Action": [
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": "*",
      "Condition": {"BoolIfExists": {"aws:MultiFactorAuthPresent": false}}
    }
  ]
}
```

Bloquee el acceso al servicio del usuario raíz

La siguiente política restringe todo acceso a las acciones especificadas para del usuario raíz de 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 de miembros dejen la organización.

La siguiente política bloquea el uso de la operación API `LeaveOrganization` para que los administradores de cuentas miembro no puedan eliminar sus cuentas de la organización.

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

SCP de ejemplo para Amazon CloudWatch

Ejemplos en esta categoría

- Evitar que los usuarios deshabiliten CloudWatch o modifiquen su configuración

Evitar que los usuarios deshabiliten CloudWatch o modifiquen su configuración

Un operador de CloudWatch de nivel inferior necesita monitorear paneles y alarmas. Sin embargo, el operador no debe poder eliminar ni cambiar ningún panel o alarma que pueden haber aplicado las personas mayores. Esta SCP evita que los usuarios o las funciones 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 para AWS Config

Ejemplos en esta categoría

- Evitar que los usuarios deshabiliten AWS Config o cambien sus reglas

Evitar que los usuarios deshabiliten AWS Config o cambien 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": "*"
    }
```

```
  ]
}
```

Ejemplos de SCP para Amazon Elastic Compute Cloud (Amazon EC2)

Ejemplos en esta categoría

- Requerir que las instancias de Amazon EC2 usen un tipo específico
- Impedir el lanzamiento de instancias de EC2 sin IMDSv2
- Impedir la desactivación del cifrado predeterminado de Amazon EBS

Requerir que las instancias de Amazon EC2 usen un tipo específico

Con esta SCP, se denegarán todos los lanzamientos de instancias que 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"
        }
      }
    }
  ]
}
```

Impedir el lanzamiento de instancias de EC2 sin IMDSv2

La siguiente política impide que todos los usuarios lancen instancias de EC2 sin IMDSv2.

```
[
   {
```

```
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
      "Condition":{
         "StringNotEquals":{
            "ec2:MetadataHttpTokens":"required"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:RunInstances",
      "Resource":"arn:aws:ec2:*:*:instance/*",
      "Condition":{
         "NumericGreaterThan":{
            "ec2:MetadataHttpPutResponseHopLimit":"3"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"*",
      "Resource":"*",
      "Condition":{
         "NumericLessThan":{
            "ec2:RoleDelivery":"2.0"
         }
      }
   },
   {
      "Effect":"Deny",
      "Action":"ec2:ModifyInstanceMetadataOptions",
      "Resource":"*"
   }
]
```

La siguiente política impide que todos los usuarios lancen instancias de EC2 sin IMDSv2, pero permite que identidades de IAM específicas modifiquen las opciones de metadatos de la instancia.

```
[
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
```

```
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:MetadataHttpTokens": "required"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "NumericGreaterThan": {
        "ec2:MetadataHttpPutResponseHopLimit": "3"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*",
    "Condition": {
      "StringNotLike": {
        "aws:PrincipalARN": [
          "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
        ]
      }
    }
  }
]
```

Impedir la desactivación del cifrado predeterminado de Amazon EBS

La siguiente política impide que todos los usuarios deshabiliten el cifrado predeterminado de Amazon EBS.

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:DisableEbsEncryptionByDefault"
  ],
  "Resource": "*"
}
```

SCP de ejemplo para Amazon GuardDuty

Ejemplos en esta categoría

- Evitar que los usuarios deshabiliten GuardDuty o modifiquen su configuración

Evitar que los usuarios deshabiliten GuardDuty o modifiquen su configuración

Esta SCP impide que los usuarios o los 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 información y los recursos de GuardDuty.

```
{
    "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 para AWS Resource Access Manager

Ejemplos en esta categoría

- Prevención de uso compartido externo
- Permitir que determinadas cuentas compartan solo tipos de recursos especificados
- Evitar compartir con organizaciones o unidades organizativas (OU)
- Permitir el uso compartido solo con usuarios y roles de IAM especificados

Prevención de uso compartido externo

En el siguiente ejemplo, SCP evita 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

La 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 compartir con organizaciones o unidades organizativas (OU)

La siguiente SCP impide que los usuarios creen recursos compartidos que comparten recursos con una organización AWS 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 de SCP permite a los usuarios compartir recursos con solamente la organización `o-12345abcdef`, unidad organizativa `ou-98765fedcba`, y cuenta `111111111111`.

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

Ejemplos de SCP para el Controlador de recuperación de aplicaciones de Amazon Route 53

Ejemplos en esta categoría

- Impedir que los usuarios actualicen los estados de control de enrutamiento de Route 53 ARC

Impedir que los usuarios actualicen los estados de control de enrutamiento de Route 53 ARC

Un operador de Route 53 ARC de nivel inferior necesita monitorear paneles y ver información de Route 53 ARC. Sin embargo, el operador no debe poder actualizar los controles de enrutamiento para realizar conmutación por error para la aplicación de una Región de AWS a otra, como podría hacer un operador sénior. Esta SCP impide que los usuarios o roles de cualquier cuenta afectada ejecuten operaciones relacionadas con Route 53 ARC que actualicen los controles de enrutamiento de Route 53 ARC.

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

```
            "Effect": "Deny",
            "Action": [
                "route53-recovery-cluster:UpdateRoutingControlState",
                "route53-recovery-cluster:UpdateRoutingControlStates"
            ],
            "Resource": "*",
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

Ejemplos de SCP para Amazon S3

Ejemplos en esta categoría

- Impedir la carga de objetos sin cifrar en Amazon S3

Impedir la carga de objetos sin cifrar en Amazon S3

La siguiente política impide que todos los usuarios carguen objetos no cifrados en buckets de S3.

```
{
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "*",
  "Condition": {
    "Null": {
      "s3:x-amz-server-side-encryption": "true"
    }
  }
}
```

La siguiente política impide que todos los usuarios carguen objetos no cifrados en los buckets de S3 y también impone un tipo de cifrado especificado (AES256 o aws:kms) para cargar objetos en sus cubos.

```
[
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
      "Null": {
        "s3:x-amz-server-side-encryption": "true"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "s3:PutObject",
    "Resource": "*",
    "Condition": {
      "StringNotEquals": {
        "s3:x-amz-server-side-encryption": "AES256"
      }
    }
  }
]
```

Ejemplo de SCP para etiquetar recursos

Ejemplos en esta categoría

- Requerir una etiqueta en los recursos creados especificados
- Impedir que las etiquetas se modifiquen excepto por entidades autorizadas

Requerir una etiqueta en los recursos creados especificados

La 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 con AWS CloudFormation como está escrito, porque ese servicio crea un secreto y luego lo etiqueta como dos pasos separados. Esta política de ejemplo bloquea eficazmente AWS CloudFormation de crear 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 en las SCP de AWS Organizations como en las políticas de permisos de IAM, consulte Acciones, recursos y claves de condición para servicios de AWS en la Guía del usuario.

Impedir que las etiquetas se modifiquen excepto por entidades autorizadas

El siguiente SCP muestra cómo una política puede permitir que solo los principales autorizados modifiquen las etiquetas adjuntas a los recursos. Esto es una parte importante del uso del control de acceso basado en atributos (ABAC) como parte de su estrategia de seguridad en la nube AWS. La política permite al autor de la llamada modificar las etiquetas solo en aquellos recursos donde la etiqueta de autorización (en este ejemplo, `access-project`) coincide exactamente con la misma etiqueta de autorización adjunta al usuario o rol de que realiza la solicitud. La política también impide que el usuario autorizado cambie el valor de la etiqueta que se utiliza para la autorización. El principal de llamada debe tener la etiqueta de autorización para realizar cualquier cambio.

Esta política solo impide que los usuarios no autorizados cambien las etiquetas. Un usuario autorizado que no esté bloqueado por esta política debe seguir teniendo una política del IAM independiente que otorgue explícitamente el permiso `Allow` en las API de etiquetado pertinentes. Por ejemplo, si el usuario tiene una política de administrador con `Allow */*` (permitir todos los servicios y todas las operaciones), entonces la combinación da como resultado que el usuario

administrador pueda cambiar solamente aquellas etiquetas que tienen un valor de etiqueta de autorización que coincide con el valor de etiqueta de autorización adjunto a la entidad principal del usuario. Esto se debe a que el `Deny` explícito en esta política anula el `Allow` explícito en la política de administrador.

> **Important**
>
> Esta no es una solución de política completa y no debe usarse como se muestra aquí. Este ejemplo solo 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, consulte Proteger las etiquetas de recursos utilizadas para la autorización mediante una política 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

- Evitar que los usuarios eliminen los registros de flujo de Amazon VPC
- Evitar que cualquier VPC que no tenga acceso a Internet lo obtenga

Evitar 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 registros de flujo de Amazon Elastic Compute Cloud (Amazon EC2) o los grupos o secuencias de registros 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 las funciones 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": "*"
    }
  ]
}
```

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, que se AWS Organizations crea automáticamente cuando la configuras por primera vez.

Temas

- Navegar por el nodo raíz y la jerarquía de la unidad organizativa
- Crear una unidad organizativa
- Cambiar el nombre de una unidad organizativa
- Edición de etiquetas asociadas a una unidad organizativa
- Mover cuentas a una unidad organizativa o entre el nodo raíz y las unidades organizativas
- Eliminar unidades organizativas

También puede revisar todas las unidades organizativas de su organización. Para obtener más información, consulte Ver detalles de una OU.

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

Para navegar por distintas unidades organizativas (OU) o al nodo raíz al desplazar cuentas o adjuntar políticas, puede utilizar la vista de “árbol” predeterminado.

AWS Management Console

Para navegar por la organización como un “árbol”

1. Inicie sesión en la consola deAWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, en la parte superior de la sección Organization (Organización), seleccione la opción de alternancia Hierarchy (Jerarquía) (en lugar de List [Lista]).
3. El árbol aparece inicialmente mostrando el nodo raíz y solo muestra el primer nivel de unidad organizativa secundaria y cuentas. Para ampliar el árbol para que muestre niveles más profundos, elija el icono de expandir ( ) junto a cualquier entidad principal. Para reducir el desorden y contraer una rama del árbol, elija el icono para colapsar ( ) junto a alguna de las entidades principales ampliadas.
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 radio situado junto al nombre y realizar ciertas operaciones en esa entidad en el menú de Acciones.

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 políticas adjuntas a ellas.

AWS Management Console

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

1. Inicie sesión en la consola deAWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la Cuentas de AWSpágina, en la parte superior de la sección Organización, selecciona el icono del botón Ver Cuentas de AWS solo para 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 con AWS Control Tower, cree sus unidades organizativas con la AWS Control Tower consola o las API. Si crea la OU en Organizations, esa OU no está registrada en ella AWS Control Tower. Para obtener más información, consulte Referencia del tipo de recurso fuera de AWS Control Tower en la Guía del usuarioAWS Control Tower .

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 deAWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Vaya a la página Cuentas de AWS.

   La consola muestra el contenido del nodo raíz OU y sus contenidos. La primera vez que visite un 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 una OU existente, vaya a la unidad organizativa secundaria eligiendo el nombre (no la casilla) de dicha unidad organizativa o eligiendo la al lado de las OU en la vista de árbol hasta que vea la que quiere, y luego elija su nombre.
4. Cuando haya seleccionado la unidad organizativa principal correcta en la jerarquía, en el menú Aciones, bajo Unidad organizacional, elija Crear nuevo
5. En el cuadro de diálogo Crear unidad organizacional, ingrese el nombre de la unidad organizativa que desee crear.
6. (Opcional) Agregue una o varias etiquetas seleccionando Agregar etiqueta y 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 unidad organizativa.
7. Por último, elija Crear unidad organizativa.

La nueva unidad organizativa aparecerá dentro de la principal. Ahora puede mover cuentas a esta unidad organizativa 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: create-organizational-unit

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

  Para encontrar la identidad del nodo raíz, utilice el comando enlistar nodo raíz. Para encontrar la identidad de una unidad organizativa, utilice la herramientaenlistar secundarios para navegar a la unidad organizativa que desee.

  En el ejemplo siguiente se muestra cómo buscar la identidad del nodo raíz y, a continuación, buscar la identidad de una unidad organizativa bajo el nodo 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"
    }
}
```

- AWS SDK: 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 una raíz de su AWS organización, debe tener los siguientes permisos:

- `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 deAWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, vaya a la unidad organizativa a la que le quiera cambiar el nombre y, a continuación, lleve a cabo uno de los siguientes pasos:
   - Seleccione el botón de opción

     situado junto a OU cuyo nombre desea cambiar. A continuación, en el menú de Acciones, en Unidad organizativa, elija Cambio de nombre.
   - Elija el nombre de la unidad organizativa para acceder a la página de detalles de la unidad organizativa. Luego, en la parte superior de la página, elija Renombrar.
3. En el cuadro de diálogo Cambiar el nombre de unidad organizativa, ingrese un nuevo nombre y, a continuación, elija Guardar 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 ejemplo siguiente se muestra cómo renombrar una OU.

```
$ 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"
    }
}
```

- AWS SDK: UpdateOrganizationalUnit

Edición de etiquetas asociadas a una unidad organizativa

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

Permisos mínimos

Para editar las etiquetas adjuntas a una unidad organizativa ubicada en una raíz de su AWS organización, debe tener 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 deAWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Cuentas de AWS, vaya a la unidad organizativa cuyas etiquetas desee editar y elíjala.
3. En la página de detalles de la unidad organizativa, elija la opción Etiquetas y, a continuación, 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 seleccionando Eliminar junto a la etiqueta que desea eliminar.
   - Agregue una nueva clave de etiqueta y valore el par. Seleccione Agregar etiqueta y, a continuación, introduzca el nuevo nombre de clave y el valor opcional en los cuadros proporcionados. Si deja el Valor en blanco, el valor es una cadena vacía; no es `null`.
5. Seleccione Guardar los cambios después 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:etiquetar recurso y desetiquetar recurso

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

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

```
    --tags Key=Department,Value=12345
```

Este comando no genera ninguna salida si se realiza correctamente.

En el ejemplo siguiente se quita la etiqueta `Department` de una OU.

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

Este comando no genera ninguna salida si se realiza correctamente.

- AWS SDK: TagResourcey UntagResource

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 nodo raíz a una unidad organizativa, de una unidad organizativa a otra, o de vuelta al nodo 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 demás unidades organizativas que van desde la principal hasta el nodo raíz. Si una cuenta no está en una unidad organizativa, solo obtendrá las políticas que se han asociado directamente al nodo raíz y las políticas que se han asociado directamente a la cuenta. Para mover cuentas, siga los pasos que se describen a continuación.

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 deAWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la páginaCuentas de AWS, busque la cuenta o cuentas que desea mover. Puede navegar por la jerarquía de unidades organizativas o habilitar Ver solo Cuentas de AWS para ver una lista plana de cuentas sin la estructura de unidad organizativa. Si tiene muchas cuentas, puede que tenga que elegir Cargar 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 menú Acciones, enCuenta de AWS, elija Mover.
5. En el cuadro de diálogo Mover Cuenta de AWS elija la unidad organizativa o el nodo raíz al que desea mover la cuenta y después elija Mover 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 siguiente ejemplo, se mueve una Cuenta de AWS de la raíz a una OU. 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 si se realiza correctamente.

- AWS SDK: MoveAccount

Eliminar unidades organizativas

Cuando inicia sesión en la cuenta de administración de su organización, puede eliminar 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 puede 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 deAWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la páginaCuentas de AWS, busque las unidades organizativas que desea eliminar y elija la casilla de verificación
   ☑
   junto al nombre de cada unidad organizativa.
3. Seleccionar Acciones y, a continuación, en Unidad organizativa, elija Eliminar.
4. Para confirmar que desea eliminar las unidades organizativas, ingrese el nombre de la unidad organizativa (si eligió eliminar solo una) o la palabra «eliminar» (si eligió más de una) y, a continuación, elija Eliminar.

   AWS Organizations elimina las unidades organizativas y las elimina de la lista.

AWS CLI & AWS SDKs

Eliminación de una unidad organizativa

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

- AWS CLI: delete-organizational-unit

  En el ejemplo siguiente se muestra cómo se elimina una OU.

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

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS SDK: DeleteOrganizationalUnit

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 128 caracteres como máximo y distingue entre 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, al igual que las claves de etiqueta, distinguen 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 utilizar una cadena vacía.

Para obtener más información acerca de los caracteres permitidos en una clave o valor de etiqueta, consulte la sección Parámetro de etiquetas 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 Prácticas recomendadas para etiquetar AWS recursos.

> **Tip**
>
> Use las políticas de etiquetas para ayudar a estandarizar su implementación de las etiquetas en todos los recursos en 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 agregar etiquetas a los siguientes tipos de recursos de la organización:
  - Cuentas de AWS
  - Unidades organizativas
  - Nodo raíz de la organización
  - Políticas

Puede agregar etiquetas en los siguientes momentos:

- Al crear el recurso: especifique las etiquetas en la consola Organizations o utilice el parámetro `Tags` con una de las operaciones de la API de `Create`. Esto no es aplicable al nodo raíz de la organización.
- Después de crear el recurso — Utilice la consola Organizations o llame a la operación `TagResource`.

Puede ver las etiquetas en cualquiera de los recursos etiquetables en AWS Organizations mediante la consola o llamando a la operación `ListTagsForResource`.

Puede eliminar etiquetas de un recurso especificando las claves que desea eliminar mediante la consola o llamando a la operación `UntagResource`.

Utilizar etiquetas

Las etiquetas le ayudan a organizar los recursos en su organización, al permitirle agruparlos 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 usar etiquetas para lo siguiente:

- Imponer estándares de etiquetado en sus recursos.
- Controlar el acceso a los recursos.

Agregar, actualizar y quitar etiquetas

Cuando inicie sesión en la cuenta de administración de su organización, puede agregar las etiquetas adjuntas a los recursos en su organización.

Adición de etiquetas a un recurso cuando lo crea

Permisos mínimos

Para agregar 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 de Organizations

Puede incluir claves y valores de etiqueta asociados a los siguientes recursos a medida que los crea.

- Cuenta de AWS
  - Cuenta creada
  - Cuenta invitada
- Unidad organizativa (OU)
- Política
  - Política de exclusión de servicios de IA
  - Política de copia de seguridad
  - Política de control de servicios
  - Política de etiquetas

El nodo raíz de la organización se genera al crear inicialmente la organización, por lo que solo puede agregarle etiquetas como un recurso existente.

Adición o actualización de etiquetas en un recurso existente

También puede agregar nuevas etiquetas o actualizar los valores de las etiquetas asociadas a recursos existentes.

Permisos mínimos

Para agregar 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 de Organizations

Para quitar etiquetas de los recursos de su organización, necesita los siguientes permisos:

- `organizations:UntagResource`

AWS Management Console

Para agregar, actualizar o quitar etiquetas para un recurso existente

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. Desplácese hasta la cuenta, nodo 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 agregar nuevas etiquetas, modificar los valores de etiquetas existentes o quitar etiquetas.

   Para agregar una etiqueta, elija Add Tag (Agregar etiqueta) y, a continuación, ingrese la Clave y el Valor de la etiqueta.

   Para eliminar una etiqueta, elija Eliminar.

   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 políticas de etiquetas que se apliquen.
5. Repita el paso anterior tantas veces como necesite.
6. Elija Guardar cambios.

AWS CLI & AWS SDKs

Para agregar o actualizar etiquetas a un recurso existente

Puede utilizar uno de los siguientes comandos para agregar etiquetas a los recursos etiquetables de su organización:

- AWS CLI: tag-resource
- AWSSDK: 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: UntagResource

Uso de AWS Organizations con otros servicios de AWS.

Puede utilizar el acceso de confianza para permitir un servicio de AWS que especifique, que se denomina servicio de confianza, que realice tareas en su organización y en las cuentas de esta en su nombre. Esto implica conceder permisos al servicio de confianza, pero no afecta de ninguna otra manera a los permisos de los usuarios o roles. Cuando se habilita el acceso, el servicio de confianza puede crear un rol de IAM denominado rol vinculado al servicio en cada cuenta de la organización. 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

Le recomendamos encarecidamente que, cuando la opción esté disponible, habilite y deshabilite el acceso de confianza mediante solamente la consola del servicio de confianza o sus equivalentes de operación de la API o la AWS CLI. 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 el vínculo Más información en la columna Admite el acceso de confianza en AWS servicios que puede utilizar con AWS Organizations.

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 un rol vinculado a un 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 desde AWS 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 políticas 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 los comandos del otro servicio para deshabilitar la integración garantiza que el otro servicio pueda limpiar los recursos necesarios solo 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 del otro servicio de AWS.

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 tanto en AWS Organizations como en el servicio de confianza, habilite el acceso utilizando las herramientas (la consola o la AWS CLI) disponibles en el servicio de confianza. Esto permite al servicio de confianza habilitar el acceso de confianza en AWS Organizations en su nombre, así como crear todos los recursos que necesita para funcionar en la organización.

  Los permisos mínimos para estas credenciales son los siguientes:

  - `organizations:EnableAWSServiceAccess`. También puede utilizar la clave de condición `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.
  - `organizations:ListAWSServiceAccessForOrganization` – obligatorio si se utiliza la consola de AWS Organizations.
  - 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 la consola de AWS Organizations.

     Para conocer los pasos para habilitar el acceso de confianza en AWS Organizations, consulte Cómo habilitar o deshabilitar el acceso de confianza.

  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 AWS servicios que puede utilizar con AWS Organizations.

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 el acceso de los usuarios y roles a un servicio de AWS, puede eliminar los permisos de IAM que conceden dicho acceso o puede utilizar políticas de control de servicio (SCP) en AWS Organizations.
> Puede aplicar SCP a las cuentas miembro únicamente. Los SCP no se aplican a la cuenta de administración. Le recomendamos que no ejecute servicios en la cuenta de administración.

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 clave de condición `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.
  - `organizations:ListAWSServiceAccessForOrganization` – obligatorio si se utiliza la consola de AWS Organizations.
  - 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 AWS servicios que puede utilizar con AWS Organizations.
  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 la consola de AWS Organizations.

Para conocer los pasos para deshabilitar el acceso de confianza en AWS Organizations, consulte Cómo habilitar o deshabilitar el acceso de confianza.

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

Le recomendamos encarecidamente que, cuando la opción esté disponible, habilite y deshabilite el acceso de confianza mediante solamente la consola del servicio de confianza o sus equivalentes de operación de la API o la AWS CLI. 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 el vínculo Más información en la columna Admite el acceso de confianza en AWS servicios que puede utilizar con AWS Organizations.

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 un rol vinculado a un 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 desde AWS 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 políticas 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 los comandos del otro servicio para deshabilitar la integración garantiza que el otro servicio pueda limpiar los recursos necesarios solo 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 del otro servicio de AWS.

AWS Management Console

Habilitar el acceso al servicio de confianza

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, 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 casilla Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir 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 de confianza

1. Inicie sesión en la consola de AWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila del servicio que desea deshabilitar y elija su nombre.
3. Espere a que el administrador del otro servicio le diga que el servicio está desactivado y que sus recursos han sido limpiados.
4. En el cuadro de diálogo de confirmación, ingrese **`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: AWS organizations enable-aws-service-access
- AWS CLI: AWS organizations disable-aws-service-access
- API de AWS: EnableAWSServiceAccess
- API de AWS: DisableAWSServiceAccess

AWS Organizations y roles vinculados al servicio

AWS Organizations usa funciones vinculadas a servicios de IAM para 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. El rol vinculado a servicio tiene permisos de IAM predefinidos que permiten al servicio de confianza realizar solamente 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 Organizations aprovisiona la cuenta miembro con un rol vinculado a un servicio denominado `AWSServiceRoleForOrganizations`. Solo el propio servicio AWS Organizations puede asumir esta función. Este rol tiene permisos que permiten a AWS Organizations crear roles vinculados a servicios para otros servicios de AWS. 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 habilitadas, el rol vinculado a un servicio denominado `AWSServiceRoleForOrganizations` no se utiliza nunca y puede eliminarlo. Si más adelante desea habilitar todas las características de la organización, el rol es necesario y debe restaurarlo. Las siguientes comprobaciones se producen cuando inicia el proceso para habilitar todas las características:

- Por cada cuenta miembro que se haya invitado a unirse a la organización – El administrador de dicha cuenta recibe una solicitud para que acepte habilitar 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.
- Por cada cuenta miembro que se haya creado en la organización – El administrador de la cuenta recibe una solicitud para volver a crear el rol vinculado al servicio. (El administrador de la cuenta de miembro no recibe una solicitud para habilitar todas las funciones porque el administrador de la cuenta de administración (antes conocida como "cuenta maestra") se considera el propietario de las cuentas de miembro creadas). AWS Organizations crea el rol vinculado al servicio cuando el administrador de la cuenta de 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.

AWS servicios que puede utilizar con AWS Organizations

Con él AWS Organizations , puede realizar actividades de administración de cuentas a gran escala mediante la consolidación de varias organizaciones Cuentas de AWS en una sola. La consolidación de cuentas simplifica el uso de otros servicios. AWS Puede aprovechar los servicios de administración de múltiples cuentas disponibles en algunos AWS Organizations AWS servicios para realizar tareas en todas las cuentas que son miembros de su organización.

En la siguiente tabla se enumeran AWS los servicios con los que puede AWS Organizations utilizarlos y las ventajas de utilizar cada servicio a nivel de toda la organización.

Acceso confiable: puede habilitar un AWS servicio compatible para realizar operaciones en todos los componentes de su Cuentas de AWS organización. Para obtener más información, consulte Uso de AWS Organizations con otros servicios de AWS..

Administrador delegado de AWS servicios: un AWS servicio compatible puede registrar una cuenta de AWS miembro en la organización como administrador de las cuentas de la organización en ese servicio. Para obtener más información, consulte Administrador delegado para los servicios de AWS que funcionan con Organizations.

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Account Management Gestione los detalles y los metadatos de todos los Cuentas de AWS componentes de su organización.	Puede crear, actualizar y eliminar la información de contacto alternativa de todas las cuentas de su organización.	Sí Más información	 Más información	Sí
AWS Servicio de migración de aplicaciones (MGN) AWS El servicio de	Puede administrar migraciones a gran escala	Sí	 Más información	Sí

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
migración de aplicaciones permite lift-and-shift a las empresas AWS acceder a una gran cantidad de servidores físicos, virtuales o en la nube sin problemas de compatibilidad, interrupciones en el rendimiento ni períodos de transición prolongados.	en varias cuentas.	Más información		
AWS Artifact Descargue los informes AWS de cumplimiento de normas de seguridad, como los informes ISO y PCI.	Puede aceptar acuerdos en nombre de todas las cuentas de su organización.	Sí Más información	Sí Consulte AWS Artifact.	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Audit Manager Automatice la recopilación continua de pruebas para ayudarle a auditar el uso de los servicios en la nube.	Audite continuamente su AWS uso en varias cuentas de su organización para simplificar la evaluación del riesgo y el cumplimiento.	Sí Más información	Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados
AWS Backup Administre y supervise las copias de seguridad de todas las cuentas de su organización.	Puede configurar y administrar planes de copias de 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.	Sí Más información	Sí Más información

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS CloudFormation Stacksets 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 delegada puede crear un conjunto de pilas con permisos administrados por servicios que implemente instancias de pila en cuentas de la organización.	Sí Más información	Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS CloudTrail Habilite la auditoría de riesgos y operaciones, el gobierno y la conformidad de su cuenta.	Un usuario con una cuenta de administración o una cuenta de administrador delegado puede crear un seguimiento de la organización o un almacén de datos de eventos que registre todos los eventos de todas las cuentas de la	Sí Más información	Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	organización.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Compute Optimizer Obtenga recomendaciones de optimización AWS informática.	Puede analizar todos los recursos que se encuentran en las cuentas de su organización para obtener recomendaciones de optimización. Para obtener más información, consulte Cuentas admitidas por Compute Optimizer en la Guía del usuario	Sí Más información	Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	de AWS Compute Optimizer.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Config 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 utilizar las operaciones de la AWS Config API para gestionar AWS Config las reglas y los paquetes de conformidad Cuentas de AWS en toda la	Sí Más información	Sí Más información: Reglas de Config Paquetes de conformidad Acumulación de datos de multicuentas y multiregiones	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	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 en AWS Organizations. Para obtener más informaci			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	ón, consulte Registro de un administrador delegado en la AWS Config Guía para desarrolladores de .			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Control Tower Configure y controle un entorno de AWS seguro con varias cuentas que cumpla con las normas correspondientes.	Puedes configurar una landing zone, un entorno de múltiples cuentas para todos tus AWS recursos. Este entorno incluye una organización y entidades de organización. Puede utilizar este entorno para hacer cumplir	Sí Más información	No	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	las normas de conformidad en todos sus Cuentas de AWSámbitos. Para obtener más información, consulte Cómo AWS Control Tower y Administrar cuentas a través de AWS Organizations en la Guía del usuario de AWS			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	Control Tower .			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados
Centro de optimización de costes de AWS Recopile recomendaciones de costos para todos los productos de AWS optimización.	Puede identificar, filtrar y agregar fácilmente las recomendaciones de optimización de AWS costos en todas las cuentas de sus AWS Organizations miembros y AWS regiones. Para obtener más información, consulte el Centro de optimizac	Sí Más información	No

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	ión de costos en la guía del usuario del Centro de optimización de costos.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Amazon Detective Genere visualizaciones a partir de sus datos de registro para analizar, investigar e identificar rápidamente la causa raíz de los hallazgos de seguridad o actividades sospechosas.	Puede integrar Amazon Detective AWS Organizations para garantizar que su gráfico de comportamiento de detective proporcione visibilidad de la actividad de todas las cuentas de su organización.	Sí Más información	Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados
El DevOps gurú de Amazon Analice los datos operativos y las métricas y eventos de las aplicaciones para identificar comportamientos que se desvían de los patrones operativos normales. Los usuarios reciben una notificación cuando DevOps Guru detecta un problema o riesgo operativo.	Puede integrarlo AWS Organizations para gestionar la información de todas las cuentas de toda su organización. Delega un administrador para ver, ordenar y filtrar información de todas las cuentas y obtener el estado de toda la organización de	Sí Más información	Sí Más información

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	todas las aplicaciones supervisadas.			
AWS Directory Service Configure y ejecute directorios en la AWS nube o conecte sus AWS recursos con un Microsoft Active Directory local existente.	Puede integrarlo AWS Organizations para AWS Directory Service compartir directorios sin problemas entre varias cuentas y cualquier VPC de una región.	Sí Más información	No	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados
Amazon EventBridge Supervise sus AWS recursos y las aplicaciones en las que se ejecuta AWS en tiempo real.	Puedes habilitar el uso compartido de todos los EventBridge eventos de Amazon, anteriormente Amazon CloudWatch Events, en todas las cuentas de tu organización. Para obtener más información, consulta Enviar y recibir	No	No

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	EventBridge eventos de Amazon entre Cuentas de AWS en la Guía del EventBridge usuario de Amazon.			
AWS Firewall Manager Configure y administre de forma centralizada las reglas de firewall para las aplicaciones web en sus cuentas y aplicaciones.	Puede configurar y gestionar AWS WAF las reglas de forma centralizada en todas las cuentas de su organización.	Sí Más información	Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados
Amazon GuardDuty GuardDuty es un servicio de monitoreo continuo de la seguridad que analiza y procesa la información de una variedad de fuentes de datos. Utiliza fuentes de información de amenazas y machine learning para identificar la actividad inesperada y potencialmente no permitida, así como la actividad malintencionada en su entorno de AWS .	Puede designar una cuenta de miembro GuardDuty para ver y administrar todas las cuentas de su organización. Al agregar cuentas de miembros, se GuardDuty habilitan automáticamente esas cuentas en la seleccionada Región de AWS.	Sí Más información	Sí Más información

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	También puede automatizar la GuardDuty activación de las nuevas cuentas que se agreguen a su organización. Para obtener más información, consulta GuardDuty Organisations in the Amazon GuardDuty User Guide.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Health Obtenga visibilidad de los eventos que podrían afectar al rendimiento de sus recursos o a los problemas de disponibilidad de AWS los servicios.	Puede agregar AWS Health eventos en todas las cuentas de su organización.	Sí Más información	Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Identity and Access Management Controle de forma segura el acceso a AWS los recursos.	Puede utilizar los datos del último acceso al servicio de IAM para conocer mejor la actividad de AWS en su organización. Puede utilizar estos datos para crear y actualizar las políticas de control del servicio (SCP) que restringen	No	No	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	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 organizativa en la Guía del usuario de IAM.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
IAM Access Analyzer Analice las políticas basadas en los recursos de su AWS entorno para identificar las políticas que otorgan acceso a un director fuera de su zona de confianza.	Puede designar una cuenta miembro para que sea administrador de IAM Access Analyzer. Para obtener más información, consulte Habilitación de Access Analyzer en la guía del usuario de IAM.	Sí Más información	Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Amazon Inspector Escanee automáticamente sus AWS cargas de trabajo en busca de vulnerabilidades para descubrir las instancias de Amazon EC2 y las imágenes de contenedores que residen en Amazon ECR para detectar vulnerabilidades de software y una exposición no intencionada a la red.	Delegue un administrador para habilitar o desactivar los análisis de cuentas de miembros, ver datos de búsqueda agregados de toda la organización, crear y administrar reglas de supresión. Para obtener más información,	Sí Más información	Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	consulte Administración de varias cuentas con AWS Organizations en la Guía del usuario de Amazon Inspector.			
AWS License Manager 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	Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados
Amazon Macie Descubre y clasifica el contenido crítico para su empresa mediante el machine learning 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 los datos en Amazon S3, en todas las cuentas desde una cuenta de administrador de Macie designada. Puede configurar Macie	Sí Más información	Sí Más información

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	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.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Marketplace Un catálogo digital curado que puede utilizar para encontrar, comprar, desplegar y gestionar el software, los datos y los servicios de terceros que necesita para crear soluciones y dirigir sus negocios.	Puede compartir las licencias de sus AWS Marketplace suscripciones y compras entre las cuentas de su organización.	Sí Más información	No	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados
AWS Marketplace Marketplace privado Le proporciona un amplio catálogo de productos disponibles en AWS Marketplace, junto con un control detallado de esos productos.	Le permite crear varias experiencias de mercado privado asociadas a toda la organización, a una o más unidades organizativas o a una o más cuentas de la organización, cada una con su propio conjunto de productos aprobados. AWS Los	Sí Más información	Sí Más información

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	administradores también pueden aplicar la marca de la empresa a cada experiencia de mercado privado con el logotipo, los mensajes y la combinación de colores de su empresa o equipo.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Network Manager Le permite gestionar de forma centralizada su red principal de WAN AWS en la nube y su red AWS Transit Gateway en todas las AWS cuentas, regiones y ubicaciones locales.	Puedes gestionar y supervisar tus redes globales de forma centralizada con las pasarelas de tránsito y sus recursos adjuntos en varias AWS cuentas de tu organización.	Sí Más información	Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados
AWS Resource Access Manager Comparta AWS los recursos específicos de su propiedad con otras cuentas.	Puede compartir recursos dentro de su organización sin intercambiar invitaciones adicionales. Entre los recursos que puede compartirse incluyen reglas de solucionador de Route 53, reservas de capacidad bajo demanda	Sí Más información	No

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	y mucho más. Para obtener información sobre cómo compartir reservas de capacidad, consulte la Guía del usuario de Amazon EC2 para instancias de Linux o la Guía del usuario de Amazon EC2 para instancias de Windows.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	Para obtener una lista de recursos compartibles, consulte Recursos compatibles en la Guía del usuario de AWS RAM .			
Explorador de recursos de AWS Explore sus recursos en una experiencia similar a la de un motor de búsqueda en Internet.	Habilite la búsqueda multicuenta.	Sí Más información	Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Security Hub Consulta el estado de tu seguridad AWS y compara tu entorno con los estándares y las mejores prácticas 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	Sí Más información	Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	proporciona una imagen más precisa de su postura general de seguridad.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Amazon S3 Storage Lens 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 las recomendaciones para todas las cuentas de miembros de su organización.	Sí Más información	Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Amazon Security Lake Amazon Security Lake centraliza los datos de seguridad de fuentes en la nube, en las instalaciones y personalizadas en un lago de datos almacenado en su cuenta.	Cree un lago de datos que recopile registros y eventos en sus cuentas.	Sí Más información	 Más información	Sí

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Service Catalog 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	Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Service Quotas 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	No	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS IAM Identity Center Proporciona acceso de inicio de sesión único para todas sus cuentas y aplicaciones en la nube.	Los usuarios pueden iniciar sesión en el portal de AWS acceso con sus credenciales corporativas y acceder a los recursos de la cuenta de administración o las cuentas de los miembros que tengan asignadas.	Sí Más información	Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Systems Manager Habilite la visibilidad y el control de sus AWS recursos.	Puede sincronizar los datos de operaciones Cuentas de AWS en toda la organización mediante Systems Manager Explorer. Puede administrar plantillas de cambios, aprobaciones e informes para todas las cuentas de miembros de su organizac	Sí Más información	Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
	ión desde una cuenta de administrador delegada mediante Systems Manager Change Manager.			

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Políticas de etiquetas Use etiquetas estandarizadas en los recursos de las cuentas de su organización.	Puede crear políticas de etiquetado para definir reglas de etiquetado para recursos y tipos de recursos específicos y adjuntar esas políticas a las unidades y cuentas de la organización para aplicar esas reglas.	Sí Más información	No	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Trusted Advisor Trusted Advisor inspecciona su AWS entorno y hace recomendaciones cuando existen oportunidades para ahorrar dinero, mejorar la disponibilidad y el rendimiento del sistema o ayudar a cerrar las brechas de seguridad.	Realiza Trusted Advisor comprobaciones para todos los miembros Cuentas de AWS de tu organización.	Sí Más información	Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
AWS Well-Architected Tool AWS Well-Architected Tool Esto le ayuda a documentar el estado de sus cargas de trabajo y a compararlas con las mejores prácticas de AWS arquitectura más recientes.	Permite a ambos AWS WA Tool y a los clientes de Organizations simplificar el proceso de compartir AWS WA Tool recursos con otros miembros de su organización.	Sí Más información	No	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Amazon VPC IP Address Manager (IPAM) IPAM es una función de VPC que le facilita la planificación, el seguimiento y la supervisión de las direcciones IP de sus cargas de AWS trabajo.	Monitoree el uso de direcciones IP en toda la organización y comparta grupos de direcciones IP entre las cuentas de miembro.	Sí Más información	Sí Más información	

AWS servicio	Ventajas de usarlo con AWS Organizations	Admite el acceso de confianza	Admite administradores delegados	
Analizador de accesibilidad de Amazon VPC El Analizador de accesibilidad es una herramienta de análisis de configuración que le permite realizar pruebas de conectividad entre un recurso de origen y un recurso de destino en las nubes privadas virtuales (VPC).	Realice un seguimiento de las rutas a través de las cuentas de sus organizaciones.	Sí Más información	Sí Más información	

AWS Account Management y AWS Organizations

AWS Account Management le ayuda a administrar la información de las cuentas y los metadatos de todas las Cuentas de AWS de su organización. Puede configurar, modificar o eliminar la información de contacto alternativa de cada una de las cuentas de miembro de su organización. Para obtener

más información, consulte Uso de AWS Account Management en su organización en la Guía del usuario de AWS Account Management.

Utilice la siguiente información para ayudarle a integrar AWS Account Management con AWS Organizations.

Para habilitar el acceso de confianza con Account Management

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Account Management requiere acceso de confianza a AWS Organizations para que se pueda designar una cuenta de miembro que sea el administrador delegado de este servicio para la organización.

Puede habilitar el acceso de confianza mediante las herramientas Organizations.

Puede habilitar el acceso de confianza mediante la consola AWS Organizations, ejecutando un comando AWS CLI, o llamando a una operación de API en uno de los SDK de AWS.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila de AWS Account Management, elija el nombre del servicio y, a continuación, elija Habilitar el acceso de confianza.
3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS Account Management que ahora pueden habilitar ese servicio usando su consola para trabajar con AWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para habilitar el acceso del servicio de confianza:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar AWS Account Management como servicio de confianza con Organizations.

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

  Este comando no genera ninguna salida si se realiza correctamente.

- API de AWS: EnableAWSServiceAccess

Para desactivar el acceso de confianza con Account Management

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo un administrador en la cuenta de administración AWS Organizations puede deshabilitar el acceso de confianza con AWS Account Management.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza mediante la consola AWS Organizations, la ejecución de una AWS CLI de Organizations, o llamando a una operación de API de Organizations en uno de los SDK de AWS.

AWS Management Console

Para deshabilitar 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Services (Servicios), busque la fila de AWS Account Management y, a continuación, elija el nombre del servicio.
3. Elija Deshabilitar el acceso de confianza.

4. En el cuadro de diálogo de confirmación, ingrese **`disable`** en el cuadro y, a continuación, elija Deshabilitar el acceso de confianza.
5. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS Account Management que ahora pueden deshabilitar ese servicio usando su consola o herramientas para trabajar con AWS Organizations.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar AWS Account Management como servicio de confianza con Organizations.

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

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

Habilitación de una cuenta de administrador delegado para Account Management

Cuando se designa una cuenta de miembro como administrador delegado de la organización, los usuarios y los roles de la cuenta designada pueden administrar los metadatos de la Cuenta de AWS de otras cuentas de miembro de la organización. Si no habilita una cuenta de administrador delegado, estas tareas solo las puede realizar la cuenta de administración de la organización. Esto le ayuda a separar la administración de la organización de la administración de los detalles de la cuenta.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado para administración de cuentas en la organización.

Para obtener instrucciones generales sobre cómo configurar una política de delegación, consulte Creación o actualización de una política de delegación basada en recursos.

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegada mediante el CLI AWS o uno de los SDK de AWS, puede usar los siguientes comandos:

- AWS CLI:

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

- AWS SDK: llame a la operación `RegisterDelegatedAdministrator` de Organizations y al número de ID de la cuenta de miembro e identifique la entidad principal del servicio de cuenta `account.amazonaws.com` como parámetros.

AWS Application Migration Service (MGN) y AWS Organizations

AWS Application Migration Service simplifica, acelera y reduce el costo de la migración de aplicaciones a AWS. Al integrarse con Organizations, puede usar la característica de visualización global para administrar migraciones a gran escala en varias cuentas. Para obtener más información, consulte Setting up your AWS Organizations en MGN user guide.

Utilice la siguiente información como ayuda para integrar AWS Application Migration Service con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a MGN realizar operaciones compatibles en las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre MGN y Organizations o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForApplicationMigrationService`

Entidades principales del servicio utilizadas por MGN

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios usados por MGN conceden acceso a las siguientes entidades de servicio:

- `mgn.amazonaws.com`

Habilitar el acceso de confianza con MGN

Cuando habilita el acceso de confianza con MGN, puede usar la característica de visualización global, que le permite administrar migraciones a gran escala entre varias cuentas. La visualización global proporciona visibilidad y la capacidad de realizar acciones específicas en los servidores de origen, las aplicaciones y las ondas de diferentes cuentas de AWS. Para obtener más información, consulte Setting up your AWS Organizations en AWS Application Migration Service user guide.

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso de confianza mediante la consola de AWS Application Migration Service o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice las herramientas o la consola de AWS Application Migration Service para habilitar la integración con Organizations. Esto permite a AWS Application Migration Service 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 con las herramientas proporcionadas por AWS Application Migration Service. Para obtener más información, consulte esta nota.
Si habilita el acceso de confianza mediante las herramientas o la consola de AWS Application Migration Service, no es necesario completar estos pasos.

Puede habilitar el acceso de confianza mediante la consola AWS Organizations, ejecutando un comando AWS CLI, o llamando a una operación de API en uno de los SDK de AWS.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila AWS Application Migration Service, elija el nombre del servicio y, a continuación, elija Habilitar el acceso de confianza.
3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS Application Migration Service que ahora pueden habilitar ese servicio con su consola para trabajar con AWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para habilitar el acceso del servicio de confianza:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar AWS Application Migration Service como servicio de confianza con Organizations.

```
$ aws organizations enable-aws-service-access \
```

```
    --service-principal mgn.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- API de AWS: EnableAWSServiceAccess

Deshabilitar el acceso con MGN

Solo un administrador de la cuenta de administración de Organizations puede deshabilitar el acceso de confianza con MGN.

Puede deshabilitar el acceso de confianza mediante AWS Application Migration Service o las herramientas de AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice las herramientas o la consola de AWS Application Migration Service para deshabilitar la integración con Organizations. Esto permite a AWS Application Migration Service realizar cualquier limpieza que requiera, como eliminar recursos o roles de acceso que el servicio ya no necesite. Continúe con estos pasos solo si no puede deshabilitar la integración con las herramientas proporcionadas por AWS Application Migration Service.
> Si deshabilita el acceso de confianza mediante las herramientas o la consola de AWS Application Migration Service, no es necesario completar estos pasos.

Puede deshabilitar el acceso de confianza mediante la consola AWS Organizations, la ejecución de una AWS CLI de Organizations, o llamando a una operación de API de Organizations en uno de los SDK de AWS.

AWS Management Console

Para deshabilitar 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila AWS Application Migration Service y, a continuación, elija el nombre del servicio.

3. Elija Deshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, ingrese **`disable`** en el cuadro y, a continuación, elija Deshabilitar el acceso de confianza.
5. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS Application Migration Service que ahora pueden deshabilitar ese servicio con su consola o herramientas para trabajar con AWS Organizations.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar AWS Application Migration Service como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal mgn.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

Habilitar una cuenta de administrador delegado para MGN

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 MGN que, de lo contrario, solo podrían realizarlas los usuarios o roles en la cuenta de administración de la organización. Esto lo ayuda a separar la administración de la organización de la de MGN. Para obtener más información, consulte Setting up your AWS Organizations en MGN user guide.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado para MGN en la organización

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegada mediante el CLI AWS o uno de los SDK de AWS, puede usar los siguientes comandos:

- AWS CLI:

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

- AWS SDK: llame a la operación `RegisterDelegatedAdministrator` de Organizations y al número de ID de la cuenta de miembro e identifique el servicio de cuenta `mgn.amazonaws.com` como parámetros.

Deshabilitar un administrador delegado para MGN

Solo un administrador de la cuenta de administración de Organizations puede eliminar un administrador delegado para MGN. Puede eliminar una cuenta de administrador delegado con la operación `DeregisterDelegatedAdministrator` de la CLI o SDK de Organizations.

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. Mediante AWS Artifact, un usuario de una cuenta de administración de la organización puede aceptar acuerdos automáticamente en nombre de todas las cuentas miembro de una organización, incluso cuando se agreguen nuevos informes y cuentas. Los usuarios de las cuentas miembro pueden ver y descargar acuerdos. Para obtener más información, consulte Administrar un acuerdo para varias cuentas en AWS Artifact en la Guía del usuario de AWS Artifact.

Utilice la siguiente información para ayudarle a integrar AWS Artifact con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguientes Rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a AWS Artifact realizar operaciones compatibles en las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre AWS Artifact y Organizations, o si elimina la cuenta de miembro de la organización.

Aunque puede eliminar o modificar este rol si elimina la cuenta de miembro de la organización, no lo recomendamos.

Se desaconseja modificar el rol porque puede provocar problemas de seguridad, como el diputado confuso entre servicios. Para obtener más información sobre la protección contra el diputado confuso, consulte Prevención contra el diputado entre servicios en la Guía del usuario de AWS Artifact.

- `AWSServiceRoleForArtifact`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios de AWS Artifact conceden acceso a las siguientes entidades de servicio:

- `artifact.amazonaws.com`

Habilitar el acceso de confianza con AWS Artifact

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso de confianza mediante las herramientas Organizations.

Puede habilitar el acceso de confianza mediante la consola AWS Organizations, ejecutando un comando AWS CLI, o llamando a una operación de API en uno de los SDK de AWS.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila de AWS Artifact, elija el nombre del servicio y, a continuación, elija Habilitar el acceso de confianza.

3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS Artifact que ahora pueden habilitar ese servicio usando su consola para trabajar con AWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para habilitar el acceso del servicio de confianza:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar AWS Artifact como servicio de confianza con Organizations.

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

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Deshabilitación del acceso con AWS Artifact

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo un administrador en la cuenta de administración AWS Organizations puede deshabilitar el acceso de confianza con AWS Artifact.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

AWS Artifact necesita tener acceso de confianza a través de AWS Organizations para poder trabajar con acuerdos de la 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 la consola AWS Organizations, la ejecución de una AWS CLI de Organizations, o llamando a una operación de API de Organizations en uno de los SDK de AWS.

AWS Management Console

Para deshabilitar 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Services (Servicios), busque la fila de AWS Artifact y, a continuación, elija el nombre del servicio.
3. Elija Deshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, ingrese **`disable`** en el cuadro y, a continuación, elija Deshabilitar el acceso de confianza.
5. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS Artifact que ahora pueden deshabilitar ese servicio usando su consola o herramientas para trabajar con AWS Organizations.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar AWS Artifact como servicio de confianza con Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal artifact.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- API de AWS: DisableAWSServiceAccess

Habilitar una cuenta de administrador delegado para AWS Artifact

Para obtener más información sobre cómo habilitar un administrador delegado para AWS Artifact, consulte AWS Artifact.

AWS Audit Manager y AWS Organizations

AWS Audit Manager lo ayuda a auditar continuamente el uso de AWS con el fin de 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, 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 Audit Manager con AWS Organizations, puede recopilar evidencia de una fuente más amplia incluyendo múltiples Cuentas de AWS de su organización en el ámbito de sus evaluaciones.

Para obtener más información, consulte Habilitar AWS Organizations en la Guía del usuario de Audit Manager.

Utilice la siguiente información para ayudarle a integrar AWS Audit Manager con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguientes Rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a Audit Manager realizar operaciones admitidas dentro de las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Audit Manager y Organizations, o si elimina la cuenta de miembro de la organización.

Para obtener más información sobre cómo Audit Manager utiliza este rol, consulte Uso de roles vinculados a servicios en la Guía del usuario de AWS Audit Manager.

- `AWSServiceRoleForAuditManager`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo 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, consulte Permisos necesarios para habilitar el acceso de confianza.

El Audit Manager requiere un acceso de confianza a AWS Organizations antes de que usted pueda designar una cuenta miembro para que sea el administrador delegado de la organización.

Puede habilitar el acceso de confianza mediante la consola de AWS Audit Manager o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola AWS Audit Manager o herramientas para habilitar la integración con Organizations. Esto permite a AWS Audit Manager 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 Audit Manager. Para obtener más información, consulte esta nota.
> Si habilita el acceso de confianza mediante la consola o las herramientas de AWS Audit Manager, no es necesario 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, consulte Configuración en la Guía del usuario de AWS Audit Manager.

> **Note**
>
> Si configura un administrador delegado mediante la Consola de AWS Audit Manager, a continuación AWS Audit Manager habilita automáticamente el acceso de confianza para usted.

Puede habilitar el acceso de confianza ejecutando el comando de Organizations AWS CLI, o llamando a una operación API de Organizations en uno de los SDK de AWS.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para habilitar el acceso del servicio de confianza:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar AWS Audit Manager como servicio de confianza con Organizations.

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

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Para deshabilitar el acceso de confianza con Audit Manager

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo un administrador en la cuenta de administración AWS Organizations puede deshabilitar el acceso de confianza con AWS Audit Manager.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando un comando de Organizations AWS CLI, o bien llamando a una operación de API de Organizations en uno de los AWS SDK.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar AWS Audit Manager como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal auditmanager.amazonaws.com
  ```

  Este comando no genera ninguna salida si 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 Audit Manager que, de lo contrario, solo 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**
>
> Solo un usuario o rol de la cuenta de administración de Organizations con el siguiente permiso puede configurar una cuenta de miembro como administrador delegado para Audit Manager en la organización:
> `audit-manager:RegisterAccount`

Para obtener instrucciones sobre cómo habilitar una cuenta de administrador delegada para Audit Manager, consulte Configuración en la Guía del usuario de AWS Audit Manager.

Si configura un administrador delegado mediante la consola de AWS Audit Manager, a continuación Audit Manager habilita automáticamente el acceso de confianza para usted.

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegada mediante el CLI AWS o uno de los SDK de AWS, puede usar los siguientes comandos:

- AWS CLI:

```
$  aws audit-manager register-account \
    --delegated-admin-account 123456789012
```

- SDK de AWS: Llame a la operación `RegisterAccount` y proporcione `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. Con AWS Backup, si 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 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 de su organización y, a continuación, crear políticas de copia de seguridad 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 las cuentas. Las políticas que están directamente asociadas a una cuenta se fusionan con las políticas heredadas de la raíz de la organización y de cualquier unidad organizativa principal para crear una política en vigor que se aplique a la cuenta. La política incluye el ID de un rol de IAM que tiene permisos para ejecutar AWS Backup en los recursos de sus cuentas. AWS Backup utiliza 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.

Supervisión

Cuando habilita el acceso de confianza para AWS Backup 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, consulte Monitorear los trabajos de copia de seguridad en la Guía del desarrollador de AWS Backup.

Para obtener más información sobre AWS Backup, consulte la Guía para desarrolladores de AWS Backup.

Utilice la siguiente información para ayudarle a integrar AWS Backup con AWS Organizations.

Habilitar el acceso de confianza con AWS Backup

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso de confianza mediante la consola de AWS Backup o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola AWS Backup o herramientas para habilitar la integración con Organizations. Esto permite a AWS Backup 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 Backup. Para obtener más información, consulte esta nota.
> Si habilita el acceso de confianza mediante la consola o las herramientas de AWS Backup, no es necesario completar estos pasos.

Para habilitar el acceso de confianza mediante AWS Backup, consulte Habilitación de backup en variosCuentas de AWSen la Guía para desarrolladores AWS Backup.

Deshabilitación del acceso con AWS Backup

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

AWS Backup requiere acceso de confianza con AWS Organizations para 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 un comando de Organizations AWS CLI, o bien llamando a una operación de API de Organizations en uno de los AWS SDK.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar AWS Backup como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal backup.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

Habilitar una cuenta de administrador delegado para AWS Backup

Consulte Administrador delegado en la Guía para desarrolladores de AWS Backup.

AWS CloudFormation StackSets y AWS Organizations

AWS CloudFormation StackSets permite crear, actualizar o eliminar pilas de varias Cuentas de AWS y Regiones de AWS en una sola operación. La integración de StackSets con AWS Organizations le 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 permite implementar instancias de pila en todas las cuentas miembro de su organización. No es preciso crear los roles

AWS Identity and Access Management necesarios; StackSets crea el rol de IAM en cada cuenta de miembro en su nombre.

También puede elegir habilitar implementaciones automáticas en cuentas que se añaden a su organización en el futuro. Con la implementación automática habilitada, los roles y la implementación de las instancias del conjunto de pilas asociadas se agregan automáticamente a todas las cuentas que se agreguen en el futuro a esa unidad organizativa.

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 stack sets 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, consulte Uso de AWS CloudFormation StackSets en la Guía del usuario de AWS CloudFormation.

Utilice la siguiente información para ayudarle a integrar StackSets AWS CloudFormation con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguientes Rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a StackSets AWS CloudFormation realizar operaciones admitidas dentro de las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre StackSets AWS CloudFormation y Organizations, o si elimina la cuenta de miembro de la organización.

- cuenta de administración: `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`

Para crear el rol `AWSServiceRoleForCloudFormationStackSetsOrgMember` vinculado a un servicio para las cuentas de miembros en su organización, debe crear primero un conjunto de pilas en la cuenta de administración. Esto crea una instancia del conjunto de pilas, que luego crea el rol en las cuentas del miembro.

- Cuentas de miembros: `AWSServiceRoleForCloudFormationStackSetsOrgMember`

Para obtener más detalles acerca de cómo crear conjuntos de pilas, consulte Trabajo con AWS CloudFormation StackSets en la Guía del usuario de AWS CloudFormation.

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios de Stacksets AWS CloudFormation otorgan acceso a las siguientes entidades de servicio:

- cuenta de administración: `stacksets.cloudformation.amazonaws.com`

  Solo puede modificar o eliminar este rol si deshabilitó el acceso de confianza entre StackSets y Organizations.
- Cuentas de miembros: `member.org.stacksets.cloudformation.amazonaws.com`

  Puede modificar o eliminar este rol de una cuenta solo si primero desactiva el acceso de confianza entre StackSets y Organizations, o si primero elimina la cuenta de la organización o unidad organizativa (OU) de destino.

Habilitar el acceso de confianza con Stacksets AWS CloudFormation

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Solo el administrador de la cuenta de administración de Organizations tiene permisos para habilitar el acceso de confianza con otro servicio AWS. Puede habilitar el acceso de confianza mediante la consola de AWS CloudFormation o la consola de Organizations.

Puede habilitar el acceso de confianza mediante StackSets AWS CloudFormation.

Para habilitar el acceso de confianza mediante la consola de Stacksets AWS CloudFormation, consulte Habilitar el acceso de confianza con AWS Organizations en la Guía del usuario de AWS CloudFormation.

Deshabilitar el acceso de confianza con Stacksets AWS CloudFormation

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo el administrador de la cuenta de gestión de Organizations tiene permisos para deshabilitar el acceso de confianza con otro servicio de AWS. Solo puede deshabilitar el acceso de confianza mediante la consola de Organizations. Si deshabilita el acceso de confianza con Organizations mientras usa StackSets, se conservan todas las instancias de pila creadas previamente. Sin embargo, los stack sets implementados mediante los permisos del rol vinculado a servicios ya no pueden realizar implementaciones en cuentas administradas por Organizations.

Puede deshabilitar el acceso de confianza mediante la consola de AWS CloudFormation o la consola de Organizations.

> **Important**
>
> Si deshabilita el acceso de confianza mediante programación (por ejemplo, con la AWS CLI o con una API), tenga en cuenta que esto eliminará el permiso. Es mejor deshabilitar el acceso de confianza con la consola de AWS CloudFormation.

Puede deshabilitar el acceso de confianza mediante la consola AWS Organizations, la ejecución de una AWS CLI de Organizations, o llamando a una operación de API de Organizations en uno de los SDK de AWS.

AWS Management Console

Para deshabilitar 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila de AWS CloudFormationStackSets y, a continuación, elija el nombre del servicio.

3. Elija Deshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, ingrese **disable** en el cuadro y, a continuación, elija Deshabilitar el acceso de confianza.
5. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de StackSets AWS CloudFormation que ahora pueden deshabilitar ese servicio usando su consola o herramientas para que no trabajen con AWS Organizations.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar StackSets AWS CloudFormation como servicio de confianza de Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal stacksets.cloudformation.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

Habilitación de una cuenta de administrador delegado de StackSets AWS CloudFormation

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 Stacksets AWS CloudFormation que, de lo contrario, solo 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 de StackSets AWS CloudFormation.

Para obtener instrucciones sobre cómo designar una cuenta de miembro como administrador delegado de StackSets AWS CloudFormation en la organización, consulte Registro de un administrador delegado en la Guía del usuario de AWS CloudFormation.

AWS CloudTrail y AWS Organizations

AWS CloudTrail es un AWS servicio que le ayuda a habilitar la gobernanza, el cumplimiento y la auditoría operativa y de riesgos de su empresa Cuenta de AWS. Con AWS CloudTrailél, un usuario de una cuenta de administración puede crear un registro de la organización que registre todos los eventos de todos los Cuentas de AWS miembros de 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, consulte Creación de un registro de seguimiento para una organización en la Guía del usuario deAWS CloudTrail .

Utilice la siguiente información para ayudarle a integrarse AWS CloudTrail con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Esta función le CloudTrail permite realizar operaciones de apoyo en las cuentas de su organización.

Puede eliminar o modificar esta función solo si deshabilita el acceso de confianza entre CloudTrail y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForCloudTrail`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados al servicio que utiliza CloudTrail otorgan acceso a los siguientes directores de servicio:

- `cloudtrail.amazonaws.com`

Habilitar el acceso de confianza con CloudTrail

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Si habilitas el acceso confiable mediante la creación de una ruta desde la AWS CloudTrail consola, el acceso confiable se configura automáticamente (recomendado). También puedes habilitar el acceso confiable mediante la AWS Organizations consola. Debes iniciar sesión con tu cuenta AWS Organizations de administración para crear un registro de la organización.

Si decide crear un registro de la organización mediante la API AWS CLI o la AWS API, debe configurar manualmente el acceso confiable. Para obtener más información, consulte Habilitar CloudTrail como servicio de confianza AWS Organizationsen la Guía delAWS CloudTrail usuario.

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la AWS CloudTrail consola o las herramientas para permitir la integración con Organizations.

Puede habilitar el acceso confiable ejecutando un AWS CLI comando de Organizations o llamando a una operación de API de Organizations en uno de los AWS SDK.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante Organizations CLI/SDK

Puedes usar los siguientes AWS CLI comandos u operaciones de API para habilitar el acceso a un servicio confiable:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitarlo AWS CloudTrail como servicio de confianza con Organizations.

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

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: habilitar AWSServiceAccess

Deshabilitación del acceso con CloudTrail

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

AWS CloudTrail requiere un acceso confiable AWS Organizations para funcionar con los registros de la organización y los almacenes de datos de los eventos de la organización. Si inhabilitas el acceso confiable AWS Organizations mientras lo usas AWS CloudTrail, se eliminarán todos los registros organizativos de las cuentas de los miembros porque no CloudTrail pueden acceder a la organización. Todos los registros organizativos de las cuentas de administración y los almacenes de datos de eventos de la organización se convierten en registros y almacenes de datos de eventos a nivel de cuenta. El `AWSServiceRoleForCloudTrail` rol creado para la integración entre la cuenta CloudTrail y AWS Organizations permanece en ella. Si vuelves a habilitar el acceso confiable, no CloudTrail se realizará ninguna acción en los almacenes de datos de senderos y eventos existentes. La cuenta de administración debe actualizar todos los almacenes de datos de rutas y eventos a nivel de cuenta para aplicarlos a la organización.

Para convertir un banco de datos de rutas o eventos a nivel de cuenta en un banco de datos de rutas o eventos de la organización, haga lo siguiente:

- Desde la CloudTrail consola, actualiza el banco de datos de rutas o eventos y selecciona la opción Activar para todas las cuentas de mi organización.
- Desde allí AWS CLI, haga lo siguiente:
  - Para actualizar una ruta, ejecute el update-trailcomando e incluya el `--is-organization-trail` parámetro.
  - Para actualizar un banco de datos de eventos, ejecute el update-event-data-storecomando e incluya el `--organization-enabled` parámetro.

Solo un administrador de la cuenta AWS Organizations de administración puede deshabilitar el acceso de confianza con AWS CloudTrail. Puede deshabilitar el acceso de confianza solo con las herramientas de Organizations, ya sea mediante la AWS Organizations consola, ejecutando un comando AWS CLI de Organizations o llamando a una operación de API de Organizations en uno de AWS los SDK.

Puede deshabilitar el acceso de confianza mediante la AWS Organizations consola, ejecutando un AWS CLI comando de Organizations o llamando a una operación de API de Organizations en uno de los AWS SDK.

AWS Management Console

Para deshabilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola deAWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Services (Servicios), busque la fila de AWS CloudTrail y, a continuación, elija el nombre del servicio.
3. Elija Deshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, ingrese **`disable`** en el cuadro y, a continuación, elija Deshabilitar el acceso de confianza.
5. Si eres el administrador de Only AWS Organizations, dile al administrador que ahora puede deshabilitar AWS CloudTrail ese servicio mediante su consola o con las herramientas con AWS Organizationslas que trabaja.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puedes usar los siguientes AWS CLI comandos u operaciones de API para deshabilitar el acceso a un servicio confiable:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitarlo AWS CloudTrail como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal cloudtrail.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: inhabilitar AWSServiceAccess

Habilitar una cuenta de administrador delegado para CloudTrail

Cuando lo utilizas CloudTrail con Organizations, puedes registrar cualquier cuenta de la organización para que actúe como administrador CloudTrail delegado y gestione los almacenes de datos de

eventos y senderos de la organización en nombre de la organización. Un administrador delegado es una cuenta de miembro de una organización que puede realizar las mismas tareas administrativas que la cuenta de administración. CloudTrail

> **Permisos mínimos**
>
> Solo un administrador de la cuenta de administración de Organizations puede registrar un administrador delegado para CloudTrail.

Puede registrar una cuenta de administrador delegado mediante la CloudTrail consola o mediante la operación `RegisterDelegatedAdministrator` CLI o SDK de Organizations. Para registrar un administrador delegado mediante la CloudTrail consola, consulte Añadir un administrador CloudTrail delegado.

Deshabilitar un administrador delegado para CloudTrail

Solo un administrador de la cuenta de administración de Organizations puede eliminar un administrador delegado para CloudTrail. Puede eliminar el administrador delegado mediante la CloudTrail consola o mediante la operación `DeregisterDelegatedAdministrator` CLI o SDK de Organizations. Para obtener información sobre cómo eliminar un administrador delegado mediante la CloudTrail consola, consulte Eliminar un administrador CloudTrail delegado.

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 si sus recursos son óptimos y genera recomendaciones de optimización para reducir el costo y mejorar el rendimiento de sus cargas de trabajo. Para obtener más información sobre Compute Optimizer, consulte la Guía del usuario de AWS Compute Optimizer.

Utilice la siguiente información para ayudarle a integrar AWS Compute Optimizer con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguientes Rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a Compute Optimizer realizar operaciones compatibles en las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Compute Optimizer y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForComputeOptimizer`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo 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

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso de confianza mediante la consola de AWS Compute Optimizer o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola AWS Compute Optimizer o herramientas para habilitar la integración con Organizations. Esto permite a AWS Compute Optimizer 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 Compute Optimizer. Para obtener más información, consulte esta nota.
>
> Si habilita el acceso de confianza mediante la consola o las herramientas de AWS Compute Optimizer, no es necesario completar estos pasos.

Para habilitar el acceso de confianza mediante la consola Compute Optimizer

Debe iniciar sesión en la consola de Compute Optimizer mediante la cuenta de administración de su organización. Inscríbase en nombre de su organización siguiendo las instrucciones en Habilitación del acceso a la cuenta en la Guía del usuario de AWS Compute Optimizer.

Puede habilitar el acceso de confianza mediante la consola AWS Organizations, ejecutando un comando AWS CLI, o llamando a una operación de API en uno de los SDK de AWS.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila de AWS Compute Optimizer, elija el nombre del servicio y, a continuación, elija Habilitar el acceso de confianza.
3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS Compute Optimizer que ahora pueden habilitar ese servicio usando su consola para trabajar con AWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para habilitar el acceso del servicio de confianza:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar AWS Compute Optimizer como servicio de confianza con Organizations.

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

Este comando no genera ninguna salida si 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, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo un administrador en la cuenta de administración AWS Organizations puede deshabilitar el acceso de confianza con AWS Compute Optimizer.

Puede deshabilitar el acceso de confianza ejecutando un comando de Organizations AWS CLI, o bien llamando a una operación de API de Organizations en uno de los AWS SDK.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar AWS Compute Optimizer como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal compute-optimizer.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

Habilitar una cuenta de administrador delegado para Compute Optimizer

Cuando se designa una cuenta de miembro como administrador delegado de la organización, los usuarios y los roles de la cuenta designada pueden administrar los metadatos de la Cuenta de AWS de otras cuentas de miembro de la organización. Si no habilita una cuenta de administrador delegado, estas tareas solo las puede realizar la cuenta de administración de la organización. Esto

le ayuda a separar la administración de la organización de la administración de los detalles de la cuenta.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado para Compute Optimizer en la organización

Para obtener instrucciones sobre cómo habilitar una cuenta de administrador delegada para Compute Optimizer, consulte https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html en la Guía del usuario de AWS Compute Optimizer.

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegada mediante el CLI AWS o uno de los SDK de AWS, puede usar los siguientes comandos:

- AWS CLI:

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

- AWS SDK: llame a la operación `RegisterDelegatedAdministrator` de Organizations y al número de ID de la cuenta de miembro e identifique la entidad principal del servicio de cuenta `account.amazonaws.com` como parámetros.

Deshabilitar un administrador delegado para Compute Optimizer

Solo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado para Compute Optimizer.

Para deshabilitar la cuenta de administrador delegada de Compute Optimizer mediante la consola de Compute Optimizer, consulte https://docs.aws.amazon.com/compute-optimizer/latest/ug/delegate-administrator-account.html en la Guía del usuario de AWS Compute Optimizer.

Para eliminar un administrador delegado mediante la AWS de AWS CLI, consulte Anular el registro del administrador delegado en la Referencia de comandos de la AWS CLI de AWS.

AWS Config y AWS Organizations

La acumulación de datos de varias cuentas y regiones de AWS Config permite agregar datos AWS Config de múltiples cuentas y Regiones de AWS en una misma cuenta. La acumulación de datos de varias cuentas y regiones permite a los administradores centrales de TI monitorear la conformidad de varias Cuentas de AWS de la compañía. 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 ConfigGuía para desarrolladores de .

También puede utilizar las API de AWS Config para administrar las reglas de AWS Config en todas Cuentas de AWS de su organización. Para obtener más información, consulte Habilitar reglas de AWS Config en todas las cuentas de su organización en la Guía del desarrollador AWS Config.

Utilice la siguiente información para ayudarle a integrar AWS Config con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

Los siguientes ejemplos de Rol vinculado al servicio se crean en las cuentas de su organización cuando se habilita el acceso de confianza. Este rol permite a AWS Config realizar operaciones compatibles en las cuentas de su organización.

- `AWSServiceRoleForConfig`

Este rol se crea cuando habilita AWS Config en su organización mediante la creación de un agregador de varias cuentas. AWS Config le pide que seleccione o cree un rol y que proporcione el nombre. No hay un nombre generado automáticamente.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre AWS Config y Organizations, o si elimina la cuenta de miembro de la organización.

Habilitar el acceso de confianza con AWS Config

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso de confianza mediante la consola de AWS Config o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola AWS Config o herramientas para habilitar la integración con Organizations. Esto permite a AWS Config 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 Config. Para obtener más información, consulte esta nota.
> Si habilita el acceso de confianza mediante la consola o las herramientas de AWS Config, no es necesario completar estos pasos.

Para habilitar el acceso de confianza desde la AWS Config consola

Para habilitar el acceso de confianza a AWS Organizations usando AWS Config, cree un agregador de varias cuentas y añádalo a la organización. Para obtener más información sobre cómo configurar un agregador de varias cuentas, consulte Configuración de un agregador mediante la consola en la Guía del desarrollador AWS Config.

Puede habilitar el acceso de confianza mediante la consola AWS Organizations, ejecutando un comando AWS CLI, o llamando a una operación de API en uno de los SDK de AWS.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila de AWS Config, elija el nombre del servicio y, a continuación, elija Habilitar el acceso de confianza.
3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS Config que ahora pueden habilitar ese servicio usando su consola para trabajar con AWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para habilitar el acceso del servicio de confianza:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar AWS Config como servicio de confianza con Organizations.

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

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Deshabilitación del acceso con AWS Config

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando un comando de Organizations AWS CLI, o bien llamando a una operación de API de Organizations en uno de los AWS SDK.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar AWS Config como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
  ```

```
    --service-principal config.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- API de AWS: DisableAWSServiceAccess

Centro de optimización de costes de AWS y AWS Organizations

Centro de optimización de costes de AWS es una función de AWS Billing and Cost Management que le ayuda a consolidar y priorizar las recomendaciones de optimización de costos en todas sus AWS cuentas y AWS regiones, para que pueda aprovechar al máximo sus AWS gastos. Cuando utiliza Cost Optimization Hub con, AWS Organizations puede identificar, filtrar y agregar fácilmente las recomendaciones de optimización de AWS costos en las cuentas de los miembros y AWS regiones de su Organización.

Para obtener más información, consulte Cost Optimization Hub en la Guía del AWS Cost Management usuario.

Utilice la siguiente información para ayudarle a integrarse Centro de optimización de costes de AWS con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Esta función permite a Cost Optimization Hub realizar operaciones de soporte en las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Cost Optimization Hub y Organizations, o si elimina la cuenta del miembro de la organización.

Para obtener más información, consulte los permisos de los roles vinculados al servicio para Cost Optimization Hub en la Guía del AWS Cost Management usuario.

- `AWSServiceRoleForCostOptimizationHub`

Principios de servicio utilizados por Cost Optimization Hub

Cost Optimization Hub utiliza el principio `cost-optimization-hub.bcm.amazonaws.com` de servicio.

Habilitar un acceso confiable con Cost Optimization Hub

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Cuando opta por utilizar la cuenta de administración de su organización e incluye todas las cuentas de los miembros de la organización, el acceso confiable a Cost Optimization Hub se habilita automáticamente en la cuenta de su organización.

Puede habilitar el acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una operación de API en uno de los AWS SDK.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila de Centro de optimización de costes de AWS, elija el nombre del servicio y, a continuación, elija Habilitar el acceso de confianza.
3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si eres el administrador de Only AWS Organizations, dile Centro de optimización de costes de AWS que ahora puede habilitar ese servicio mediante su consola para trabajar con AWS Organizationsél.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante OrganizationsCLI/SDK

Puedes usar los siguientes AWS CLI comandos u operaciones de API para habilitar el acceso a un servicio confiable:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitarlo Centro de optimización de costes de AWS como un servicio de confianza con Organizations.

```
$ aws organizations enable-aws-service-access \
    --service-principal cost-optimization-hub.bcm.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: habilitar AWSServiceAccess

Deshabilitación del acceso de confianza

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

> **Important**
>
> Si desactiva el acceso de confianza de Cost Optimization Hub después de activar esta opción, Cost Optimization Hub deniega el acceso a las recomendaciones de las cuentas de los miembros de su organización. Además, las cuentas de los miembros de la organización no están habilitadas para usar Cost Optimization Hub. Obtenga más información en Cost Optimization Hub y en el acceso confiable de Organizations en la Guía del AWS Cost Management usuario.

Puedes inhabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una operación de la API de Organizations en uno de los AWS SDK.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puedes usar los siguientes AWS CLI comandos u operaciones de API para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para inhabilitarlo Centro de optimización de costes de AWS como servicio de confianza con Organizations.

```
$ aws organizations disable-aws-service-access \
```

```
    --service-principal cost-optimization-hub.bcm.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: inhabilitar AWSServiceAccess

AWS Control Tower y AWS Organizations

AWS Control Tower ofrece una forma sencilla de configurar y gobernar un entorno con varias cuentas de AWS, de acuerdo con las prácticas recomendadas prescriptivas. La orquestación de AWS Control Tower amplía las capacidades de AWS Organizations.AWS Control Tower aplica controles preventivos y de detección (barreras de protección) para ayudar a evitar que sus organizaciones y cuentas diverjan de las mejores prácticas (desviación).

La orquestación de AWS Control Tower amplía las capacidades de AWS Organizations.

Para obtener más información, consulte la Guía del usuario de AWS Control Tower.

Utilice la siguiente información para ayudarle a integrar AWS Control Tower con AWS Organizations.

Roles necesarios para la integración

El rol `AWSControlTowerExecution` debe estar presente en todas las cuentas inscritas. Permite a AWS Control Tower administrar sus cuentas individuales y notificar información sobre ellas a sus cuentas de auditoría y archivo de registros.

Para obtener más información sobre los roles utilizados por AWS Control Tower, consulte Cómo funciona AWS Control Tower con roles para crear y administrar cuentas y Uso de políticas basadas en identidad (políticas de IAM) para AWS Control Tower.

Entidades principales del servicio utilizadas por AWS Control Tower

AWS Control Tower utiliza la entidad principal del servicio `controltower.amazonaws.com`.

Habilitar el acceso de confianza con AWS Control Tower

AWS Control Tower utiliza un acceso fiable para detectar desviaciones en los controles preventivos y realizar un seguimiento de los cambios de cuentas y unidades organizativas que causan desviaciones.

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso de confianza mediante las herramientas Organizations.

Para habilitar el acceso de confianza desde la consola de Organizations, seleccione **Enable access** junto a AWS Control Tower.

Puede habilitar el acceso de confianza ejecutando el comando de Organizations AWS CLI, o llamando a una operación API de Organizations en uno de los SDK de AWS.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para habilitar el acceso del servicio de confianza:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar AWS Control Tower como servicio de confianza con Organizations.

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

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Deshabilitación del acceso con AWS Control Tower

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

> **Important**
>
> Si desactiva el acceso de confianza de AWS Control Tower, su zona de aterrizaje de AWS Control Tower se desvía. La única forma de corregir la deriva es utilizar la reparación de la zona de aterrizaje de AWS Control Tower. Volver a habilitar el acceso confiable en

Organizaciones no soluciona la deriva. Obtenga más información sobre la deriva en la guía del usuario de AWS Control Tower.

Puede deshabilitar el acceso de confianza ejecutando un comando de Organizations AWS CLI, o bien llamando a una operación de API de Organizations en uno de los AWS SDK.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar AWS Control Tower como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal controltower.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

Amazon Detective y AWS Organizations

Amazon Detective utiliza sus datos de registro para generar visualizaciones que le permiten analizar, investigar e identificar la causa raíz de los hallazgos de seguridad o actividades sospechosas.

El uso de AWS Organizations le permite asegurarse de que el gráfico de comportamiento de Detective proporciona visibilidad de la actividad de todas las cuentas de su organización.

Cuando concede acceso de confianza a Detective, el servicio Detective puede reaccionar automáticamente a los cambios en la membresía de la organización. El administrador delegado puede habilitar cualquier cuenta de organización como cuenta de miembro en el gráfico de comportamiento. El Detective también puede habilitar automáticamente nuevas cuentas de organización como cuentas miembro. Las cuentas de organización no pueden desasociarse del gráfico de comportamiento.

Para obtener más información, consulte Uso de Amazon Detective en su organización en la Guía de administración de Amazon Detective.

Utilice la siguiente información para ayudarle a integrar Amazon Detective con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a Detective realizar operaciones soportadas por las cuentas de su organización.

Puede eliminar o modificar este rol sólo si desactiva el acceso de confianza entre Detective y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForDetective`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios de Detective conceden acceso a las siguientes entidades principales de servicio:

- `detective.amazonaws.com`

Para habilitar el acceso de confianza con Detective

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

> **Note**
>
> Cuando se designa un administrador delegado para Amazon Detective, se Detective habilita automáticamente el acceso de confianza para Detective en su organización.
> Detective requiere acceso de confianza a AWS Organizations para que se pueda designar una cuenta de miembro que sea el administrador delegado de este servicio para la organización.

Puede habilitar el acceso de confianza mediante las herramientas Organizations.

Puede habilitar el acceso de confianza mediante la consola AWS Organizations.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Services (Servicios), busque la fila de Amazon Detective, elija el nombre del servicio y, a continuación, elija Enable trusted access (Habilitar el acceso de confianza).
3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si es el administrador solamente de AWS Organizations, dígale al administrador de Amazon Detective que ahora pueden habilitar ese servicio usando su consola para trabajar con AWS Organizations.

Para desactivar el acceso de confianza con Detective

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo un administrador en la cuenta de administración AWS Organizations puede desactivar el acceso de confianza con Amazon Detective.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza mediante la consola de AWS Organizations.

AWS Management Console

Para deshabilitar 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Services (Servicios), busque la fila de Amazon Detective y, a continuación, elija el nombre del servicio.

3. Elija Deshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, ingrese **`disable`** en el cuadro y, a continuación, elija Deshabilitar el acceso de confianza.
5. Si es el administrador solamente de AWS Organizations, dígale al administrador de Amazon Detective que ahora pueden desactivar ese servicio usando su consola o herramientas para trabajar con AWS Organizations.

Habilitación de una cuenta de administrador delegado para Detective

La cuenta de administrador delegado de Detective es la cuenta de administrador de un gráfico de comportamiento de Detective. El administrador delegado determina qué cuentas de organización se van a habilitar y desactivar como cuentas de miembro en ese gráfico de comportamiento. El administrador delegado puede configurar Detective para habilitar automáticamente nuevas cuentas de organización como cuentas de miembro a medida que se agregan a la organización. Para obtener información sobre cómo un administrador delegado administra las cuentas de la organización, consulte Gestión de cuentas de organización como cuentas miembro en la Guía de administración de Amazon Detective.

Solo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado para Detective.

Puede especificar una cuenta de administrador delegada desde la consola o la API de Detective, o utilizando la operación dl SDK o de CLI de Organizations.

> **Permisos mínimos**
>
> Sólo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado para Detective en la organización

Para configurar un administrador delegado mediante la consola o la API Detective, consulte Designación de una cuenta de administrador de Detective para una organización en la Guía de administración de Amazon Detective.

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegada mediante el CLI AWS o uno de los SDK de AWS, puede usar los siguientes comandos:

- AWS CLI:

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

- AWS SDK: llame a la operación `RegisterDelegatedAdministrator` de Organizations y al número de ID de la cuenta de miembro e identifique la entidad principal del servicio de cuenta `account.amazonaws.com` como parámetros.

Desactivación de un administrador delegado para Detective

Puede eliminar el administrador delegado mediante la consola o la API de Detective, o bien mediante la operación del SDK o de la CLI `DeregisterDelegatedAdministrator` de Organizations. Para obtener información sobre cómo quitar un administrador delegado mediante la consola o la API de Detective o la API de Organizations, consulte Designación de una cuenta de administrador de Detective para una organización en la Guía de administración de Amazon Detective.

Amazon DevOps Guru y AWS Organizations

Amazon DevOps Guru analiza los datos operativos y las métricas y eventos de las aplicaciones para identificar comportamientos que se desvían de los patrones operativos normales. Se notifica a los usuarios cuando DevOps Guru detecta un problema o riesgo operativo.

El uso de DevOps Guru habilita el soporte para varias cuentas con AWS Organizations, para que pueda designar una cuenta miembro para administrar la información de toda su organización. A continuación, este administrador delegado puede ver, ordenar y filtrar información de todas las cuentas de su organización para desarrollar una visión holística del estado de todas las aplicaciones supervisadas de su organización sin necesidad de personalización adicional.

Para obtener más información, consulte Supervisar cuentas en toda la organización en la Guía del usuario de Amazon DevOps Guru.

Utilice la siguiente información para ayudarle a integrar Amazon DevOps Guru con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a DevOps Guru realizar operaciones soportadas en las cuentas de su organización.

Puede eliminar o modificar este rol solo si desactiva el acceso de confianza entre DevOps Guru y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForDevOpsGuru`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios de DevOps Guru conceden acceso a las siguientes entidades principales de servicio:

- `devops-guru.amazonaws.com`

Para obtener más información, consulte El uso roles vinculados al servicio de Amazon DevOps Guru en la Guía del usuario de Amazon DevOps Guru.

Para habilitar el acceso de confianza con DevOps Guru

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

> **Note**
>
> Cuando se designa un administrador delegado para Amazon DevOps Guru, DevOps Guru habilita automáticamente el acceso de confianza para DevOps Guru en su organización. DevOps Guru requiere acceso de confianza a AWS Organizations para que se pueda designar una cuenta de miembro que sea el administrador delegado de este servicio para la organización.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola Amazon DevOps Guru o herramientas para habilitar la integración con Organizations. Esto permite a Amazon DevOps Guru 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 Amazon DevOps Guru. Para obtener más información, consulte esta nota.

Puede habilitar el acceso de confianza mediante la consola de Amazon DevOps Guru o la consola de AWS Organizations.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Services (Servicios), busque la fila de Amazon DevOps Guru, elija el nombre del servicio y, a continuación, elija Enable trusted access (Habilitar el acceso de confianza).
3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si es el administrador solamente de AWS Organizations, dígale al administrador de Amazon DevOps Guru que ahora pueden habilitar ese servicio usando su consola para trabajar con AWS Organizations.

DevOps Guru console

Para habilitar el acceso de confianza mediante la consola DevOps Guru

1. Inicie sesión como administrador en la cuenta de administración y abra la consola DevOps Guru: Amazon DevOps Guru console (consola de Amazon DevOps Guru)
2. Elija Habilitar acceso de confianza.

Para desactivar el acceso de confianza con DevOps Guru

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo un administrador en la cuenta de administración AWS Organizations puede desactivar el acceso de confianza con Amazon DevOps Guru.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza mediante la consola de AWS Organizations.

AWS Management Console

Para deshabilitar 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Services (Servicios), busque la fila de Amazon DevOps Guru y, a continuación, elija el nombre del servicio.
3. Elija Deshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, ingrese **`disable`** en el cuadro y, a continuación, elija Deshabilitar el acceso de confianza.
5. Si es el administrador solamente de AWS Organizations, dígale al administrador de Amazon DevOps Guru que ahora pueden desactivar ese servicio usando su consola o herramientas para trabajar con AWS Organizations.

Habilitación de una cuenta de administrador delegado para DevOps Guru

La cuenta de administrador delegado de DevOps Guru puede ver los datos de información de todas las cuentas de miembros incorporadas a DevOps Guru desde la organización. Para obtener información sobre cómo un administrador delegado administra las cuentas de la organización, consulte Supervisar cuentas en toda la organización en la Guía del usuario de Amazon DevOps Guru.

Solo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado para DevOps Guru.

Puede especificar una cuenta de administrador delegado desde la consola de DevOps Guru, o utilizando la operación de Organizations `RegisterDelegatedAdministrator` CLI o SDK.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado para DevOps Guru en la organización

DevOps Guru console

Para configurar un administrador delegado en la consola de DevOps Guru

1. Inicie sesión como administrador en la cuenta de administración y abra la consola DevOps Guru: Amazon DevOps Guru console (consola de Amazon DevOps Guru)
2. Elija Registrar administrador delegado. Puede elegir una cuenta de administración o cualquier cuenta de miembro como administrador delegado.

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegada mediante el CLI AWS o uno de los SDK de AWS, puede usar los siguientes comandos:

- AWS CLI:

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

- AWS SDK: llame a la operación `RegisterDelegatedAdministrator` de Organizations y al número de ID de la cuenta de miembro e identifique la entidad principal del servicio de cuenta `account.amazonaws.com` como parámetros.

Desactivación de un administrador delegado para DevOps Guru

Puede remover una cuenta de administrador delegado utilizando la consola de DevOps Guru, o utilizando la operación de Organizations `DeregisterDelegatedAdministrator` CLI o SDK. Para obtener información sobre cómo quitar un administrador delegado mediante la consola de

DevOps Guru, consulte Supervisar cuentas en toda la organización en la Guía del usuario de Amazon DevOps Guru.

AWS Directory Service y AWS Organizations

AWS Directory Service para Microsoft Active Directory, o AWS Managed Microsoft AD, permite ejecutar Microsoft Active Directory (AD) como un servicio administrado. AWS Directory Service facilita la configuración y ejecución de directorios en la nube de AWS o ayuda a conectar los recursos de AWS con una instancia local existente de Microsoft Active Directory. AWS Managed Microsoft AD mantiene también una estrecha integración con AWS Organizations para permitir que se puedan compartir directorios fácilmente entre varias Cuentas de AWS y cualquier VPC de una región. Para obtener más información, consulte la Guía de administración de AWS Directory Service.

Utilice la siguiente información para ayudarle a integrar AWS Directory Service con AWS Organizations.

Habilitar el acceso de confianza con AWS Directory Service

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso de confianza mediante la consola de AWS Directory Service o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola AWS Directory Service o herramientas para habilitar la integración con Organizations. Esto permite a AWS Directory Service 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 Directory Service. Para obtener más información, consulte esta nota.
> Si habilita el acceso de confianza mediante la consola o las herramientas de AWS Directory Service, no es necesario completar estos pasos.

Para habilitar el acceso de confianza desde la AWS Directory Service consola

Para compartir un directorio, que habilita automáticamente el acceso de confianza, consulte Compartir el directorio en la Guía de administración AWS Directory Service. Para obtener instrucciones paso a paso, consulte Tutorial: Compartir su Directorio de Microsoft AD administrado AWS.

Puede habilitar el acceso de confianza mediante la consola AWS Organizations.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila de AWS Directory Service, elija el nombre del servicio y, a continuación, elija Habilitar el acceso de confianza.
3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS Directory Service que ahora pueden habilitar ese servicio usando su consola para trabajar con AWS Organizations.

Deshabilitación del acceso con AWS Directory Service

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Si se deshabilita el acceso de confianza con AWS Organizations mientras se está utilizando AWS Directory Service, todos los directorios que se hayan compartido previamente seguirán funcionando con normalidad. Sin embargo, ya no podrá compartir nuevos directorios en la organización hasta que rehabilite el acceso de confianza.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza mediante la consola de AWS Organizations.

AWS Management Console

Para deshabilitar 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Services (Servicios), busque la fila de AWS Directory Service y, a continuación, elija el nombre del servicio.
3. Elija Deshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, ingrese **`disable`** en el cuadro y, a continuación, elija Deshabilitar el acceso de confianza.
5. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS Directory Service que ahora pueden deshabilitar ese servicio usando su consola o herramientas para trabajar con AWS Organizations.

AWS Firewall Manager y AWS Organizations

AWS Firewall Manager es un servicio de administración de seguridad que se utiliza para configurar y administrar de forma centralizada reglas de firewall y otras protecciones en el Cuentas de AWS y en aplicaciones de su organización. Con Firewall Manager, puede implementar reglas AWS WAF, crear protecciones AWS Shield Advanced, configurar y auditar grupos de seguridad de Amazon Virtual Private Cloud (Amazon VPC), e implementar AWS Network Firewall. Utilice Firewall Manager para configurar las reglas de protección una única vez de forma que se apliquen automáticamente en todas las cuentas y recursos de la organización, incluso cuando se agreguen 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 para ayudarle a integrar AWS Firewall Manager con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguientes Rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a Firewall Manager realizar operaciones admitidas dentro de las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Firewall Manager y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForFMS`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo 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.

Puede habilitar el acceso de confianza mediante la consola de AWS Firewall Manager o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola AWS Firewall Manager o herramientas para habilitar la integración con Organizations. Esto permite a AWS Firewall Manager 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 Firewall Manager. Para obtener más información, consulte esta nota.
>
> Si habilita el acceso de confianza mediante la consola o las herramientas de AWS Firewall Manager, no es necesario completar estos pasos.

Debe iniciar sesión con su cuenta de administración de AWS Organizations para configurar una cuenta en la organización como la cuenta de administrador de AWS Firewall Manager. Para obtener más información, consulte Establecimiento de la cuenta de administrador de AWS Firewall Manager en la Guía para desarrolladores AWS Firewall Manager.

Puede habilitar el acceso de confianza mediante la consola AWS Organizations, ejecutando un comando AWS CLI, o llamando a una operación de API en uno de los SDK de AWS.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila de AWS Firewall Manager, elija el nombre del servicio y, a continuación, elija Habilitar el acceso de confianza.
3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS Firewall Manager que ahora pueden habilitar ese servicio usando su consola para trabajar con AWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para habilitar el acceso del servicio de confianza:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar AWS Firewall Manager como servicio de confianza con Organizations.

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

  Este comando no genera ninguna salida si 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, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Puede deshabilitar el acceso de confianza mediante la AWS Firewall Manager o herramientas AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola AWS Firewall Manager o herramientas para deshabilitar la integración con Organizations. Esto permite a AWS Firewall Manager realizar 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 por AWS Firewall Manager.
> Si desactiva el acceso de confianza mediante la consola o las herramientas de AWS Firewall Manager, no es necesario completar estos pasos.

Para deshabilitar el acceso de confianza mediante la consola Firewall Manager

Puede cambiar o revocar la cuenta de administrador de AWS Firewall Manager siguiendo las instrucciones de Designación de una cuenta diferente como cuenta de administrador de AWS Firewall Manager en la Guía para desarrolladores de AWS Firewall Manager.

Si revoca la cuenta de administrador, debe iniciar sesión en la cuenta de administración de AWS Organizations y establecer una nueva cuenta de administrador para AWS Firewall Manager.

Puede deshabilitar el acceso de confianza mediante la consola AWS Organizations, la ejecución de una AWS CLI de Organizations, o llamando a una operación de API de Organizations en uno de los SDK de AWS.

AWS Management Console

Para deshabilitar 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

2. En la página Services (Servicios), busque la fila de AWS Firewall Manager y, a continuación, elija el nombre del servicio.
3. Elija Deshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, ingrese **`disable`** en el cuadro y, a continuación, elija Deshabilitar el acceso de confianza.
5. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS Firewall Manager que ahora pueden deshabilitar ese servicio usando su consola o herramientas para trabajar con AWS Organizations.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar AWS Firewall Manager como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal fms.amazonaws.com
  ```

  Este comando no genera ninguna salida si 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, solo 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 Firewall Manager.

> **Permisos mínimos**
>
> Solo un usuario o rol de 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, consulte Establecimiento de cuenta de administración de AWS Firewall Manager en la Guía para desarrolladores AWS Firewall Manager.

Amazon GuardDuty y AWS Organizations

Amazon GuardDuty es un servicio de monitorización de la seguridad continuo que analiza y procesa diversas fuentes de datos, mediante fuentes de información de amenazas y Machine Learning para identificar actividad inesperada y potencialmente no autorizada y malintencionada en su entorno AWS. Esto puede incluir problemas como escalado de privilegios, uso de credenciales expuestas, comunicación con direcciones IP, URL o dominios malintencionados o la presencia de malware en las cargas de trabajo de contenedores e instancias de Amazon Elastic Compute Cloud.

Puede ayudar a simplificar la administración de GuardDuty mediante Organizations para administrar GuardDuty en todas las cuentas de su organización.

Para obtener más información, consulte Administrar cuentas de GuardDuty con AWS Organizations en la Guía del usuario de Amazon GuardDuty

Utilice la siguiente información para ayudarle a integrar Amazon GuardDuty con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

Los siguientes roles vinculados al servicio se crean automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Estos roles permiten a GuardDuty realizar operaciones compatibles en las cuentas de su organización. Puede eliminar un rol solo si desactiva el acceso de confianza entre GuardDuty y Organizations, o si elimina la cuenta de miembro de la organización.

- El rol vinculado al servicio `AWSServiceRoleForAmazonGuardDuty` se crea automáticamente en las cuentas que han integrado GuardDuty con Organizations. Para obtener más información, consulte Administrar cuentas de GuardDuty con Organizations en la Guía del usuario de Amazon GuardDuty

- El rol vinculado a un servicio `AmazonGuardDutyMalwareProtectionServiceRolePolicy` se activa automáticamente en cuentas que tienen la protección contra malware de GuardDuty habilitada. Para obtener más información, consulte Service-linked role permissions for GuardDuty Malware Protection (Permisos de roles vinculados a servicios para la protección contra malware de GuardDuty) en la Guía del usuario de Amazon GuardDuty

Los principales de servicios utilizados por los roles vinculados a servicios

- `guardduty.amazonaws.com`, utilizado por el rol vinculado al servicio `AWSServiceRoleForAmazonGuardDuty`.
- `malware-protection.guardduty.amazonaws.com`, utilizado por el rol vinculado al servicio `AmazonGuardDutyMalwareProtectionServiceRolePolicy`.

Habilitar el 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.

Puede habilitar el acceso de confianza mediante Amazon GuardDuty.

Amazon GuardDuty requiere un acceso de confianza a AWS Organizations antes de que usted pueda designar una cuenta miembro para que sea el administrador delegado de GuardDuty para la organización. Si configura un administrador delegado mediante la Consola de GuardDuty, a continuación GuardDuty habilita automáticamente el acceso de confianza para usted.

Sin embargo, si desea configurar una cuenta de administrador delegada mediante el AWS CLI o una de las SDK AWS, debe llamar de forma explícita a la operación EnableAWSServiceAccess y proporcionar la entidad de servicio como parámetro. Entonces puede llamar EnableOrganizationAdminAccount para delegar la cuenta de administrador de GuardDuty.

Deshabilitar el acceso de confianza con GuardDuty

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando un comando de Organizations AWS CLI, o bien llamando a una operación de API de Organizations en uno de los AWS SDK.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para 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 si se realiza correctamente.

- API de AWS: DisableAWSServiceAccess

Habilitar una cuenta de administrador delegado para GuardDuty

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 GuardDuty que, de lo contrario, solo 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 de GuardDuty.

> **Permisos mínimos**
>
> Para obtener información acerca de los permisos necesarios para designar una cuenta de miembro como administrador delegado, consulte Permisos necesarios para designar un administrador delegado en la Guía del usuario de Amazon GuardDuty

Para designar una cuenta de miembro como administrador delegado para GuardDuty

Consulte Designar un administrador delegado y agregar cuentas de miembro (consola) y Designar un administrador delegado y agregar cuentas miembro (API)

AWS Health y AWS Organizations

AWS Health proporciona una visibilidad continua del rendimiento de sus recursos y la disponibilidad de sus servicios AWS y cuentas. AWS Health ofrece eventos cuando sus recursos AWS 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 agregar eventos AWS Health en todas las cuentas de la organización. La vista organizativa muestra solo eventos AWS Health entregados después de que la característica esté habilitada y los retiene durante 90 días.

Puede habilitar la vista organizativa mediante la consola AWS Health, la AWS Command Line Interface (AWS CLI), o el API AWS Health.

Para obtener más información, consulte Agregar eventos AWS Health en la Guía del usuario AWS Health.

Utilice la siguiente información para ayudarle a integrar AWS Health con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguientes Rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a AWS Health realizar operaciones compatibles en las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre AWS Health y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForHealth_Organizations`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios de AWS Health conceden acceso a las siguientes entidades de servicio:

- `health.amazonaws.com`

Habilitar el acceso de confianza con AWS Health

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Cuando habilita la característica de vista organizativa para AWS 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, siempre que sea posible, utilice la consola AWS Health o herramientas para habilitar la integración con Organizations. Esto permite a AWS Health 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 Health. Para obtener más información, consulte esta nota.
> Si habilita el acceso de confianza mediante la consola o las herramientas de AWS Health, no es necesario completar estos pasos.

Para habilitar el acceso de confianza desde la AWS Health consola

Puede habilitar el acceso de confianza utilizando AWS Health y una de las siguientes opciones:

- Use la consola de AWS Health. Para obtener más información, consulte Vista organizativa (consola) en la Guía del usuario de AWS Health.
- Utilice la AWS CLI. Para obtener más información, consulte Vista organizativa (CLI) en la Guía del usuario de AWS Health.
- Llame a la EnableHealthServiceAccessForOrganization operación de API.

Puede habilitar el acceso de confianza ejecutando el comando de Organizations AWS CLI, o llamando a una operación API de Organizations en uno de los SDK de AWS.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para habilitar el acceso del servicio de confianza:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar AWS Health como servicio de confianza con Organizations.

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

  Este comando no genera ninguna salida si se realiza correctamente.

- API de AWS: EnableAWSServiceAccess

Deshabilitación del acceso con AWS Health

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Después de deshabilitar la características de vista organizativa, AWS Health deja de agregar eventos para todas las demás cuentas de la organización. Esto también deshabilita automáticamente el acceso de confianza.

Puede deshabilitar el acceso de confianza mediante la AWS Health o herramientas AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola AWS Health o herramientas para deshabilitar la integración con Organizations. Esto permite a AWS Health realizar 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 por AWS Health.
> Si desactiva el acceso de confianza mediante la consolao las herramientas de AWS Health, no es necesario completar estos pasos.

Para habilitar el acceso de confianza mediante la consola AWS Health

Puede deshabilitar el acceso de confianza con una de las siguientes opciones:

- Use la consola de AWS Health. Para obtener más información, consulte Deshabilitar la vista organizativa (consola) en la Guía del usuario de AWS Health.
- Utilice la AWS CLI. Para obtener más información, consulte Deshabilitar la vista organizativa (CLI) en la Guía del usuario de AWS Health.
- Llame a la DisableHealthServiceAccessForOrganization operación de API.

Puede deshabilitar el acceso de confianza ejecutando un comando de Organizations AWS CLI, o bien llamando a una operación de API de Organizations en uno de los AWS SDK.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar AWS Health como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal health.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

Habilitar una cuenta de administrador delegado para AWS Health

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 AWS Health que, de lo contrario, solo podrían realizarlas los usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la gestión de la organización de la de AWS Health.

Para designar una cuenta de miembro como administrador delegado para AWS Health

Consulte Registrar un administrador delegado de la vista organizacional

Para eliminar un administrador delegado para AWS Health

Consulte Eliminar un administrador delegado de la vista organizacional

Amazon Inspector y AWS Organizations

Amazon Inspector es un servicio automatizado de administración de vulnerabilidades que analiza continuamente Amazon EC2 y las cargas de trabajo de contenedores en busca de vulnerabilidades de software y exposición no deseada de la red.

Con Amazon Inspector puede administrar varias cuentas asociadas a través de AWS Organizations simplemente al delegar una cuenta de administrador para Amazon Inspector. El administrador delegado administra Amazon Inspector para la organización y recibe permisos especiales para realizar tareas en nombre de su organización, tales como:

- Habilitar o desactivar los análisis de cuentas de miembro
- Ver datos de búsqueda agregados de toda la organización
- Crear y administrar reglas de supresión

Para obtener más información, consulte Administración de varias cuentas con AWS Organizations en la Guía del usuario de Amazon Inspector.

Utilice la siguiente información para facilitar la integración de Amazon Inspector con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a Amazon Inspector realizar operaciones soportadas en las cuentas de su organización.

Puede eliminar o modificar este rol sólo si desactiva el acceso de confianza entre Amazon Inspector y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForAmazonInspector2`

Para obtener más información, consulte Uso de roles vinculados a servicios de Amazon Inspector en la Guía del usuario de Amazon Inspector.

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados al servicio utilizados por Amazon Inspector permiten el acceso a los siguientes entidades de servicio:

- `inspector2.amazonaws.com`

Para habilitar el acceso de confianza con Amazon Inspector

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Amazon Inspector requiere acceso de confianza para AWS Organizations antes de que pueda designar una cuenta de miembro para que sea el administrador delegado de este servicio para su organización.

Al designar un administrador delegado para Amazon Inspector, Amazon Inspector habilita automáticamente el acceso de confianza a Amazon Inspector para su organización.

Sin embargo, si desea configurar una cuenta de administrador delegada mediante el AWS CLI o una de las AWS SDK, debe llamar de forma explícita a la operación `EnableAWSServiceAccess` y proporcionar la entidad principal de servicio como parámetro. A continuación, puede llamar a `EnableDelegatedAdminAccount` para delegar la cuenta de administrador del Inspector.

Puede habilitar el acceso de confianza ejecutando el comando de Organizations AWS CLI, o llamando a una operación API de Organizations en uno de los SDK de AWS.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para habilitar el acceso del servicio de confianza:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar Amazon Inspector como servicio de confianza con Organizations.

```
$ aws organizations enable-aws-service-access \
```

```
    --service-principal inspector2.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- API de AWS: EnableAWSServiceAccess

> **Note**
>
> Si utiliza el API `EnableAWSServiceAccess`, también necesita llamar a `EnableDelegatedAdminAccount` para delegar la cuenta de administrador del Inspector.

Para desactivar el acceso de confianza con Amazon Inspector

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Sólo un administrador de la cuenta de administración de AWS Organizations puede desactivar el acceso de confianza con Amazon Inspector.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando un comando de Organizations AWS CLI, o bien llamando a una operación de API de Organizations en uno de los AWS SDK.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para desactivar Amazon Inspector como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal inspector2.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- API de AWS: DisableAWSServiceAccess

Habilitación de una cuenta de administrador delegado para Amazon Inspector

Con Amazon Inspector puede administrar varias cuentas de una organización mediante un administrador delegado con el servicio AWS Organizations.

La cuenta de AWS Organizations de administración designa una cuenta dentro de la organización como cuenta de administrador delegado de Amazon Inspector. El administrador delegado administra Amazon Inspector para la organización y se le conceden permisos especiales para realizar tareas en nombre de su organización, tales como: habilitar o desactivar los escaneos para las cuentas de los miembros, ver los datos de búsqueda agregados de toda la organización y crear y administrar las reglas de supresión

Para obtener información sobre cómo un administrador delegado administra las cuentas de la organización, consulte Descripción de la relación entre las cuentas de administrador y de miembro en la Guía del usuario de Amazon Inspector.

Sólo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado para Amazon Inspector.

Puede especificar una cuenta de administrador delegada desde la consola o la API de Amazon Inspector, o utilizando la operación de la CLI o el SDK de Organizations.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado para Amazon Inspector en la organización

Para configurar un administrador delegado mediante la consola de Amazon Inspector, consulte Paso 1: Habilitar Amazon Inspector - Entorno multicuenta en la Guía del usuario de Amazon Inspector.

> **Note**
>
> Debe llamar a `inspector2:enableDelegatedAdminAccount` en cada región en la que se utiliza Amazon Inspector.

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegada mediante el CLI AWS o uno de los SDK de AWS, puede usar los siguientes comandos:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal inspector2.amazonaws.com
```

- AWS SDK: llame a la operación `RegisterDelegatedAdministrator` de Organizations y al número de ID de la cuenta de miembro e identifique la entidad principal del servicio de cuenta `account.amazonaws.com` como parámetros.

Desactivación de un administrador delegado para Amazon Inspector

Sólo un administrador de la cuenta de administración AWS Organizations puede eliminar una cuenta de administrador delegado de la organización.

Puede eliminar el administrador delegado mediante la consola o la API de Amazon Inspector, o bien mediante la operación del SDK o de la CLI `DeregisterDelegatedAdministrator` de las Organizations. Para quitar un administrador delegado mediante la consola de Amazon Inspector, consulte Eliminación de un administrador delegado en la Guía del usuario de Amazon Inspector.

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 cree la infraestructura de nube de AWS, 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.

Para obtener más información acerca del Administrador de licencias de License Manager, consulte la Guía del usuario de License Manager.

Si vincula License Manager con AWS Organizations, puede:

- Habilitar el descubrimiento entre cuentas de recursos informáticos en toda su organización.
- Ver y administrar suscripciones comerciales de Linux que posea y ejecute en AWS. Para obtener más información, consulte Suscripciones de Linux en AWS License Manager.

Utilice la siguiente información para ayudarle a integrar AWS License Manager con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

Los siguientes roles vinculados al servicio se crean automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Estos roles permiten que License Manager realice operaciones admitidas en las cuentas de su organización.

Puede eliminar o modificar roles solo si deshabilita el acceso de confianza entre License Manager y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSLicenseManagerMasterAccountRole`
- `AWSLicenseManagerMemberAccountRole`
- `AWSServiceRoleForAWSLicenseManagerRole`
- `AWSServiceRoleForAWSLicenseManagerLinuxSubscriptionsService`

Para obtener más información, consulte License Manager: rol de cuenta de administración, License Manager: rol de cuenta de miembro y License Manager: rol de suscripciones de Linux.

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo 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`
- `license-manager-linux-subscriptions.amazonaws.com`

Habilitación del acceso de confianza License Manager

Puede habilitar el acceso de confianza solamente mediante AWS 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.

Para habilitar el acceso de confianza con el License Manager

Debe iniciar sesión en la consola de License Manager con su cuenta de administración AWS Organizations y asóciela a su cuenta de License Manager. Para obtener más información, consulte Configuración de AWS License Manager.

Deshabilitación del acceso de confianza con el License Manager

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza ejecutando un comando de la AWS CLI Organizations, o bien llamando a una operación de la API de Organizations de uno de los AWS SDK.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar AWS License Manager como servicio de confianza con Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal license-manager.amazonaws.com
```

  Este comando no genera ninguna salida si se realiza correctamente.

  Para deshabilitar el uso del acceso de confianza en las suscripciones de Linux:

```
$  aws organizations disable-aws-service-access \
    --service-principal license-manager-linux-subscriptions.amazonaws.com
```

- 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, solo 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 License Manager.

Para delegar una cuenta de miembro como administrador para License Manager, siga los pasos que se indican en Registro de un administrador delegado en la Guía del usuario de License Manager.

Amazon Macie yAWS Organizations

Amazon Macie es un servicio de privacidad y seguridad de datos completamente administrado que utiliza machine learning y coincidencia de patrones para descubrir, monitorear y ayudar a proteger sus datos confidenciales en Amazon Simple Storage Service (Amazon S3). Macie automatiza el descubrimiento de información confidencial, 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, consulte Administración de cuentas de Amazon Macie con AWS Organizations en la Guía del usuario de Amazon Macie.

Utilice la siguiente información para ayudarle a integrar Amazon Macie con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado a servicio se crea automáticamente para la cuenta de administrador de Macie delegado de su organización cuando se habilita el acceso de confianza. Este rol permite a Macie realizar operaciones admitidas en las cuentas de la organización.

Puede eliminar o modificar este rol solo si desactiva el acceso de confianza entre Macie y Organizations, o bien si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleRorAmazonMacie`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo 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`

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.

Puede habilitar el acceso de confianza mediante la consola de Amazon Macie o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola de Amazon Macie o herramientas para habilitar la integración con Organizations. Esto permite a Amazon Macie 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 Amazon Macie. Para obtener más información, consulte esta nota.
> Si habilita el acceso de confianza mediante la consola o las herramientas de Amazon Macie, no es necesario completar estos pasos.

Para habilitar el acceso de confianza mediante la consola Macie

Amazon Macie requiere un acceso de confianza a AWS Organizations para designar una cuenta miembro para que Macie sea el administrador de su organización. Si configura un administrador delegado mediante Management Console de Macie, a continuación Macie habilita automáticamente el acceso de confianza para usted.

Para obtener más información, consulte Integración y configuración de una organización en Amazon Macie en laGuía del usuario de Amazon Macie.

Puede habilitar el acceso de confianza ejecutando el comando de Organizations AWS CLI, o llamando a una operación API de Organizations en uno de los SDK de AWS.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para 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 si se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Para habilitar 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, solo 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

Solo un usuario o rol de 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 un acceso de confianza a AWS Organizations para designar una cuenta miembro para que Macie sea el administrador de su organización. Si configura un administrador

delegado mediante Management Console de Macie, a continuación Macie habilita automáticamente el acceso de confianza para usted.

Para obtener más información, consulte https://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 encontrar, comprar, implementar y gestionar el software, los datos y los servicios de terceros que necesita para crear soluciones y dirigir sus negocios.

AWS Marketplace crea y administra licencias mediante AWS License Manager para sus 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, consulte Uso de roles vinculados a servicios en AWS Marketplace en la Guía para comprador de AWS Marketplace.

Utilice la siguiente información para ayudarle a integrar AWS Marketplace con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguientes Rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a AWS Marketplace realizar operaciones compatibles en las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre AWS Marketplace y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForMarketplaceLicenseManagement`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios de AWS Marketplace conceden acceso a las siguientes entidades de servicio:

- `license-management.marketplace.amazonaws.com`

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.

Puede habilitar el acceso de confianza mediante la consola de AWS Marketplace o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola AWS Marketplace o herramientas para habilitar la integración con Organizations. Esto permite a 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.
> Si habilita el acceso de confianza mediante la consola o las herramientas de AWS Marketplace, no es necesario completar estos pasos.

Para habilitar el acceso de confianza desde la AWS Marketplace consola

Consulte Creación de un rol vinculado a un servicio de AWS Marketplace en la Guía del comprador de AWS Marketplace.

Puede habilitar el acceso de confianza mediante la consola AWS Organizations, ejecutando un comando AWS CLI, o llamando a una operación de API en uno de los SDK de AWS.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila de AWS Marketplace, elija el nombre del servicio y, a continuación, elija Habilitar el acceso de confianza.

3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS Marketplace que ahora pueden habilitar ese servicio usando su consola para trabajar con AWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para habilitar el acceso del servicio de confianza:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar AWS Marketplace como servicio de confianza con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal license-management.marketplace.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Deshabilitación del acceso 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.

Puede habilitar el acceso de confianza mediante las herramientas Organizations.

Puede deshabilitar el acceso de confianza ejecutando un comando de Organizations AWS CLI, o bien llamando a una operación de API de Organizations en uno de los AWS SDK.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar AWS Marketplace como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal license-management.marketplace.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

AWS Marketplace Private Marketplace y AWS Organizations

AWS Marketplace es un catálogo digital seleccionado que puede usar para buscar, comprar, implementar y administrar el software, los datos y los servicios de terceros que necesita para crear soluciones y administrar sus negocios. Un mercado privado le ofrece un amplio catálogo de productos disponibles AWS Marketplace, además de un control detallado de dichos productos.

AWS Marketplace Private Marketplace le permite crear varias experiencias de mercado privado asociadas a toda la organización, a una o más unidades organizativas o a una o más cuentas de la organización, cada una con su propio conjunto de productos aprobados. AWS Los administradores también pueden aplicar la marca de la empresa a cada experiencia de mercado privado con el logotipo, los mensajes y la combinación de colores de su empresa o equipo.

Para obtener más información, consulte Uso de funciones para configurar Private Marketplace AWS Marketplaceen la Guía delAWS Marketplace comprador.

Utilice la siguiente información para ayudarle a integrar AWS Marketplace Private Marketplace con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso confiable mediante la consola de Private AWS Marketplace Marketplace. Esta función permite a Private Marketplace realizar operaciones compatibles en las

cuentas de su organización. Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre AWS Marketplace Private Marketplace y Organizations y desvincula todas las experiencias de mercado privado de su organización.

Si habilita el acceso de confianza directamente desde la consola, la CLI o el SDK de Organizations, el rol vinculado al servicio no se crea automáticamente.

- `AWSServiceRoleForPrivateMarketplaceAdmin`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Las funciones vinculadas a servicios que utiliza Private Marketplace otorgan acceso a los siguientes principios de servicio:

- `private-marketplace.marketplace.amazonaws.com`

Habilitar un acceso confiable con Private Marketplace

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puedes habilitar el acceso de confianza mediante la consola de AWS Marketplace Private Marketplace o la AWS Organizations consola.

> **Important**
>
> Recomendamos encarecidamente que, siempre que sea posible, utilice la consola o las herramientas de AWS Marketplace Private Marketplace para permitir la integración con Organizations. Esto permite a AWS Marketplace Private Marketplace realizar cualquier configuración que necesite, como la creación de los recursos que necesite el servicio. Continúe con estos pasos solo si no puede habilitar la integración con las herramientas que proporciona AWS Marketplace Private Marketplace. Para obtener más información, consulte esta nota.
>
> Si habilitas el acceso de confianza mediante la consola o las herramientas de AWS Marketplace Private Marketplace, no necesitas completar estos pasos.

Para habilitar el acceso de confianza mediante la consola de Private Marketplace

Consulta Cómo empezar a usar Private Marketplace en la Guía delAWS Marketplace comprador.

Puede habilitar el acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una operación de API en uno de los AWS SDK.

AWS Management Console

Para habilitar el acceso de confianza mediante la consola de Organizations

1. Inicie sesión en la consola deAWS Organizations. Debe iniciar sesión como usuario de IAM, asumir un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busca la fila de AWS Marketplace Private Marketplace, elige el nombre del servicio y, a continuación, selecciona Habilitar acceso de confianza.
3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si eres el administrador de Only AWS Organizations, dile al administrador de AWS Marketplace Private Marketplace que ahora puede habilitar ese servicio mediante su consola para trabajar con él AWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante OrganizationsCLI/SDK

Puedes usar los siguientes AWS CLI comandos u operaciones de API para habilitar el acceso a un servicio confiable:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar AWS Marketplace Private Marketplace como un servicio de confianza en Organizations.

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

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: habilitar AWSServiceAccess

Inhabilitar el acceso de confianza con Private Marketplace

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puedes inhabilitar el acceso de confianza ejecutando un AWS CLI comando de Organizations o llamando a una operación de la API de Organizations en uno de los AWS SDK.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puedes usar los siguientes AWS CLI comandos u operaciones de API para deshabilitar el acceso a los servicios de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar AWS Marketplace Private Marketplace como un servicio de confianza en Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal private-marketplace.marketplace.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: inhabilitar AWSServiceAccess

Habilitar una cuenta de administrador delegado para Private Marketplace

El administrador de la cuenta de administración puede delegar los permisos administrativos de Private Marketplace a una cuenta de miembro designada, conocida como administrador delegado. Para registrar una cuenta como administrador delegado en el mercado privado, el administrador de la cuenta de administración debe asegurarse de que el acceso confiable y la función vinculada al servicio estén habilitados, seleccionar Registrar un nuevo administrador, proporcionar el número de AWS cuenta de 12 dígitos y elegir Enviar.

Las cuentas de administración y las cuentas de administrador delegado pueden realizar tareas administrativas de Private Marketplace, como crear experiencias, actualizar la configuración de

marca, asociar o disociar audiencias, añadir o eliminar productos y aprobar o rechazar solicitudes pendientes.

Para configurar un administrador delegado mediante la consola de Private Marketplace, consulta Crear y gestionar un mercado privado en la Guía delAWS Marketplace comprador.

También puede configurar un administrador delegado mediante la `RegisterDelegatedAdministrator` API de Organizations. Para obtener más información, consulte RegisterDelegatedAdministratorla Referencia de comandos de Organizations.

Inhabilitar un administrador delegado para Private Marketplace

Solo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado para Private Marketplace.

Puede eliminar al administrador delegado mediante la consola o la API de Private Marketplace, o mediante la operación `DeregisterDelegatedAdministrator` CLI o SDK de Organizations.

Para inhabilitar la cuenta de Private Marketplace de administrador delegado mediante la consola de Private Marketplace, consulta Crear y administrar un mercado privado en la Guía del AWS Marketplace comprador

AWS Network Manager y AWS Organizations

Network Manager le permite administrar de forma centralizada su AWS Red central de WAN en la nube y su AWS red de Transit Gateway en AWS cuentas, regiones y ubicaciones en las instalaciones. Con el soporte multicuenta, puede crear una única red global para cualquiera de sus AWS cuentas y registrar las puertas de enlace de tránsito de varias cuentas a la red global desde la consola de Network Manager.

Con el acceso de confianza entre Network Manager y Organizations habilitado, los administradores delegados registrados y las cuentas de administración pueden aprovechar el rol vinculado a servicios implementado en las cuentas de miembro para describir los recursos asociados a sus redes globales. Desde la consola de Network Manager, los administradores delegados registrados y las cuentas de administración pueden asumir los roles de IAM personalizados implementados en las cuentas miembro: `CloudWatch-CrossAccountSharingRole` para monitoreo y eventos de múltiples cuentas y `IAMRoleForAWSNetworkManagerCrossAccountResourceAccess` para el acceso del rol de conmutador de consola (para ver y administrar recursos de varias cuentas)

Important

- Recomendamos encarecidamente utilizar la consola de Network Manager para administrar la configuración multicuentas (habilitar/deshabilitar el acceso de confianza y registrar/anular el registro de administradores delegados). La administración de esta configuración desde la consola implementa y administra automáticamente todas las funciones vinculadas a servicios necesarios y los roles de IAM personalizados en las cuentas de miembro necesarias para el acceso multicuenta.
- Cuando habilita el acceso seguro para Network Manager en la consola de Network Manager, esta misma también habilita AWS CloudFormation el servicio StackSets. Network Manager utiliza StackSets para implementar roles de IAM personalizados necesarios para la administración multicuenta.

Para obtener más información sobre la integración de Network Manager con las Organizations, consulte Administrar multicuentas en Network Manager con AWS Organizations en la Guía de usuario de Amazon VPC.

Utilice la siguiente información para obtener ayuda al integrar AWS Network Manager con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Estos roles permiten a Network Manager realizar operaciones compatibles en las cuentas de su organización. Si deshabilita el acceso de confianza, Network Manager no eliminará estos roles de las cuentas de su organización. Puede eliminarlos manualmente desde la consola de IAM.

Cuenta de administración

- `AWSServiceRoleForNetworkManager`
- `AWSServiceRoleForCloudFormationStackSetsOrgAdmin`
- `AWSServiceRoleForCloudWatchCrossAccount`

Cuentas de miembros

- `AWSServiceRoleForNetworkManager`
- `AWSServiceRoleForCloudFormationStackSetsOrgMember`

Cuando registra una cuenta de miembro como administrador delegado, se crea automáticamente el siguiente rol adicional en la cuenta de administrador delegado:

- `AWSServiceRoleForCloudWatchCrossAccount`

Los principales de servicios utilizados por los roles vinculados a servicios

Los roles vinculados a los servicios solo pueden asumirse por las entidades principales de servicio autorizadas por las relaciones de confianza definidas para el rol.

- Para el `AWSServiceRoleForNetworkManager service-linked` rol, `networkmanager.amazonaws.com` es el único servicio principal que tiene acceso.
- Para el `AWSServiceRoleForCloudFormationStackSetsOrgMember` rol vinculado al servicio, `member.org.stacksets.cloudformation.amazonaws.com` es el único servicio principal que tiene acceso.
- Para el `AWSServiceRoleForCloudFormationStackSetsOrgAdmin` rol vinculado al servicio, `stacksets.cloudformation.amazonaws.com` es el único servicio principal que tiene acceso.
- Para el `AWSServiceRoleForCloudWatchCrossAccount` rol vinculado al servicio, `cloudwatch-crossaccount.amazonaws.com` es el único servicio principal que tiene acceso.

La eliminación de estos roles perjudicará la funcionalidad multicuenta de Network Manager.

Habilitar el acceso de confianza con Network Manager

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Solo el administrador de la cuenta de administración de Organizations tiene permisos para habilitar el acceso de confianza con otro servicio AWS. Asegúrese de utilizar la consola de Network Manager para habilitar el acceso de confianza y evitar problemas de permisos. Para obtener más información, consulte Gestionar multicuentas en Network Manager con AWS Organizations en la Guía del usuario de Amazon VPC.

Deshabilitar el acceso de confianza con Network Manager

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo el administrador de la cuenta de gestión de Organizations tiene permisos para deshabilitar el acceso de confianza con otro servicio de AWS.

> **Important**
>
> Le recomendamos encarecidamente que use la consola de Network Manager para deshabilitar el acceso de confianza. Si deshabilita el acceso de confianza de cualquier otro modo como, por ejemplo, usando AWS CLI con una API o con la consola AWS CloudFormation, es posible que los StackSets AWS CloudFormation implementados y los roles de IAM personalizados no se eliminen correctamente. Para deshabilitar el acceso de confianza, inicie sesión en la consola de Network Manager.

Habilitar una cuenta de administrador delegado para Network 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 Network Manager que, de lo contrario, solo podrían realizarlas los usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la gestión de la organización de la de Network Manager.

Para obtener más información sobre cómo designar una cuenta de miembro como administrador delegado de Network Manager en la organización, consulte Registrar un administrador delegador en la Guía del usuario de Amazon VPC.

AWS Resource Access Manager y AWS Organizations

AWS Resource Access Manager (AWS RAM) le permite compartir recursos de AWS especificados de los que es propietario con otras 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 para ayudarle a integrar AWS Resource Access Manager con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguientes Rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a AWS RAM realizar operaciones compatibles en las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre AWS RAM y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForResourceAccessManager`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios de AWS RAM conceden acceso a las siguientes entidades de servicio:

- `ram.amazonaws.com`

Habilitar el acceso de confianza con AWS RAM

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso de confianza mediante la consola de AWS Resource Access Manager o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola AWS Resource Access Manager o herramientas para habilitar la integración con Organizations. Esto permite a AWS Resource Access Manager 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 Resource Access Manager. Para obtener más información, consulte esta nota.
> Si habilita el acceso de confianza mediante la consola o las herramientas de AWS Resource Access Manager, no es necesario completar estos pasos.

Para habilitar el acceso de confianza mediante la consola AWS RAM o CLI

Consulte Habilitar el uso compartido conAWS Organizations en la Guía del usuario de AWS RAM.

Puede habilitar el acceso de confianza mediante la consola AWS Organizations, ejecutando un comando AWS CLI, o llamando a una operación de API en uno de los SDK de AWS.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila de AWS Resource Access Manager, elija el nombre del servicio y, a continuación, elija Habilitar el acceso de confianza.
3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS Resource Access Manager que ahora pueden habilitar ese servicio usando su consola para trabajar con AWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para habilitar el acceso del servicio de confianza:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar AWS Resource Access Manager como servicio de confianza con Organizations.

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

  Este comando no genera ninguna salida si se realiza correctamente.

- API de AWS: EnableAWSServiceAccess

Deshabilitación del acceso con AWS RAM

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Puede deshabilitar el acceso de confianza mediante la AWS Resource Access Manager o herramientas AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola AWS Resource Access Manager o herramientas para deshabilitar la integración con Organizations. Esto permite a AWS Resource Access Manager realizar 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 por AWS Resource Access Manager.
> Si desactiva el acceso de confianza mediante la consola o las herramientas de AWS Resource Access Manager, no es necesario completar estos pasos.

Para desactivar el acceso de confianza mediante la consola de AWS Resource Access Manager o la CLI

Consulte Habilitar el uso compartido conAWS Organizations en la Guía del usuario de AWS RAM.

Puede deshabilitar el acceso de confianza mediante la consola AWS Organizations, la ejecución de una AWS CLI de Organizations, o llamando a una operación de API de Organizations en uno de los SDK de AWS.

AWS Management Console

Para deshabilitar 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.

2. En la página Services (Servicios), busque la fila de AWS Resource Access Manager y, a continuación, elija el nombre del servicio.
3. Elija Deshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, ingrese **`disable`** en el cuadro y, a continuación, elija Deshabilitar el acceso de confianza.
5. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS Resource Access Manager que ahora pueden deshabilitar ese servicio usando su consola o herramientas para trabajar con AWS Organizations.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar AWS Resource Access Manager como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ram.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

Explorador de recursos de AWS y AWS Organizations

Explorador de recursos de AWS es un servicio de búsqueda y exploración de recursos. Con Resource Explorer, puede analizar sus recursos, como las instancias de Amazon Elastic Compute Cloud, las tablas de Amazon Kinesis Data Streams o Amazon DynamoDB, mediante una experiencia similar a la de un motor de búsqueda en Internet. Puede buscar sus recursos mediante metadatos de recursos, como nombres, etiquetas e identificadores. Resource Explorer funciona en todas las regiones de AWS en su cuenta para simplificar las cargas de trabajo entre regiones.

Al integrar Resource Explorer con AWS Organizations, puede recopilar evidencia de una fuente más amplia incluyendo múltiples Cuentas de AWS de su organización en el ámbito de sus evaluaciones.

Utilice la siguiente información para ayudarle a integrar Explorador de recursos de AWS con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a Resource Explorer realizar operaciones compatibles en las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Resource Explorer y Organizations, o si elimina la cuenta de miembro de la organización.

Para obtener más información sobre cómo Resource Explorer utiliza este rol, consulte Uso de roles vinculados a servicios en la Guía del usuario de Explorador de recursos de AWS.

- `AWSServiceRoleForResourceExplorer`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios usados por Resource Explorer conceden acceso a las siguientes entidades de servicio:

- `resource-explorer-2.amazonaws.com`

Para habilitar el acceso de confianza con Explorador de recursos de AWS

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Resource Explorer requiere un acceso de confianza a AWS Organizations antes de que usted pueda designar una cuenta miembro para que sea el administrador delegado de la organización.

Puede habilitar el acceso de confianza mediante la consola de Resource Explorer o la consola de Organizations. Le recomendamos que, siempre que sea posible, utilice la consola o herramientas de Resource Explorer para habilitar la integración con Organizations. Esto permite a Explorador de

recursos de AWS realizar cualquier configuración que requiera, como la creación de los recursos necesarios para el servicio.

Para habilitar el acceso de confianza desde la consola de Resource Explorer

Para obtener instrucciones sobre cómo habilitar el acceso confiable, consulte Requisitos previos para usar Resource Explorer en la Guía del usuario de Explorador de recursos de AWS.

> **Note**
>
> Si configura un administrador delegado mediante la Consola de Explorador de recursos de AWS, a continuación Explorador de recursos de AWS habilita automáticamente el acceso de confianza para usted.

Puede habilitar el acceso de confianza ejecutando el comando de Organizations AWS CLI, o llamando a una operación API de Organizations en uno de los SDK de AWS.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para habilitar el acceso del servicio de confianza:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar Explorador de recursos de AWS como servicio de confianza con Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal resource-explorer-2.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Para deshabilitar el acceso de confianza con Resource Explorer

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo un administrador en la cuenta de administración AWS Organizations puede deshabilitar el acceso de confianza con Explorador de recursos de AWS.

Puede deshabilitar el acceso de confianza mediante la Explorador de recursos de AWS o herramientas AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola Explorador de recursos de AWS o herramientas para deshabilitar la integración con Organizations. Esto permite a Explorador de recursos de AWS realizar 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 por Explorador de recursos de AWS.
> Si desactiva el acceso de confianza mediante la consola o las herramientas de Explorador de recursos de AWS, no es necesario completar estos pasos.

Puede deshabilitar el acceso de confianza ejecutando un comando de Organizations AWS CLI, o bien llamando a una operación de API de Organizations en uno de los AWS SDK.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar Explorador de recursos de AWS como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal resource-explorer-2.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- API de AWS: DisableAWSServiceAccess

Habilitar una cuenta de administrador delegado para Resource Explorer

Use su cuenta de administrador delegado para crear vistas de recursos de varias cuentas y asignarlas a una unidad organizativa o a toda la organización. Puede compartir vistas de varias cuentas con cualquier cuenta de su organización mediante AWS Resource Access Manager al crear recursos compartidos.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations con el siguiente permiso puede configurar una cuenta de miembro como administrador delegado para Resource Explorer en la organización: `resource-explorer:RegisterAccount`

Para obtener instrucciones sobre cómo habilitar una cuenta de administrador delegada para Resource Explorer, consulte Configuración en la Guía del usuario de Explorador de recursos de AWS.

Si configura un administrador delegado mediante la consola de Explorador de recursos de AWS, a continuación Resource Explorer habilita automáticamente el acceso de confianza para usted.

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegada mediante el CLI AWS o uno de los SDK de AWS, puede usar los siguientes comandos:

- AWS CLI:

```
$ aws organizations register-delegated-administrator \
    --account-id 123456789012 \
    --service-principal resource-explorer-2.amazonaws.com
```

- AWS SDK: llame a la operación `RegisterDelegatedAdministrator` de Organizations y al número de ID de la cuenta de miembro e identifique el servicio de cuenta `resource-explorer-2.amazonaws.com` como parámetros.

Desactivación de un administrador delegado para Resource Explorer

Sólo un administrador de la cuenta de administración de Organizations o de la cuenta de administrador delegado de Resource Explorer puede eliminar una cuenta de administrador delegado para Resource Explorer. Puede deshabilitar el acceso de confianza mediante la operación de CLI o SDK de `DeregisterDelegatedAdministrator` de Organizations.

AWS Security Hub y AWS Organizations

AWS Security Hub le proporciona una visión completa del estado de su seguridad AWS y le ayuda a comparar su entorno con los estándares y las mejores prácticas del sector de la seguridad.

Security Hub recopila datos de seguridad de todos tus productos Cuentas de AWS, de los AWS servicios que utilizas y de los productos de socios externos compatibles. Lo ayuda a analizar sus tendencias de seguridad y a identificar los problemas de seguridad de mayor prioridad.

Si utilizas Security Hub y de forma AWS Organizations conjunta, puedes habilitar automáticamente Security Hub para todas tus cuentas, incluidas las cuentas nuevas a medida que se vayan añadiendo. Esto aumenta la cobertura de las comprobaciones y hallazgos de Security Hub, lo que proporciona una imagen más completa y precisa de su posición general de seguridad.

Para obtener más información sobre Security Hub, consulte la Guía del usuario deAWS Security Hub.

Usa la siguiente información para ayudarte a integrarte AWS Security Hub con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguientes Rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a Security Hub realizar operaciones compatibles dentro de las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Security Hub y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForSecurityHub`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo 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 de confianza 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.

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, solo 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 Security Hub.

Para obtener información, consulte Designación de una cuenta de administrador de Security Hub en la Guía del usuario deAWS Security Hub .

Para designar una cuenta de miembro como administrador delegado para Security Hub

1. Inicie sesión en Organizations mediante la cuenta de administración de su organización.
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, elija Ir a Security Hub.
   - Si su cuenta de administración tiene activado Security Hub, en la consola de Security Hub, en General, elija Configuración.
3. En Administrador delegado, ingrese el ID de la cuenta.

Amazon S3 Storage Lens y AWS 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 de 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 la sección Uso de roles vinculados a servicios para Amazon S3 Storage Lens en la Guía del usuario de Amazon S3 Storage Lens.

Utilice la siguiente información para ayudarle a integrar Amazon S3 Storage Lens con AWS Organizations.

Rol vinculado al servicio creados al habilitar la integración

El siguiente rol vinculado a servicio se crea automáticamente en la cuenta de administrador delegado de su organización cuando se habilita el acceso de confianza y se aplica la configuración de Storage Lens a su organización. Este rol permite a Amazon S3 Storage Lens realizar operaciones compatibles en las cuentas de su organización.

Puede eliminar o modificar este rol 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`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo 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 Amazon S3 Storage Lens otorgan acceso a las siguientes entidades de servicio:

- `storage-lens.s3.amazonaws.com`

Habilitación del acceso de confianza para 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.

Puede habilitar el acceso de confianza mediante la consola de Amazon S3 Storage Lens o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola de Amazon S3 Storage Lens o herramientas para habilitar la integración con Organizations. Esto permite a Amazon S3 Storage Lens 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 Amazon S3 Storage Lens. Para obtener más información, consulte esta nota.
> Si habilita el acceso de confianza mediante la consola o las herramientas de Amazon S3 Storage Lens, no es necesario completar estos pasos.

Para habilitar el acceso de confianza mediante la consola de Amazon S3

Consulte Cómo habilitar el acceso de confianza en la Guía del usuario de Amazon Simple Storage Service.

Puede habilitar el acceso de confianza mediante la consola AWS Organizations, ejecutando un comando AWS CLI, o llamando a una operación de API en uno de los SDK de AWS.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila de Amazon S3 Storage Lens, elija el nombre del servicio y, a continuación, elija Habilitar el acceso de confianza.
3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si usted es el administrador de AWS Organizations, dígale al administrador de Amazon S3 Storage Lens que ahora puede habilitar ese servicio mediante su consola para que funcione con AWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para 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 Organizations.

  ```
  $ aws organizations enable-aws-service-access \
      --service-principal storage-lens.s3.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Deshabilitación del acceso de confianza para Amazon S3 Storage Lens

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Amazon S3 Storage Lens.

Puede deshabilitar el acceso de confianza mediante la consola de Amazon S3, CLI AWS o cualquiera de los SDK de AWS.

Para deshabilitar el acceso de confianza mediante la consola Amazon S3

Consulte Cómo desactivar el acceso de confianza en la Guía del usuario de Amazon Simple Storage Service.

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, solo 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 de Amazon S3 Storage Lens.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations con el siguiente permiso puede configurar una cuenta de miembro como administrador delegado para la Lente de almacenamiento de Amazon S3 en la organización:
> `organizations:RegisterDelegatedAdministrator`
> `organizations:DeregisterDelegatedAdministrator`

Amazon S3 Storage Lens admite un máximo de 5 cuentas de administrador delegado en su organización.

Para designar una cuenta de miembro como administrador delegado para Amazon S3 Storage Lens

Puede registrar un administrador delegado mediante la consola de Amazon S3, CLI AWS o cualquiera de los SDK de AWS. Para registrar una cuenta de miembro como cuenta de administrador delegado para su organización mediante la consola de Amazon S3, consulte Cómo registrar un administrador delegado en la Guía del usuario de Amazon Simple Storage Service.

Para anular un registro de un administrador delegado para Amazon S3 Storage Lens

Puede anular el registro de un administrador delegado mediante la consola de Amazon S3, CLI AWS o cualquiera de los SDK de AWS. Para anular el registro de un administrador delegado mediante la consola de Amazon S3, consulte Cómo anular el registro de un administrador delegado en la Guía del usuario de Amazon Simple Storage Service.

Amazon Security Lake y AWS Organizations

Amazon Security Lake centraliza los datos de seguridad de fuentes en la nube, en las instalaciones y personalizadas en un lago de datos almacenado en su cuenta. Al integrarse con Organizations, puede crear un lago de datos que recopile registros y eventos en todas sus cuentas. Para obtener más información, consulte Administración de varias cuentas con AWS Organizations en la Guía del usuario de Amazon Security Lake.

Utilice la siguiente información para ayudarle a integrar Amazon Security Lake con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Esta función permite a Amazon Security Lake realizar operaciones compatibles en las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Amazon Security Lake y Organizations, o si elimina la cuenta del miembro de la organización.

- `AWSServiceRoleForSecurityLake`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Las funciones vinculadas a servicios que utiliza Amazon Security Lake otorgan acceso a los siguientes principios de servicio:

- `securitylake.amazonaws.com`

Habilitar el acceso confiable con Amazon Security Lake

Cuando habilita el acceso de confianza con Security Lake, este puede reaccionar automáticamente a los cambios en la membresía de la organización. El administrador delegado puede habilitar la recopilación de AWS registros de los servicios compatibles en cualquier cuenta de la organización. Para obtener más información, consulte Rol vinculado al servicio para Amazon Security Lake en la guía del usuario de Amazon Security Lake.

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso de confianza mediante las herramientas Organizations.

Puede habilitar el acceso confiable mediante la AWS Organizations consola, ejecutando un AWS CLI comando o llamando a una operación de API en uno de los AWS SDK.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila de Amazon Security Lake, elija el nombre del servicio y, a continuación, elija Habilitar el acceso de confianza.
3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si es el administrador de Only AWS Organizations, dígale al administrador de Amazon Security Lake que ahora puede habilitar ese servicio mediante su consola para trabajar con él AWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante OrganizationsCLI/SDK

Puede usar los siguientes AWS CLI comandos u operaciones de API para habilitar el acceso a un servicio confiable:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar Amazon Security Lake como servicio de confianza con Organizations.

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

  Este comando no genera ninguna salida si se realiza correctamente.
- AWS API: habilitar AWSServiceAccess

Inhabilitar el acceso de confianza con Amazon Security Lake

Solo un administrador de la cuenta de administración de Organizations puede deshabilitar el acceso de confianza con Amazon Security Lake.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza mediante la AWS Organizations consola, ejecutando un AWS CLI comando de Organizations o llamando a una operación de API de Organizations en uno de los AWS SDK.

AWS Management Console

Para deshabilitar 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila de Amazon Security Lake y, a continuación, elija el nombre del servicio.
3. Elija Deshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, ingrese **`disable`** en el cuadro y, a continuación, elija Deshabilitar el acceso de confianza.
5. Si usted es el administrador de Only AWS Organizations, dígale al administrador de Amazon Security Lake que ahora puede deshabilitar ese servicio mediante su consola o sus herramientas para que no funcione AWS Organizations.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede usar los siguientes AWS CLI comandos u operaciones de API para deshabilitar el acceso a un servicio confiable:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para desactivar Amazon Security Lake como servicio de confianza con Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal securitylake.amazonaws.com
```

  Este comando no genera ninguna salida si se realiza correctamente.

- AWS API: inhabilitar AWSServiceAccess

Habilitar una cuenta de administrador delegado para Amazon Security Lake

El administrador delegado de Amazon Security Lake añade otras cuentas de la organización como cuentas de miembros. El administrador delegado puede activar Amazon Security Lake y configurar los ajustes de Amazon Security Lake para las cuentas de los miembros. El administrador delegado puede recopilar registros en una organización en todas AWS las regiones en las que Amazon Security Lake esté activado (independientemente del punto de conexión regional que utilice actualmente).

También puede configurar el administrador delegado para que añada automáticamente nuevas cuentas en la organización como miembros. El administrador delegado de Amazon Security Lake tiene acceso a los registros y eventos de las cuentas de los miembros asociadas. En consecuencia, puede configurar Amazon Security Lake para que recopile los datos que son propiedad de las cuentas de los miembros asociadas. También puede conceder permiso a los suscriptores para que consuman los datos que pertenecen a las cuentas asociadas de los miembros.

Para obtener más información, consulte Administración de varias cuentas con AWS Organizations en la Guía del usuario de Amazon Security Lake.

> **Permisos mínimos**
>
> Solo un administrador de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado de Amazon Security Lake en la organización.

Puede especificar una cuenta de administrador delegado mediante la consola de Amazon Security Lake, la acción de la `CreateDatalakeDelegatedAdmin` API de Amazon Security Lake o el comando `create-datalake-delegated-admin` CLI. También puede utilizar la operación `RegisterDelegatedAdministrator` CLI o SDK de Organizations. Para obtener instrucciones sobre cómo habilitar una cuenta de administrador delegado para Amazon Security Lake, consulte Designación del administrador delegado de Security Lake y adición de cuentas de miembros en la guía del usuario de Amazon Security Lake.

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegado mediante la AWS CLI o uno de los AWS SDK, puede utilizar los siguientes comandos:

- AWS CLI:

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

- AWS SDK: llame a la `RegisterDelegatedAdministrator` operación de la organización y al número de identificación de la cuenta del miembro e identifique el principal de servicio de la cuenta `account.amazonaws.com` como parámetros.

Inhabilitar un administrador delegado para Amazon Security Lake

Solo un administrador de la cuenta de administración de Organizations o de la cuenta de administrador delegado de Amazon Security Lake puede eliminar una cuenta de administrador delegado de la organización.

Puede eliminar la cuenta de administrador delegado mediante la acción de la `DeleteDatalakeDelegatedAdmin` API de Amazon Security Lake, el comando `delete-datalake-delegated-admin` CLI o la operación de `DeregisterDelegatedAdministrator` CLI o SDK de Organizations. Para eliminar un administrador delegado mediante Amazon Security Lake, consulte Eliminar el administrador delegado de Amazon Security Lake en la guía del usuario de Amazon Security Lake.

AWS Service Catalog y AWS Organizations

Service Catalog le permite crear y administrar catálogos de servicios de TI aprobados para su uso en AWS.

La integración de Service Catalog con AWS Organizations simplifica el intercambio de carteras y la copia de productos en toda la organización. Los administradores de Service Catalog pueden hacer referencia a una organización existente en AWS Organizations al compartir una cartera y pueden compartir la cartera con cualquier unidad organizativa (OU) de confianza de 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 dentro de la vista Cartera importada del administrador en Service Catalog.

Para obtener más información sobre Service Catalog, consulte la Guía del administrador de Service Catalog.

Utilice la siguiente información para ayudarle a integrar AWS Service Catalog con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

AWS Service Catalog no 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 siguiente entidad de servicio:

- `servicecatalog.amazonaws.com`

Habilitación del acceso de confianza con 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.

Puede habilitar el acceso de confianza mediante la consola de AWS Service Catalog o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola AWS Service Catalog o herramientas para habilitar la integración con Organizations. Esto permite a AWS Service Catalog 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 Service Catalog. Para obtener más información, consulte esta nota.
> Si habilita el acceso de confianza mediante la consola o las herramientas de AWS Service Catalog, no es necesario completar estos pasos.

Para habilitar el acceso de confianza mediante la CLI de Service Catalog o el SDK de AWS

Llame a uno de los siguientes comandos u operaciones:

- AWS CLI: aws servicecatalog enable-aws-organizations-access
- SDK de AWS: AWSServiceCatalog::EnableAWSOrganizationsAccess

Puede habilitar el acceso de confianza mediante la consola AWS Organizations, ejecutando un comando AWS CLI, o llamando a una operación de API en uno de los SDK de AWS.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila de AWS Service Catalog, elija el nombre del servicio y, a continuación, elija Habilitar el acceso de confianza.
3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS Service Catalog que ahora pueden habilitar ese servicio usando su consola para trabajar con AWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para habilitar el acceso del servicio de confianza:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar AWS Service Catalog como servicio de confianza con Organizations.

```
$ aws organizations enable-aws-service-access \
```

```
    --service-principal servicecatalog.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- API de AWS: EnableAWSServiceAccess

Desactivar el acceso de confianza con Service Catalog

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Si desactiva el acceso de confianza mediante AWS Organizations mientras utiliza 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 AWS Service Catalog o herramientas AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola AWS Service Catalog o herramientas para deshabilitar la integración con Organizations. Esto permite a AWS Service Catalog realizar 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 por AWS Service Catalog.
> Si desactiva el acceso de confianza mediante la consola o las herramientas de AWS Service Catalog, no es necesario completar estos pasos.

Para desactivar el acceso de confianza mediante la CLI de Service Catalog o el SDK de AWS

Llame a uno de los siguientes comandos u operaciones:

- AWS CLI: aws servicecatalog disable-aws-organizations-access
- SDK de AWS: DisableAWSOrganizationsAccess

Puede deshabilitar el acceso de confianza mediante la consola AWS Organizations, la ejecución de una AWS CLI de Organizations, o llamando a una operación de API de Organizations en uno de los SDK de AWS.

AWS Management Console

Para deshabilitar 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Services (Servicios), busque la fila de AWS Service Catalog y, a continuación, elija el nombre del servicio.
3. Elija Deshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, ingrese **`disable`** en el cuadro y, a continuación, elija Deshabilitar el acceso de confianza.
5. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS Service Catalog que ahora pueden deshabilitar ese servicio usando su consola o herramientas para trabajar con AWS Organizations.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar AWS Service Catalog como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal servicecatalog.amazonaws.com
  ```

  Este comando no genera ninguna salida si 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 para ayudarle a integrar Service Quotas con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguientes Rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite que Service Quotas realice operaciones admitidas dentro de las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Service Quotas y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForServiceQuotas`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo 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 otros servicios de 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.

Puede habilitar el acceso de confianza mediante Service Quotas.

Puede habilitar el acceso de confianza mediante la consola Service Quotas, la AWS CLI o el SDK:

- Para habilitar el acceso de confianza mediante la consola Service Quotas.

  Inicie sesión en su cuenta de administración de AWS Organizations y, a continuación, configure 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 Quotas AWS CLI o SDK

  Llame al siguiente comando u operación:
  - AWS CLI: aws service-quotas associate-service-quota-template
  - SDK de AWS: AssociateServiceQuotaTemplate

AWS IAM Identity Center y AWS Organizations

AWS IAM Identity Center proporciona acceso de inicio de sesión único para todas sus 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 de AWS con sus nombres de usuario y contraseñas de Active Directory. Desde el portal de acceso de AWS, los usuarios tienen acceso a todas las Cuentas de AWS y aplicaciones en la nube para las que tienen permisos.

Para obtener más información acerca de IAM Identity Center, consulte la Guía del usuario de AWS IAM Identity Center.

Utilice la siguiente información para ayudarle a integrar AWS IAM Identity Center con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a IAM Identity Center realizar operaciones compatibles en las cuentas de su organización.

Puede eliminar o modificar este rol solo si desactiva el acceso de confianza entre IAM Identity Center y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForSSO`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios de IAM Identity Center conceden acceso a las siguientes entidades principales de servicio:

- `sso.amazonaws.com`

Habilitar el acceso de confianza con IAM Identity Center

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso de confianza mediante la consola de AWS IAM Identity Center o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola AWS IAM Identity Center o herramientas para habilitar la integración con Organizations. Esto permite a AWS IAM Identity Center 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 IAM Identity Center. Para obtener más información, consulte esta nota.
> Si habilita el acceso de confianza mediante la consola o las herramientas de AWS IAM Identity Center, no es necesario completar estos pasos.

IAM Identity Center requiere un acceso de confianza con AWS Organizations para funcionar. El acceso de confianza se habilita al configurar IAM Identity Center. Para obtener más información, consulte Comienzo - Paso 1: Habilitar AWS IAM Identity Center en la Guía del usuario AWS IAM Identity Center.

Puede habilitar el acceso de confianza mediante la consola AWS Organizations, ejecutando un comando AWS CLI, o llamando a una operación de API en uno de los SDK de AWS.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila de AWS IAM Identity Center, elija el nombre del servicio y, a continuación, elija Habilitar el acceso de confianza.
3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS IAM Identity Center que ahora pueden habilitar ese servicio usando su consola para trabajar con AWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para habilitar el acceso del servicio de confianza:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar AWS IAM Identity Center como servicio de confianza con Organizations.

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

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Desactivar el acceso de confianza con IAM Identity Center

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

IAM Identity Center requiere un acceso de confianza con AWS Organizations para operar. Si desactiva el acceso de confianza con IAM Identity Center mientras utiliza AWS Organizations, este deja de funcionar porque no puede obtener acceso a la organización. Los usuarios no pueden utilizar IAM Identity Center para tener acceso a las cuentas. Los roles creados por IAM Identity Center se mantienen, pero el servicio IAM Identity Center no puede obtener acceso a ellos. Los roles vinculados al servicio de IAM Identity Center permanecen. Si vuelve a habilitar el acceso de confianza, IAM Identity Center seguirá funcionando como lo hacía antes sin necesidad de volver a configurar el servicio.

Si elimina una cuenta de su organización, IAM Identity Center limpia automáticamente los metadatos y los recursos, como su rol vinculada al servicio. Una cuenta independiente que se elimina de una organización deja de funcionar con IAM Identity Center.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza mediante la consola AWS Organizations, la ejecución de una AWS CLI de Organizations, o llamando a una operación de API de Organizations en uno de los SDK de AWS.

AWS Management Console

Para deshabilitar 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Services (Servicios), busque la fila de AWS IAM Identity Center y, a continuación, elija el nombre del servicio.
3. Elija Deshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, ingrese **`disable`** en el cuadro y, a continuación, elija Deshabilitar el acceso de confianza.
5. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS IAM Identity Center que ahora pueden deshabilitar ese servicio usando su consola o herramientas para trabajar con AWS Organizations.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar AWS IAM Identity Center como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal sso.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.

- API de AWS: DisableAWSServiceAccess

Habilitar una cuenta de administrador delegado para IAM Identity Center

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 IAM Identity Center que, de lo contrario, solo podrían realizarlas los usuarios o roles en la cuenta de administración de la organización. Esto le ayuda a separar la gestión de la organización de la de IAM Identity Center.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado para IAM Identity Center en la organización.

Para obtener más información sobre cómo habilitar una cuenta de administrador delegado para IAM Identity Center, consulte Administrar un delegado en la Guía del usuario de AWS IAM Identity Center.

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. Las siguientes capacidades de Systems Manager funcionan con Organizations en todas las Cuentas de AWS de su organización:

- Systems Manager Explorer es un panel de operaciones personalizable que le ofrece información acerca de sus recursos de AWS. Puede sincronizar los datos de las operaciones entre todas las Cuentas de AWS de su organización mediante Organizations y Systems Manager Explorer. Para obtener más información, consulte el Systems Manager Explorer en la Guía del usuario de AWS Systems Manager.
- Systems Manager Change Manager es un marco empresarial de administración de cambios con el que se pueden solicitar, aprobar, implementar e informar los cambios operativos de la configuración y la infraestructura de la aplicación. Para obtener más información, consulte Cambiar administrador de AWS Systems Manager en la Guía del usuario de AWS Systems Manager.
- Systems Manager OpsCenter proporciona una ubicación central donde los ingenieros de operaciones y profesionales de TI pueden ver, investigar y resolver los elementos de trabajo operativos (OpsItems) relacionados con los recursos de AWS. Cuando utiliza OpsCenter con Organizations, puede trabajar con OpsItems desde una cuenta de administración (ya sea una cuenta de administración de Organizations o una cuenta de administrador delegado de Systems Manager) y otra cuenta distinta en una misma sesión. Una vez configurados, los usuarios pueden realizar los siguientes tipos de acciones:
  - Crear, ver y actualizar OpsItems en otra cuenta.
  - Ver información detallada sobre los recursos de AWS que se especifican en OpsItems en otra cuenta.
  - Iniciar los manuales de procedimientos de Systems Manager Automation para solucionar problemas con los recursos de AWS en otra cuenta.

  Para obtener más información, consulte AWS Systems Manager OpsCenter en la Guía del usuario de AWS Systems Manager.

Utilice la siguiente información para ayudarle a integrar AWS Systems Manager con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguientes Rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a Systems Manager realizar operaciones compatibles dentro de las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Systems Manager y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForAmazonSSM_AccountDiscovery`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo 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.

Puede habilitar el acceso de confianza mediante las herramientas Organizations.

Puede habilitar el acceso de confianza mediante la consola AWS Organizations, ejecutando un comando AWS CLI, o llamando a una operación de API en uno de los SDK de AWS.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila de AWS Systems Manager, elija el nombre del servicio y, a continuación, elija Habilitar el acceso de confianza.
3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS Systems Manager que ahora pueden habilitar ese servicio usando su consola para trabajar con AWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para habilitar el acceso del servicio de confianza:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar AWS Systems Manager como servicio de confianza con Organizations.

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

  Este comando no genera ninguna salida si 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, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Systems Manager requiere un acceso de confianza con AWS Organizations para 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.

Solo puede deshabilitar el acceso de confianza mediante las herramientas de Organizations.

Puede deshabilitar el acceso de confianza mediante la consola AWS Organizations, la ejecución de una AWS CLI de Organizations, o llamando a una operación de API de Organizations en uno de los SDK de AWS.

AWS Management Console

Para deshabilitar 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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Services (Servicios), busque la fila de AWS Systems Manager y, a continuación, elija el nombre del servicio.
3. Elija Deshabilitar el acceso de confianza.
4. En el cuadro de diálogo de confirmación, ingrese **`disable`** en el cuadro y, a continuación, elija Deshabilitar el acceso de confianza.
5. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS Systems Manager que ahora pueden deshabilitar ese servicio usando su consola o herramientas para trabajar con AWS Organizations.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar AWS Systems Manager como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal ssm.amazonaws.com
  ```

  Este comando no genera ninguna salida si 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, solo 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 de Systems Manager.

Si utiliza Change Manager en una organización, debe utilizar una cuenta de administrador delegado. 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 de administrador delegado se encarga de las actividades de cambio en toda la organización. Cuando se configura la organización para utilizar Change Manager, se debe especificar cuál de sus cuentas llevará a cabo este rol. No tiene que ser la cuenta de gestión de la organización. La cuenta de administrador delegado no es necesaria si se utiliza el Administrador de cambios con una sola cuenta.

Para designar una cuenta de miembro como administrador delegado, consulte los siguientes temas en la Guía del usuario de AWS Systems Manager:

- Para el Explorador y OpsCenter, consulte Configuración de un administrador delegado.
- Para el Administrador de cambios de Systems Manager, consulte Configuración de una organización y una cuenta delegada para el Administrador de cambios.

Políticas de etiquetas y AWS Organizations

Las políticas de etiquetas son un tipo de política en AWS Organizations que le puede ayudar a estandarizar las etiquetas en todos los recursos en las cuentas de su organización. Para obtener más información acerca de las políticas de etiquetas, consulte Políticas de etiquetas.

Utilice la siguiente información para ayudarle a integrar políticas de etiquetas con AWS Organizations.

Los principales de servicios utilizados por los roles vinculados a servicios

Organizations interactúa con las etiquetas adjuntas a los recursos mediante la siguiente entidad de servicio.

- `tagpolicies.tag.amazonaws.com`

Habilitación del acceso de confianza para las políticas de etiquetas

Puede habilitar el acceso de confianza mediante la habilitación de políticas de etiquetas en la organización o mediante la consola de AWS Organizations.

> **Important**
>
> Le recomendamos encarecidamente que habilite el acceso de confianza mediante políticas de etiquetas. Esto permite a Organizations realizar las tareas de configuración necesarias.

Puede habilitar el acceso de confianza para las políticas de etiquetas habilitando el tipo de política de etiqueta en la consola de AWS Organizations. Para obtener más información, consulte Habilitar un tipo de política .

Puede habilitar el acceso de confianza mediante la consola AWS Organizations, ejecutando un comando AWS CLI, o llamando a una operación de API en uno de los SDK de AWS.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila de Políticas de etiquetas, elija el nombre del servicio y, a continuación, elija Habilitar el acceso de confianza.
3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de políticas de etiquetas que ahora puede habilitar ese servicio mediante su consola para trabajar con AWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para habilitar el acceso del servicio de confianza:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar políticas 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 si se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Deshabilitación del acceso de confianza con políticas de etiquetas

Puede deshabilitar el acceso de confianza para las políticas de etiquetas deshabilitando el tipo de política de etiqueta en la consola de AWS Organizations. Para obtener más información, consulte Deshabilitar un tipo de política .

AWS Trusted Advisor y AWS Organizations

AWS Trusted Advisor inspecciona el entorno de AWS y realiza recomendaciones cuando surge la oportunidad de ahorrar dinero, mejorar el rendimiento y la disponibilidad del sistema o ayudar a cerrar los errores de seguridad. Cuando se integra con Organizations, puede recibir resultados de control de Trusted Advisor de todas las cuentas de su organización y descargar informes para ver los resúmenes de sus comprobaciones y de los recursos afectados.

Para obtener más información, consulte Vista organizativa para AWS Trusted Advisor en la Guía del usuario de AWS Support.

Utilice la siguiente información para ayudarle a integrar AWS Trusted Advisor con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguientes Rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a Trusted Advisor realizar operaciones compatibles en las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre Trusted Advisor y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForTrustedAdvisorReporting`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios de Trusted Advisor conceden acceso a las siguientes entidades de servicio:

- `reporting.trustedadvisor.amazonaws.com`

Habilitar el acceso de confianza con Trusted Advisor

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso de confianza solamente mediante AWS Trusted Advisor.

Para habilitar el acceso de confianza desde la Trusted Advisor consola

Consulte Habilitación de la vista organizativa en la Guía del usuario de AWS Support.

Deshabilitación del acceso con Trusted Advisor

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Después de deshabilitar esta característica, Trusted Advisor deja de registrar la información de comprobación de 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 AWS Trusted Advisor o herramientas AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola AWS Trusted Advisor o herramientas para deshabilitar la integración con Organizations. Esto permite a AWS Trusted Advisor realizar 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 por AWS Trusted Advisor.
Si desactiva el acceso de confianza mediante la consola o las herramientas de AWS Trusted Advisor, no es necesario completar estos pasos.

Para habilitar el acceso de confianza mediante la consola Trusted Advisor

Consulte Deshabilitar la vista organizativa en la Guía del usuario de AWS Support.

Puede deshabilitar el acceso de confianza ejecutando un comando de Organizations AWS CLI, o bien llamando a una operación de API de Organizations en uno de los AWS SDK.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar AWS Trusted Advisor como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal reporting.trustedadvisor.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

Habilitar una cuenta de administrador delegado para Trusted Advisor

Cuando se designa una cuenta de miembro como administrador delegado de la organización, los usuarios y los roles de la cuenta designada pueden administrar los metadatos de la Cuenta de AWS de otras cuentas de miembro de la organización. Si no habilita una cuenta de administrador delegado, estas tareas solo las puede realizar la cuenta de administración de la organización. Esto le ayuda a separar la administración de la organización de la administración de los detalles de la cuenta.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado para Trusted Advisor en la organización

Para obtener más información sobre cómo habilitar una cuenta de administrador delegado para Trusted Advisor, consulte Registro de administradores delegados en la Guía del usuario de AWS Support.

AWS CLI, AWS API

Si desea configurar una cuenta de administrador delegada mediante el CLI AWS o uno de los SDK de AWS, puede usar los siguientes comandos:

- AWS CLI:

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

- AWS SDK: llame a la operación `RegisterDelegatedAdministrator` de Organizations y al número de ID de la cuenta de miembro e identifique la entidad principal del servicio de cuenta `account.amazonaws.com` como parámetros.

Desactivación de un administrador delegado para Trusted Advisor

Puede remover una cuenta de administrador delegado utilizando la consola de Trusted Advisor, o utilizando la operación `DeregisterDelegatedAdministrator` de la CLI o SDK de Organizations. Para obtener información sobre cómo deshabilitar la cuenta de Trusted Advisor del administrador delegado mediante la consola de Trusted Advisor, consulte Anulación del registro de administradores delegados en la Guía del usuario de AWS Support.

AWS Well-Architected Tool y AWS Organizations

AWS Well-Architected Tool ayuda a documentar el estado de sus cargas de trabajo y las compara con las prácticas recomendadas arquitectónicas de AWS más recientes.

El uso de AWS Well-Architected Tool con Organizations permite que tanto los clientes de AWS Well-Architected Tool como los de Organizations simplifiquen el proceso de compartir los recursos de AWS Well-Architected Tool con otros miembros de su organización.

Para obtener más información, consulte Cómo compartir los recursos de AWS Well-Architected Tool en la Guía del usuario de AWS Well-Architected Tool.

Utilice la siguiente información para ayudarle a integrar AWS Well-Architected Tool con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguientes Rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite a AWS WA Tool realizar operaciones compatibles en las cuentas de su organización.

Puede eliminar o modificar este rol solo si deshabilita el acceso de confianza entre AWS WA Tool y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForWellArchitected`

La política de roles de servicio es `AWSWellArchitectedOrganizationsServiceRolePolicy`

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo puede ser asumido por las entidades de servicio autorizadas por las relaciones de confianza definidas para el rol. Los roles vinculados a servicios de AWS WA Tool conceden acceso a las siguientes entidades de servicio:

- `wellarchitected.amazonaws.com`

Habilitar el acceso de confianza con AWS WA Tool

Permite la actualización de AWS WA Tool para reflejar los cambios jerárquicos de una organización.

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Puede habilitar el acceso de confianza mediante la consola de AWS Well-Architected Tool o la consola de AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola AWS Well-Architected Tool o herramientas para habilitar la integración con Organizations. Esto permite a AWS Well-Architected Tool 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 Well-Architected Tool. Para obtener más información, consulte esta nota.
> Si habilita el acceso de confianza mediante la consola o las herramientas de AWS Well-Architected Tool, no es necesario completar estos pasos.

Para habilitar el acceso de confianza desde la AWS WA Tool consola

Consulte Cómo compartir los recursos de AWS Well-Architected Tool en la Guía del usuario de AWS Well-Architected Tool.

Puede habilitar el acceso de confianza mediante la consola AWS Organizations, ejecutando un comando AWS CLI, o llamando a una operación de API en uno de los SDK de AWS.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila de AWS Well-Architected Tool, elija el nombre del servicio y, a continuación, elija Habilitar el acceso de confianza.
3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si usted es el administrador solamente de AWS Organizations, dígale al administrador de AWS Well-Architected Tool que ahora pueden habilitar ese servicio usando su consola para trabajar con AWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para habilitar el acceso del servicio de confianza:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar AWS Well-Architected Tool como servicio de confianza con Organizations.

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

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Deshabilitación del acceso con AWS WA Tool

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Puede deshabilitar el acceso de confianza mediante la AWS Well-Architected Tool o herramientas AWS Organizations.

> **Important**
>
> Le recomendamos que, siempre que sea posible, utilice la consola AWS Well-Architected Tool o herramientas para deshabilitar la integración con Organizations. Esto permite a AWS Well-Architected Tool realizar 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 por AWS Well-Architected Tool.
> Si desactiva el acceso de confianza mediante la consola o las herramientas de AWS Well-Architected Tool, no es necesario completar estos pasos.

Para habilitar el acceso de confianza mediante la consola AWS WA Tool

Consulte Cómo compartir los recursos de AWS Well-Architected Tool en la Guía del usuario de AWS Well-Architected Tool.

Puede deshabilitar el acceso de confianza ejecutando un comando de Organizations AWS CLI, o bien llamando a una operación de API de Organizations en uno de los AWS SDK.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

  Puede ejecutar el siguiente comando para deshabilitar AWS Well-Architected Tool como servicio de confianza con Organizations.

  ```
  $ aws organizations disable-aws-service-access \
      --service-principal wellarchitected.amazonaws.com
  ```

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: DisableAWSServiceAccess

Amazon VPC IP Address Manager (IPAM) y AWS Organizations

Amazon VPC IP Address Manager (IPAM) es una característica de VPC que facilita la planificación, el seguimiento y el monitoreo de las direcciones IP de las cargas de trabajo de AWS.

Utilizar AWS Organizations permite monitorear el uso de direcciones IP en toda la organización y compartir grupos de direcciones IP entre las cuentas de miembro.

Para obtener más información, consulte Integración de IPAM con AWS Organizations en la Guía del usuario de Amazon VPC IPAM.

Utilice la siguiente información como ayuda para integrar Amazon VPC IP Address Manager (IPAM) con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado a servicio se crea automáticamente en la cuenta de administración de su organización y en cada cuenta de miembro cuando se integra IPAM con AWS Organizations bien mediante la consola de IPAM o bien utilizando la API `EnableIpamOrganizationAdminAccount` de IPAM.

- `AWSServiceRoleForIPAM`

Para obtener más información, consulte Roles vinculados a servicios de IPAM en la Guía del usuario de Amazon VPC IPAM.

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo 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 IPAM conceden acceso a las siguientes entidades principales de servicio:

- `ipam.amazonaws.com`

Para habilitar el acceso de confianza con IPAM

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

> **Note**
>
> Cuando se designa un administrador delegado para IPAM, se habilita automáticamente el acceso de confianza para IPAM en su organización.
> IPAM requiere acceso de confianza a AWS Organizations para que se pueda designar una cuenta de miembro que sea el administrador delegado de este servicio para la organización.

Puede habilitar el acceso de confianza utilizando únicamente las herramientas de Amazon VPC IP Address Manager (IPAM).

Si se integra IPAM con AWS Organizations mediante la consola de IPAM o utilizando la API `EnableIpamOrganizationAdminAccount` de IPAM, automáticamente se concede

acceso de confianza a IPAM. Conceder acceso de confianza crea el rol vinculado a servicio `AWSServiceRoleForIPAM` en la cuenta de administración y en todas las cuentas de miembro de la organización. IPAM utiliza el rol vinculado a servicio para monitorear los CIDR asociados a los recursos de red de EC2 de su organización y para almacenar métricas relacionadas con IPAM en Amazon CloudWatch. Para obtener más información, consulte Roles vinculados a servicios de IPAM en la Guía del usuario de Amazon VPC IPAM.

Para obtener instrucciones sobre cómo habilitar el acceso de confianza, consulte Integración de IPAM con AWS Organizations en la Guía del usuario de Amazon VPC IPAM.

> **Note**
>
> No puede habilitar el acceso de confianza con IPAM mediante la consola de AWS Organizations o con la API `EnableAWSServiceAccess`.

Para desactivar el acceso de confianza con IPAM

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Solo un administrador de la cuenta de administración de AWS Organizations puede desactivar el acceso de confianza con IPAM mediante la API `disable-aws-service-access` de AWS Organizations.

Para obtener información sobre cómo desactivar los permisos de cuentas de IPAM y eliminar el rol vinculado a servicio, consulte Roles vinculados a servicios de IPAM en la Guía del usuario de Amazon VPC IPAM.

Puede deshabilitar el acceso de confianza ejecutando un comando de Organizations AWS CLI, o bien llamando a una operación de API de Organizations en uno de los AWS SDK.

AWS CLI, AWS API

Para deshabilitar el acceso de confianza mediante Organizations CLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para deshabilitar el acceso del servicio de confianza:

- AWS CLI: disable-aws-service-access

Puede ejecutar el siguiente comando para desactivar Amazon VPC IP Address Manager (IPAM) como servicio de confianza con Organizations.

```
$ aws organizations disable-aws-service-access \
    --service-principal ipam.amazonaws.com
```

Este comando no genera ninguna salida si se realiza correctamente.

- API de AWS: DisableAWSServiceAccess

Habilitación de una cuenta de administrador delegado para IPAM

La cuenta de administrador delegado de IPAM es responsable de crear los grupos de IPAM y de direcciones IP, administrar y monitorear el uso de direcciones IP en la organización, y compartir grupos de direcciones IP entre las cuentas de miembro. Para obtener más información, consulte Integración de IPAM con AWS Organizations en la Guía del usuario de Amazon VPC IPAM.

Solo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado para IPAM.

Puede especificar una cuenta de administrador delegado desde la consola de IPAM o mediante la API `enable-ipam-organization-admin-account`. Para obtener más información, consulte enable-ipam-organization-admin-account en la Referencia de los comandos de AWS AWS CLI.

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado para IPAM en la organización

Para configurar un administrador delegado mediante la consola de IPAM, consulte Integración de IPAM con AWS Organizations en la Guía del usuario de Amazon VPC IPAM.

Desactivación de un administrador delegado para IPAM

Solo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado para IPAM.

Para eliminar un administrador delegado mediante AWS AWS CLI, consulte disable-ipam-organization-admin-account en la Referencia de los comandos de AWS AWS CLI .

Para desactivar la cuenta de IPAM de administrador delegado mediante la consola de IPAM, consulte (Integración de IPAM con AWS Organizations en la Guía del usuario de Amazon VPC IPAM.

Analizador de accesibilidad de Amazon VPC y AWS Organizations

El Analizador de accesibilidad es una herramienta de análisis de configuración que le permite realizar pruebas de conectividad entre un recurso de origen y un recurso de destino en las nubes privadas virtuales (VPC).

El uso de AWS Organizations junto con el Analizador de accesibilidad le permite trazar rutas a través de las cuentas de sus organizaciones.

Para obtener más información, consulte Cross-account analyses for Reachability Analyzer (Análisis entre cuentas para el Analizador de accesibilidad) en la Reachability Analyzer user guide (Guía del usuario del analizador de accesibilidad).

Utilice la siguiente información para ayudarle a integrar el analizador de accesibilidad con AWS Organizations.

Roles vinculados al servicio creados al habilitar la integración

El siguiente rol vinculado al servicio se crea automáticamente en la cuenta de administración de su organización cuando habilita el acceso de confianza. Este rol permite al Analizador de accesibilidad realizar operaciones compatibles en las cuentas de su organización.

Puede eliminar o modificar este rol solo si desactiva el acceso de confianza entre el Analizador de accesibilidad y Organizations, o si elimina la cuenta de miembro de la organización.

- `AWSServiceRoleForReachabilityAnalyzer`

Para obtener más información, consulte Cross-account analyses for Reachability Analyzer (Análisis entre cuentas para el Analizador de accesibilidad) en la Reachability Analyzer user guide (Guía del usuario del analizador de accesibilidad).

Los principales de servicios utilizados por los roles vinculados a servicios

El rol vinculado al servicio de la sección anterior solo 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 el Analizador de accesibilidad otorgan acceso a las siguientes entidades de servicio:

- `reachabilityanalyzer.networkinsights.amazonaws.com`

Para habilitar el acceso de confianza con el Analizador de accesibilidad

Para obtener información acerca de los permisos necesarios para habilitar el acceso de confianza, consulte Permisos necesarios para habilitar el acceso de confianza.

Al designar un administrador delegado para el Analizador de accesibilidad, se habilita automáticamente el acceso de confianza para el Analizador de accesibilidad de su organización.

El Analizador de accesibilidad requiere acceso de confianza a AWS Organizations para que se pueda designar una cuenta de miembro que sea el administrador delegado de este servicio para la organización.

Important

- Puede habilitar el acceso de confianza mediante la consola del Analizador de accesibilidad o la consola de Organizations. No obstante, le recomendamos encarecidamente que utilice la consola del Analizador de accesibilidad o la API de `EnableMultiAccountAnalysisForAwsOrganization` para permitir la integración con Organizations. Esto permite al Analizador de accesibilidad realizar cualquier configuración que requiera, como la creación de los recursos necesarios para el servicio.
- Conceder acceso de confianza crea el rol vinculado a servicio `AWSServiceRoleForReachabilityAnalyzer` en la cuenta de administración y en todas las cuentas de miembro de la organización. El Analizador de accesibilidad utiliza la función vinculada al servicio para permitir a la dirección y al administrador delegado ejecutar análisis de conectividad entre cualquier recurso de la organización. El Analizador de accesibilidad es capaz de tomar instantáneas de los elementos de red de las cuentas de una organización para responder a consultas de conectividad.
- Para obtener más información e instrucciones sobre cómo habilitar el acceso de confianza a través del Analizador de accesibilidad, consulte Cross-account analyses for Reachability Analyzer (Análisis de cuentas cruzadas para el Analizador de accesibilidad) en la Reachability Analyzer user guide (Guía del usuario del Analizador de accesibilidad).

Puede habilitar el acceso de confianza mediante la consola AWS Organizations, ejecutando un comando AWS CLI, o llamando a una operación de API en uno de los SDK de AWS.

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 un rol de IAM; o iniciar sesión como usuario raíz (no se recomienda) en la cuenta de administración de la organización.
2. En la página Servicios, busque la fila de Analizador de accesibilidad de VPC, elija el nombre del servicio y, a continuación, elija Habilitar el acceso de confianza.
3. En el cuadro de diálogo de confirmación, habilite Mostrar la opción para habilitar el acceso de confianza, introduzca **`enable`** en el cuadro y, a continuación, elija Permitir el acceso de confianza.
4. Si usted es el administrador solamente de AWS Organizations, dígale al administrador del Analizador de accesibilidad que ahora pueden habilitar ese servicio usando su consola para trabajar con AWS Organizations.

AWS CLI, AWS API

Para habilitar el acceso de confianza mediante OrganizationsCLI/SDK

Puede utilizar los siguientes comandos de la AWS CLI o las operaciones de API para habilitar el acceso del servicio de confianza:

- AWS CLI: enable-aws-service-access

  Puede ejecutar el siguiente comando para habilitar el Analizador de accesibilidad como servicio de confianza con Organizations.

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

  Este comando no genera ninguna salida si se realiza correctamente.
- API de AWS: EnableAWSServiceAccess

Para desactivar el acceso de confianza mediante el Analizador de accesibilidad

Para obtener información acerca de los permisos necesarios para deshabilitar el acceso de confianza, consulte Permisos necesarios para deshabilitar el acceso de confianza.

Puede desactivar el acceso de confianza mediante la consola del Analizador de accesibilidad (recomedado) o la consola de Organizations. Para desactivar el acceso de confianza mediante la consola del Analizador de accesibilidad, consulte Cross-account analyses for Reachability Analyzer (Análisis de cuentas cruzadas para el Analizador de accesibilidad) en la Reachability Analyzer user guide (Guía del usuario del Analizador de accesibilidad).

Para habilitar una cuenta de administrador delegado para el Analizador de accesibilidad

La cuenta de administrador delegado puede ejecutar análisis de conectividad en cualquiera de los recursos de la organización. Para obtener más información, consulte Integración del Analizador de accesibilidad con AWS Organizations en la Guía del usuario del Analizador de accesibilidad.

Solo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado para el Analizador de accesibilidad.

Puede especificar una cuenta de administrador delegado desde la consola del Analizador de accesibilidad o mediante la API `RegisterDelegatedAdministrator`. Para obtener más información, consulte RegisterDelegatedAdministrator en la Organizations Command Reference (Referencia de comandos de Organizations).

> **Permisos mínimos**
>
> Solo un usuario o rol de la cuenta de administración de Organizations puede configurar una cuenta de miembro como administrador delegado para el Analizador de accesibilidad en la organización

Para configurar un administrador delegado mediante la consola del Analizador de accesibilidad, consulte Integración del Analizador de accesibilidad con AWS Organizations en la Guía del usuario del Analizador de accesibilidad.

Desactivación de un administrador delegado para el Analizador de accesibilidad

Solo un administrador de la cuenta de administración de la organización puede configurar un administrador delegado para el Analizador de accesibilidad.

Puede eliminar el administrador delegado mediante la consola o la API del Analizador de accesibilidad, o bien mediante la operación `DeregisterDelegatedAdministrator` de la CLI de Organizations o el SDK.

Para desactivar la cuenta de administrador delegado del Analizador de accesibilidad mediante la consola del Analizador de accesibilidad, consulte Cross-account analyses for Reachability Analyzer (Análisis de cuentas cruzadas para el Analizador de accesibilidad) en la Reachability Analyzer user guide (Guía del usuario del Analizador de accesibilidad).

Administrador delegado para los servicios de AWS que funcionan con Organizations

Le recomendamos que utilice la cuenta de administración de AWS Organizations y sus usuarios y roles únicamente para las tareas que deba realizar dicha cuenta. También le recomendamos que almacene sus recursos de AWS en otras cuentas de miembros de la organización y los mantenga fuera de la cuenta de administración. Esto se debe a que las características de seguridad, como las políticas de control de servicios (SCP) de las organizaciones, no restringen ni los usuarios ni los roles de la cuenta de administración. Separar los recursos de su cuenta de administración también lo ayudará a comprender los cargos de sus facturas.

Muchos servicios de AWS que se integran con Organizations le permiten reducir el uso de la cuenta de administración. Estos servicios le permiten registrar una o más cuentas de miembros como administradores que pueden administrar todas las cuentas de la organización utilizadas en el servicio. Estas cuentas se denominan administradores delegados para ese servicio específico. Al registrar una cuenta de miembro como administrador delegado de un servicio de AWS, permite que esa cuenta tenga algunos permisos administrativos para ese servicio, así como permisos para las acciones de solo lectura de la organización.

Antes de registrar una cuenta como administrador delegado de un servicio:

- Confirme que el servicio es compatible con los administradores delegados. Consulte la tabla de AWS servicios que puede utilizar con AWS Organizations para obtener información sobre los servicios que admiten a los administradores delegados.
- Habilite el acceso de confianza para ese servicio.

> **Note**
>
> Para obtener información sobre cómo habilitar un servicio para un administrador delegado, consulte la tabla de AWS servicios que puede utilizar con AWS Organizations y seleccione el enlace Más información de la columna Admite administradores delegados de ese servicio.

Permisos concedidos a cuentas de administrador delegado

Cada cuenta de administrador delegado específica de un servicio tiene permisos concedidos por ese servicio. Para obtener más información, consulte la tabla AWS servicios que puede utilizar con AWS Organizations y seleccione el enlace Más información en la columna Admite administradores delegados de ese servicio.

Una cuenta de administrador delegado también tiene estos permisos de solo lectura:

- `DescribeAccount`
- `DescribeCreateAccountStatus`
- `DescribeEffectivePolicy`
- `DescribeHandshake`
- `DescribeOrganization`
- `DescribeOrganizationalUnit`
- `DescribePolicy`
- `DescribeResourcePolicy`
- `ListAccounts`
- `ListAccountsForParent`
- `ListAWSServiceAccessForOrganization`
- `ListChildren`
- `ListCreateAccountStatus`
- `ListDelegatedAdministrators`
- `ListDelegatedServicesForAccount`
- `ListHandshakesForAccount`
- `ListHandshakesForOrganization`
- `ListOrganizationalUnitsForParent`
- `ListParents`
- `ListPolicies`
- `ListPoliciesForTarget`
- `ListRoots`
- `ListTagsForResource`

- `ListTargetsForPolicy`

Estos permisos le permiten ver, pero no cambiar, los siguientes elementos de la consola:

- Estructura de la organización, todas las cuentas y unidades organizativas y políticas organizativas
- Pertenencias
- Todas las cuentas y unidades organizativas.
- Políticas organizativas

Seguridad en AWS Organizations

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores independientes prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad aplicables AWS Organizations, consulte los AWS servicios incluidos en el ámbito de aplicación por programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Organizations. En los siguientes temas, se le mostrará cómo configurar Organizations para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger los recursos de su Organización.

Temas

- AWS PrivateLink para AWS Organizations
- AWS Identity and Access Management y AWS Organizations
- Registro y monitoreo en AWS Organizations
- Validación de conformidad en AWS Organizations
- Resiliencia en AWS Organizations
- Seguridad de la infraestructura en AWS Organizations

AWS PrivateLink para AWS Organizations

Con AWS PrivateLink for AWS Organizations, puede acceder al AWS Organizations servicio desde la Nube Privada Virtual (VPC) sin tener que cruzar la Internet pública.

Amazon VPC le permite lanzar AWS recursos en una red virtual personalizada. Puede utilizar una VPC para controlar la configuración de red, como el intervalo de direcciones IP, las subredes, las tablas de enrutamiento y las puertas de enlace de red. Para obtener más información sobre VPC, consulte la Guía del usuario de Amazon VPC.

Para conectar su Amazon VPC AWS Organizations, primero debe definir un punto de enlace de la VPC de interfaz (puntos de enlace de interfaz). Los puntos de enlace de la interfaz se representan mediante una o más interfaces de red elásticas (elastic network interfaces, ENI) a las que se asignan direcciones IP privadas desde subredes de la VPC. Las solicitudes de su VPC a puntos de enlace a AWS Organizations través de la interfaz permanecen en la red de Amazon.

Para obtener información general sobre los puntos de enlace de la interfaz, consulte Acceder a un AWS servicio mediante un punto de enlace de VPC de interfaz en la Guía del usuario de Amazon VPC.

Temas

- Limitaciones y restricciones de la forma AWS PrivateLinkAWS Organizations
- Creación de un punto de conexión de VPC
- Creación de una política de punto de conexión de VPC para AWS Organizations

Limitaciones y restricciones de la forma AWS PrivateLinkAWS Organizations

Se aplican limitaciones de VPC a AWS PrivateLink . AWS Organizations Para obtener más información, consulte Acceder a un AWS servicio mediante un punto final de VPC de interfaz y AWS PrivateLink cuotas en la Guía del usuario de Amazon VPC. Además, se aplican las siguientes restricciones:

- Disponible solo en la región `us-east-1`
- No es compatible con Transport Layer Security (TLS) 1.1

Creación de un punto de conexión de VPC

Puede crear un AWS Organizations punto de conexión en su VPC mediante la consola de Amazon VPC, el AWS Command Line Interface () o.AWS CLI AWS CloudFormation

Para obtener información sobre cómo crear y configurar un punto de conexión mediante la consola de Amazon VPC o la AWS CLI, consulte Crear un punto de enlace de VPC en la Guía del usuario de Amazon VPC. Para obtener información sobre cómo crear y configurar un punto final mediante AWS CloudFormation, consulte el recurso AWS: :EC2: :VPCendpoint en la Guía del usuario.AWS CloudFormation

Al crear un AWS Organizations punto final, utilice lo siguiente como nombre del servicio:

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

Si necesita módulos criptográficos validados por FIPS 140-2 para acceder AWS, utilice el siguiente nombre de servicio AWS Organizations FIPS:

```
com.amazonaws.us-east-1.organizations-fips
```

Creación de una política de punto de conexión de VPC para AWS Organizations

Puede adjuntar una política de punto final a su punto final de VPC que controle el acceso a Organizations. La política especifica la siguiente información:

- La entidad principal que puede realizar acciones.
- Las acciones que se pueden realizar.
- Los recursos en los que se pueden llevar a cabo las acciones.

Para obtener más información, consulte Controlar el acceso a los puntos de enlace de la VPC mediante políticas de puntos de enlace en la Guía del usuario de Amazon VPC.

Ejemplo: política de punto de conexión de VPC para acciones de AWS Organizations

```
{
   "Statement":[
      {
```

```
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "Organizations:DescribeAccount"
         ],
         "Resource":"*"
      }
   ]
}
```

AWS Identity and Access Management y AWS Organizations

El acceso a AWS Organizations requiere credenciales. Estas credenciales deben tener permisos para obtener acceso a los recursos de AWS, como un bucket de Amazon Simple Storage Service (Amazon S3), una instancia de Amazon Elastic Compute Cloud (Amazon EC2) o una unidad organizativa de AWS Organizations. En las secciones siguientes se incluye información detallada acerca de cómo puede utilizar AWS Identity and Access Management (IAM) para ayudar a proteger el acceso a su organización y controlar quién puede administrarla.

Para determinar quién puede administrar las distintas partes de su organización, AWS Organizations utiliza el mismo modelo de permisos basado en IAM que otros servicios de AWS. Como administrador de la cuenta de administración de una organización, puede conceder permisos basados en IAM para realizar tareas de AWS Organizations asociando políticas a usuarios, grupos y funciones en la cuenta de administración. Estas políticas especifican las acciones que pueden realizar esas entidades. Puede asociar una política de permisos de IAM adjuntar un grupo del que el usuario es miembro o directamente a un usuario o rol. 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 de AWS 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 los permisos de AWS Organizations a un Rol de IAM en la cuenta de administración y permitir que el usuario de la cuenta miembro asuma dicho rol. Para obtener información general sobre las políticas de permisos de IAM, consulte Información general sobre políticas del AM en la Guía del usuario de IAM.

Temas

- Autenticación

- Control de acceso
- Administración de permisos en su organización de AWS
- Uso de políticas basadas en identidad (políticas de IAM) para AWS Organizations
- Control de acceso basado en atributos con etiquetas y AWS Organizations

Autenticación

Puede obtener acceso a AWS con los siguientes tipos de identidades:

- Usuario raíz de Cuenta de AWS: cuando se inscribe en AWS, 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**
  >
  > Al registrarse en una Cuenta de AWS, se crea un Usuario raíz de la cuenta de AWS. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario administrativo y utilice únicamente el usuario raíz para realizar tareas que requieran acceso de usuario raíz.

- Usuario de IAM: un usuario de IAM es simplemente una identidad dentro de su Cuenta de AWS que tiene permisos personalizados específicos (por ejemplo, permisos para crear un Amazon Elastic File System). Puede utilizar un nombre de usuario y una contraseña de IAM para iniciar sesión en páginas web seguras de AWS tales como AWS Management Console, foros de discusión de AWS o el Centro de asistencia AWS.

  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 sobre la autenticación de solicitudes, consulte Firmar solicitudes de AWS API en la Guía del usuario de IAM.
- 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 obtener acceso a los recursos y servicios de AWS. 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 de AWS Directory Service, el directorio de usuarios de la empresa o un proveedor de identidad 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 permisos a otra Cuenta de AWS a fin de tener acceso a los recursos de su cuenta. Encontrará un ejemplo de ello en la sección Tutorial: Delegación del acceso entre Cuentas de AWS con roles de IAM de la Guía del usuario de IAM.
- Acceso a servicios de AWS: puede utilizar un rol de IAM de su cuenta para conceder permisos a un servicio de AWS a fin de acceder a los recursos de su cuenta. Por ejemplo, puede crear un rol que permita a Amazon Redshift acceder a un bucket de Amazon S3 en su nombre y, a continuación, cargar los datos almacenados en ese bucket en un clúster de Amazon Redshift. Para obtener más información, consulte Creación de un rol para delegar permisos a un servicio de AWS en la Guía del usuario de IAM.
- Aplicaciones que se ejecutan en Amazon EC2: en lugar de almacenar claves de acceso en la instancia EC2 con el objetivo de que las utilicen aplicaciones que se ejecutan en la instancia y que realizan solicitudes de API de AWS, puede utilizar un rol de IAM a fin de 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 un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias 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) a una cuenta.

En las secciones siguientes, se describe cómo administrar los permisos de AWS Organizations.

- Administración de permisos en su organización de AWS
- Uso de políticas basadas en identidad (políticas de IAM) para AWS Organizations
- Control de acceso basado en atributos con etiquetas y AWS Organizations

Administración de permisos en su organización de AWS

Todos los recursos de AWS, incluidos los nodos raíz, las unidades organizativas, las cuentas y las políticas de una organización, son propiedad de una 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 más información, consulte Prácticas recomendadas de seguridad en 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 rol 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 cómo se corresponden los conceptos de AWS Organizations con los conceptos equivalentes de IAM.

Recursos

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 el elemento `Resource` de una política de permisos de IAM. Para obtener una lista completa de los formatos de ARN de los recursos que se utilizanAWS Organizations, consulte Tipos de recursos definidos AWS Organizations en la Referencia de autorización de servicio.

Operaciones

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. A la mayoría de las operaciones se puede hacer referencia en el elemento `Action` de una política de IAM para controlar quién puede utilizar dicha operación. Para obtener una lista de AWS Organizations las operaciones que se pueden usar como permisos en una política de IAM, consulte Actions defined by AWS Organizations en la Referencia de autorización de servicios.

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 elemento `Condition` de una política de IAM para especificar las circunstancias adicionales que se deben cumplir para que se aplique la instrucción.

Las siguientes claves de condición son especialmente útiles con AWS Organizations:

- `aws:PrincipalOrgID` - simplifica la especificación del elemento `Principal` en una política basada en recursos. Esta clave global proporciona una alternativa a mostrar todos los ID de todas las Cuentas de AWS de una organización. En lugar de mostrar todas las cuentas de la organización, puede especificar el ID de organización 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 las claves de contexto `PrincipalOrgID` en estado AWS global en la Guía del usuario de IAM.

- `aws:PrincipalOrgPaths` - Utiliza esta clave de condición para hacer coincidir los miembros de una raíz de organización específica, una unidad organizativa o sus secundarias. La clave de condición `aws:PrincipalOrgPaths` vuelve como verdadera cuando el elemento principal (usuario raíz, usuario o rol de IAM) 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 sobre las rutas, consulte Comprender la ruta de la AWS Organizations entidad en la Guía del usuario de IAM. Para obtener más información sobre el uso de esta clave de condición, consulte aws: PrincipalOrgPaths en la Guía 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 política de Organizations para que funcionen únicamente en políticas 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 Organizations.

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 utiliza las AWSServiceAccess operaciones de activación AWSServiceAccess o desactivación para activar o desactivar el acceso de confianza con otros AWS servicios. 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 obtener una lista de todas las claves de AWS Organizations condición específicas que se pueden utilizar como permisos en una política de IAM, consulte las claves de condición de la Referencia AWS Organizations de autorización de servicios.

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, la propietaria de los recursos es la Cuenta de AWS de la entidad principal (es decir, el usuario raíz, un usuario de IAM o un rol de IAM) que autentica la solicitud de creación de recursos. Para una organización de AWS, siempre es la cuenta de administración. 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 le concede permisos para crear unidades organizativas, este puede crearlas. Sin embargo, la cuenta de administración, a la que pertenece el usuario, es 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 y crearlos. La cuenta de administración, a la que pertenece el rol (y no el usuario que lo asume), es la propietaria del recurso de unidad organizativa.

Administrar el 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 información sobre la sintaxis y las descripciones de las políticas de IAM, consulte la referencia de la política JSON de IAM en la Guía del usuario de IAM.

Las políticas que se asocian a una identidad de IAM se denominan políticas basadas en la identidad (políticas de IAM). Las políticas que se asocian a un recurso se denominan políticas basadas en recursos. AWS Organizations solamente admite las políticas basadas en identidades (políticas de IAM).

Temas

- Políticas basadas en permiso de identidades (políticas de IAM)
- Políticas basadas en recursos

Políticas basadas en permiso de identidades (políticas de IAM)

Puede asociar políticas a identidades de IAM para permitir que esas identidades realicen operaciones en recursos de AWS. Por ejemplo, puede hacer lo siguiente:

- Asociar una política de permisos a un usuario o un grupo de su cuenta: para conceder a un usuario permisos para crear un recurso de AWS Organizations, como una política de control de servicio (SCP) o una unidad organizativa, puede asociar una política de permisos a un usuario o a un 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 la 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 un rol de IAM y asocia una política de permisos al rol, 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 la entidad `Principal`, la cual 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, consulte Administración de accesos en la Guía del usuario de IAM.

A continuación se ofrecen ejemplos de políticas 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":"*"
      }
   ]
```

```
}
```

También puede facilitar un ARN parcial en el elemento `Resource` de la política para indicar el tipo de recurso.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowCreatingAccountsOnResource",
         "Effect":"Allow",
         "Action":"organizations:CreateAccount",
         "Resource":"arn:aws:organizations::*:account/*"
      }
   ]
}
```

También puede denegar la creación de cuentas que no incluyan etiquetas específicas en la cuenta que se está creando.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyCreatingAccountsOnResourceBasedOnTag",
         "Effect":"Deny",
         "Action":"organizations:CreateAccount",
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/key":"value"
            }
         }
      }
   ]
}
```

Para obtener más información sobre los usuarios, los grupos, las funciones y los permisos, consulte las identidades de IAM (usuarios, grupos de usuarios y funciones) 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 Organizations actualmente no admite 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:

- Action - Puede utilizar 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, consulte Elementos de la política JSON de IAM: acciones en la Guía del usuario de IAM.
- Resource - Utilice esta palabra clave para especificar el ARN del recurso al que se aplica la instrucción de la política. Para obtener más información, consulte Elementos de la política JSON de IAM: recurso en la guía del usuario de IAM.
- Condition - Utilice esta palabra clave para especificar condiciones adicionales que se deben cumplir para que la instrucción de política sea aplicable. `Condition` suele especificar circunstancias adicionales que deben estar definidas como "true" para que la política coincida. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.

- Effect - Puede utilizar 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, consulte Elementos de la política JSON de IAM: efecto en la guía del usuario de IAM.
- Principal: en las políticas basadas en la 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 sobre la sintaxis y las descripciones de las políticas de IAM, consulte la referencia de la política JSON de IAM en la Guía del usuario de IAM.

Uso de políticas basadas en identidad (políticas de IAM) para AWS Organizations

Como administrador de la cuenta de administración de una organización, puede controlar el acceso a los recursos de AWS asociando políticas de permisos a identidades de AWS Identity and Access Management (IAM) (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: el nodo raíz de la organización, las unidades organizativas (OU), las cuentas y las políticas. Para obtener más información, consulte Control de acceso basado en atributos con etiquetas y AWS Organizations.

Conceder permisos completos de administrador a un usuario

Puede crear una política del IAM que conceda permisos de administrador de AWS Organizations completos a 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 el panel de navegación de la izquierda, seleccione Políticas.

   Si es la primera vez que elige Políticas, aparecerá la página Bienvenido a políticas administradas. Elija Comenzar.
3. En la parte superior de la página, seleccione Crear política.
4. En la sección Editor de políticas, seleccione la opción JSON.
5. Ingrese el siguiente documento de política JSON:

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

6. Elija Siguiente.

> **Note**
>
> Puede alternar entre las opciones Visual y JSON del editor en todo momento. No obstante, si realiza cambios o selecciona Siguiente en la opción Visual del editor, es posible que IAM reestructure la política, con el fin de optimizarla para el editor visual. Para obtener más información, consulte Reestructuración de política en la Guía del usuario de IAM.

7. En la página Revisar y crear, introduzca el Nombre de la política y la Descripción (opcional) para la política que está creando. Revise los Permisos definidos en esta política para ver los permisos que concede la política.
8. Elija Create Policy (Crear política) para guardar la nueva política.

Para obtener más información sobre la creación de una política de IAM, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Conceder acceso limitado por 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 el elemento `Action` de la política 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, consulte Acciones definidas por AWS Organizations en la Referencia de autorización de servicios.

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: Conceder permisos a una sola unidad organizativa

La primera instrucción de la siguiente política concede acceso de lectura a un usuario de IAM en toda la organización, pero la segunda instrucción permite al usuario realizar acciones administrativas de AWS Organizations solo en una unidad organizativa especificada (OU). Esto no se extiende a ninguna unidad organizativa secundaria. No se concede acceso a la facturación. Tenga en cuenta que esto no le da acceso administrativo a las Cuentas de AWS en la unidad organizativa. Concede únicamente permisos para realizar operaciones de AWS Organizations en las cuentas 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 grupo al que aplica esta política puede realizar cualquier acción (`"organizations:*"`) en cualquier entidad que esté directamente incluida en la unidad

organizativa especificada. La unidad organizativa se identifica por el Nombre de recurso de Amazon (ARN).

Para obtener más información sobre los ARN de varios recursos, consulte los tipos de recursos definidos AWS Organizations en la Referencia de autorización de servicios.

Concesión de 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: Concesión de 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 IAM Identity Center, 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 sobre los ARN de varios recursos, consulte los tipos de recursos definidos AWS Organizations en la Referencia de autorización de servicios.

Control de acceso basado en atributos con etiquetas y AWS Organizations

El Control de acceso basado en atributos le permite usar atributos administrados por el administrador, como etiquetas adjuntas tanto a recursos AWS como identidades AWS para controlar

el acceso a esos 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.

Los recursos etiquetables AWS Organizations incluyen Cuentas de AWS, el nodo raíz, las 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. Esto se hace agregando elementos `Condition` a sus instrucciones de permisos de política de AWS Identity and Access Management (IAM) 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 efectivamente dice "Permitir al usuario administrar solo aquellas OU que tienen una etiqueta con una clave `X` y un valor `Y`" o "Permitir al usuario gestionar solo aquellas OU que están etiquetadas con una clave `Z` que tiene el mismo valor que la clave de la etiqueta adjunta del usuario `Z`".

Puede basar sus pruebas `Condition` en diferentes tipos de referencias de etiquetas en una política de IAM.

- Comprobación de las etiquetas que se asocian a los recursos especificados en la solicitud
- Comprobación de las etiquetas que se asocian al usuario o rol de IAM que realiza la solicitud
- Compruebe las etiquetas que se incluyen como parámetros en la solicitud

Para obtener más información sobre el uso de etiquetas para el control de acceso en las políticas, consulte Controlar el acceso a y para los usuarios y roles de IAM utilizando etiquetas de recursos. Para obtener la sintaxis completa de las políticas de permisos de IAM, consulte la Referencia de políticas JSON de IAM

Comprobación de las etiquetas que se asocian a los recursos especificados en la solicitud

Cuando realiza una solicitud mediante el comando AWS Management Console, el AWS Command Line Interface (AWS CLI), o uno de las SDK de AWS, 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 políticas de permisos de IAM que se adjuntan a los usuarios y roles. En estas políticas, 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 verificar una etiqueta adjunta al recurso, haga referencia a la etiqueta en un elemento `Condition` al anteponer el nombre de la clave de la etiqueta con la siguiente cadena: `aws:ResourceTag/`

Por ejemplo, la siguiente política de ejemplo permite al usuario o rol realizar cualquier AWS Organizations operación a menos que ese recurso tenga una etiqueta con la clave `department` y el valor `security`. Si esa clave y valor están presentes, entonces la política deniega explícitamente la operación `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, consulte Control del acceso a los recursos y aws:ResourceTag en la Guía 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 que se asocian al usuario o rol de IAM. Para ello, utilice la clave de condición `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 valor `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, consulte Control del acceso a los recursos IAM y `aws:PrincipalTag` en la Guía 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 un elemento `Condition` 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. Solo comprueba si está presente una etiqueta con la clave especificada.

Para comprobar la clave de etiqueta, o una lista de claves, especifique un elemento `Condition` con la sintaxis siguiente:

```
"aws:TagKeys": [ "tag-key-1", "tag-key-2", ... , "tag-key-n" ]
```

Puede utilizar `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 si las tres 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"
                ]
            }
        }
    }
}
```

De manera alternativa, puede utilizar `ForAnyValue:` para prefaciar un operador de comparación para asegurarse de que al menos una de las claves de la solicitud deben coincidir con una de las claves especificadas en la política. Por ejemplo, la siguiente política permite cualquier operación de Organizations solo si al menos una de las claves de etiqueta especificadas está presente en la solicitud.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "organizations:*",
        "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 elemento `Condition` al 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 política de muestra 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 sobre el uso de estos elementos, consulte aws:TagKeys y aws:RequestTag en la Guía 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

- Registro de llamadas a la API de AWS Organizations con AWS CloudTrail
- Amazon EventBridge

Registro de 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 hechas por un usuario, un rol o un servicio de AWS en AWS Organizations. CloudTrail captura todas las llamadas a la API de AWS Organizations como eventos, incluidas las llamadas procedentes de la consola de AWS Organizations y las llamadas de código a las API de AWS Organizations. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos para AWS Organizations. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Historial de eventos. Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a AWS Organizations, la dirección IP desde la que se realizó, quién la realizó, cuándo y otros detalles.

Para obtener más información acerca de CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

> **Important**
>
> Puede ver toda la información de CloudTrail de AWS Organizations solo en la región de EE.UU. Este (Norte de Virginia). Si no ve su actividad AWS Organizations en la consola de CloudTrail, configure la consola para EE. UU. Este (Norte de Virginia) con el menú de la

esquina superior derecha. Si consulta CloudTrail con las herramientas AWS CLI o SDK, dirija la consulta al punto de enlace de EE. UU. Este (Norte de Virginia).

Información de AWS Organizations en CloudTrail

CloudTrail se habilita en su Cuenta de AWS cuando crea la cuenta. Cuando se produce una actividad en AWS Organizations, esa actividad se registra en un evento de CloudTrail junto con otros eventos de servicio de AWS en el Historial de eventos. Puede ver, buscar y descargar los últimos eventos de la Cuenta de AWS. Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de eventos en la Cuenta de AWS, incluidos los eventos de AWS 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 Cuenta de AWS, las llamadas a la API realizadas en acciones de AWS Organizations se escriben en los archivos de registro de CloudTrail junto con otros registros del servicio de AWS. También puede configurar otros servicios de AWS para analizar y actuar según los datos de eventos recopilados en los registros de CloudTrail. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- Servicios e integraciones compatibles con CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail

Todas las acciones de AWS Organizations las registra CloudTrail y se documentan en la Referencia de la API de AWS Organizations. Por ejemplo, las llamadas a `CreateAccount` (incluido el evento `CreateAccountResult`), `ListHandshakesForAccount`, `CreatePolicy` y `InviteAccountToOrganization` generan 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 del usuario raíz o del usuario de IAM
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol de IAM o un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte el Elemento userIdentity de CloudTrail.

Descripción de las entradas de los archivos de registro de AWS Organizations

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que especifique. Los archivos de registro de CloudTrail pueden contener una o varias entradas de registro. 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.

Entradas de registro de ejemplo: CloseAccount

En el ejemplo siguiente se muestra una entrada de registro de CloudTrail para una llamada de `CloseAccount` de muestra que se genera cuando se llama a la API y el flujo de trabajo para cerrar la cuenta comienza a procesar en segundo plano.

```
{
    "eventVersion": "1.08",
    "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": "2022-03-18T18:17:06Z"
            }
        }
    },
    "eventTime": "2022-03-18T18:17:06Z",
    "eventSource": "organizations.amazonaws.com",
    "eventName": "CloseAccount",
```

```
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.168.0.1",
    "userAgent":  "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)...",
    "requestParameters": {
        "accountId": "555555555555"
    },
    "responseElements": null,
    "requestID": "e28932f8-d5da-4d7a-8238-ef74f3d5c09a",
    "eventID": "19fe4c10-f57e-4cb7-a2bc-6b5c30233592",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

En el ejemplo siguiente, se muestra una entrada de registro de CloudTrail para una llamada `CloseAccountResult` después de que el flujo de trabajo en segundo plano para cerrar la cuenta se completa correctamente.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "accountId": "111122223333",
    "invokedBy": "organizations.amazonaws.com"
  },
  "eventTime": "2022-03-18T18:17:06Z",
  "eventSource": "organizations.amazonaws.com",
  "eventName": "CloseAccountResult",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "organizations.amazonaws.com",
  "userAgent": "organizations.amazonaws.com",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "EXAMPLE8-90ab-cdef-fedc-ba987EXAMPLE",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "closeAccountStatus": {
```

```
      "accountId": "555555555555",
      "state": "SUCCEEDED",
      "requestedTimestamp": "Mar 18, 2022 6:16:58 PM",
      "completedTimestamp": "Mar 18, 2022 6:16:58 PM"
    }
   },
   "eventCategory": "Management"
}
```

Entradas de registro de ejemplo: CreateAccount

En el ejemplo siguiente se muestra una entrada de log de CloudTrail para una llamada de muestra `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 log de CloudTrail para una llamada `CreateAccount` después de que el flujo de trabajo en segundo plano crea la cuenta que se completa 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"
    }
  }
}
```

El siguiente ejemplo muestra una entrada de registro de CloudTrail que se genera después de que un flujo de trabajo en segundo plano `CreateAccount` falle al 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 una llamada `CreateOrganizationalUnit` de ejemplo:

```
{
    "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 una llamada `InviteAccountToOrganization` de ejemplo:


```
{
    "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 una llamada `AttachPolicy` de ejemplo: 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 EventBridge

AWS Organizations puede operar con Amazon EventBridge, antes Eventos de Amazon CloudWatch, 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 EventBridge que buscan estas acciones y, cuando las detectan, envían los eventos generados a los objetivos definidos por el administrador. El objetivo puede 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 EventBridge para monitorear la actividad clave de su organización, consulte Tutorial: supervisión de cambios importantes en la organización mediante Amazon EventBridge.

Para obtener más información sobre EventBridge, incluido cómo configurarlo y habilitarlo, consulte la Guía del usuario de Amazon EventBridge.

Validación de conformidad en AWS Organizations

Para saber si un Servicio de AWS está incluido en el ámbito de programas de conformidad específicos, consulte Servicios de AWS en el ámbito del programa de conformidad y escoja el programa de conformidad que le interese. Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar los informes de auditoría de terceros utilizando AWS Artifact. Para más información, consulte Descarga de informes en AWS Artifact.

Su responsabilidad de conformidad al utilizar Servicios de AWS se determina en función de la sensibilidad de los datos, los destinos de cumplimiento de su empresa y la legislación y los reglamentos correspondientes. AWS proporciona los siguientes recursos para ayudar con la conformidad:

- Guías de inicio rápido de seguridad y conformidad: estas guías de implementación tratan consideraciones sobre arquitectura y ofrecen pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Arquitectura para la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones compatibles con HIPAA.

> **Note**
>
> No todos los Servicios de AWS son compatibles con HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- Recursos de conformidad de AWS: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- AWS Customer Compliance Guides: comprenda el modelo de responsabilidad compartida desde el punto de vista de la conformidad. En las guías se resumen las prácticas recomendadas para garantizar la seguridad de los Servicios de AWS y se orientan los controles de seguridad en varios marcos (incluidos el National Institute of Standards and Technology o NIST, el Payment Card Industry Security Standards Council o PCI y la International Organization for Standardization o ISO).
- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config: el servicio AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub: este Servicio de AWS proporciona una visión completa de su estado de seguridad en AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la referencia de controles de Security Hub.
- AWS Audit Manager: este Servicio de AWS le ayuda a auditar continuamente el uso de AWS con el fin de simplificar la forma en que administra el riesgo y la conformidad con las normativas y los estándares del sector.

Resiliencia en AWS Organizations

La infraestructura global de AWS se divide en Regiones de AWS y zonas de disponibilidad. Las Regiones de AWS 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 sobre las Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global de AWS.

Seguridad de la infraestructura en AWS Organizations

Como se trata de un servicio administrado, AWS Organizations está protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y cómo AWS protege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS con las prácticas recomendadas de seguridad de infraestructura, consulte Protección de la infraestructura en Portal de seguridad de AWS Well-Architected Framework.

Puede utilizar llamadas a la API publicadas en AWS para obtener acceso a Organizations a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Nosotros exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) tales como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

AWS OrganizationsReferencia de

Consulte los temas de esta sección para encontrar información de referencia detallada de distintos aspectos de AWS Organizations.

Temas

- Cuotas para AWS Organizations
- Políticas administradas de AWS disponibles para su uso con AWS Organizations

Cuotas para AWS Organizations

En esta sección se especifican las cuotas que afectan a AWS Organizations.

Directrices de nomenclatura

Las siguientes son pautas para los nombres que se crean AWS Organizations, incluidos los nombres de las cuentas, las unidades organizativas (OU), las raíces y las 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 la Referencia de la API AWS Organizations y busque la operación de API que crea el objeto. Mire los detalles del parámetro `Name` de esa operación. Por ejemplo :Nombre de cuenta, o bien Nombre de OU.

Valores mínimos y máximos

Los siguientes son los máximos predeterminados para las entidades en AWS Organizations.

> **Note**
>
> Puede solicitar aumentos de algunos de estos valores mediante la Consola Service Quotas. Organizations es un servicio global alojado físicamente en la región EE. UU. Este (Norte de Virginia) (`us-east-1`). Por lo tanto, debe `us-east-1` utilizarlas para acceder a las cuotas de Organizations cuando utilice la consola Service Quotas AWS CLI, el o un AWS SDK.

Número de Cuentas de AWS en una organización	El número máximo de cuentas permitidas en una organización de forma predeterminada es 10. Si necesita más cuentas, puede solicitar las contactándose con la consola de Service Quotas. 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. Las cuentas y organizaciones recién creadas pueden tener una cuota inferior a la predeterminada de 10 cuentas.
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	1000 por tipo de política
Tamaño máximo de un documento de política	Políticas de control de servicios: 5120 caracteres Políticas de exclusión de servicios de IA: 2500 caracteres Políticas de copia de seguridad: 10 000 caracteres Políticas de etiquetas: 10 000 caracteres Nota: Si guardas la política utilizando los AWS Management Console espacios en blanco adicionales (como espacios y saltos de línea) entre los elementos JSON y fuera de las comillas, se eliminan y no se cuentan. Si guardas la política mediante una operación del SDK o la AWS CLI, la política se guardará exactamente como la proporcionaste y no se eliminarán caracteres automáticamente.
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 puede realizar en un periodo de 24 horas	Ya sea 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 cuentas de miembro que se pueden cerrar en un plazo de 30 días	El 10% de las cuentas de los miembros de una organización, con un máximo de 1000. • Menos de 100 cuentas: puede cerrar hasta 10 cuentas de miembro • De 100 a 10 000 cuentas: puedes cerrar hasta un 10% de las cuentas de tus miembros • > 10 000 cuentas: puedes cerrar hasta 1000 cuentas de miembros Por ejemplo, si tiene 10 500 cuentas de miembros, puede cerrar hasta 1000 (no 1050) cuentas en un período de 30 días. Una vez alcanzado este límite, puede cerrar cuentas adicionales en la consola de AWS Billing o esperar hasta que se restablezca la cuota. Para obtener más información, consulta lo que debes saber antes de cerrar tu cuenta en la Guía de administración de AWS cuentas.
Número de cuentas de miembro que se pueden cerrar de forma simultánea	3: solo se pueden realizar tres cierres de cuentas al mismo tiempo. Tan pronto como termine uno, puede cerrar otra cuenta.

Número de entidades a las que puede asociar una política	Sin límite
Número de etiquetas que puede asociar a un nodo raíz, OU o cuenta	50
Tamaño máximo de la política de delegación basada en recursos	40 000 caracteres

Tiempo de vencimiento de protocolos de enlace (handshakes)

Los siguientes son los tiempos de espera para dar un apretón de manos. 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

El mínimo y máximo depende 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 solo se aplican a las políticas que están directamente adjuntas a una unidad organizativa o a una cuenta. Las políticas que afectan a una unidad organizativa o a una cuenta por herencia no cuentan contra estos límites.

Tipo de política	Mínimo que se puede asociar a una entidad	Máximo adjunto al nodo raíz	Máximo adjunto por OU	Máximo adjunto por cuenta
Política de control de servicios	1 - Cada entidad debe tener al menos una SCP asociada 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 de copia de seguridad	0	10	10	10
Política de etiquetas	0	10	10	10

> **Note**
>
> Actualmente, solo puede tener un nodo raíz en una organización.

Límites de limitación

En la siguiente tabla, se enumeran las AWS Organizations API por categoría de administración y se muestran sus tasas de aceleración respectivas a nivel de cuenta y organización.

AWS Organizations API	Límite por cuenta (tasa, ráfaga)	Límite por organización (velocidad, ráfaga)
Administración de cuentas		
CloseAccount	0,5, 1	
CreateAccount, CreateGovCloudAccount	0,1, 3	
DescribeAccount	20, 30	24, 36
DescribeCreateAccountStatus	2, 2	2, 3
LeaveOrganization	1, 1	
ListCreateAccountStatus	5, 8	6, 10
Gestión del apretón de manos		
AcceptHandshake, DescribeHandshake	1, 1	
CancelHandshake	2, 3	
DeclineHandshake	1, 3	
InviteAccountToOrganization	3, 5	
ListHandshakesForAccount, ListHandshakesForOrganization	5, 8	6, 10
Gestión de la organización		

AWS Organizations API	Límite por cuenta (tasa, ráfaga)	Límite por organización (velocidad, ráfaga)
CreateOrganization, DeleteOrganization, EnableFullControl	1, 1	
CreateOrganizationalUnit, DescribeOrganization	1, 2	
MoveAccount, UpdateOrganizationalUnit, DeleteOrganizationalUnit	2, 3	
DescribeOrganizationalUnit	2, 2	2, 3
ListAccounts	8, 12	9, 15
ListChildren	6, 10	7, 12
ListParents, ListAccountsForParent, ListOrganizationalUnitsForParent	5, 8	6, 10
ListRoots	1, 2	1, 3
ListTagsForResource	10, 15	12, 18
RemoveAccountFromOrganization	2, 2	
TagResource, UntagResource	4, 6	
Gestión de políticas		
CreatePolicy, DeletePolicy, AttachPolicy, DetachPolicy	2, 3	
DescribePolicy	2, 2	2, 3

AWS Organizations API	Límite por cuenta (tasa, ráfaga)	Límite por organización (velocidad, ráfaga)
DisablePolicyType, EnablePolicyType	1, 1	
ListPolicies, ListPoliciesForTarget, ListTargetsForPolicy	5, 8	6, 10
UpdatePolicy	2, 3	
Administración de servicios		
HabilitarAWSServiceAccess, deshabilitar AWSServiceAccess	1, 2	
ListaAWSServiceAccessForOrganization, ListDelegatedServicesForAccount	1, 3	1, 4
ListDelegatedAdministrators	5, 8	6, 10
RegisterDelegatedAdministrator, DeregisterDelegatedAdministrator	1, 2	

Políticas administradas de AWS disponibles para su uso con AWS Organizations

En esta sección se identifican las políticas administradas por AWS que puede usar para las tareas de organización. No puede modificar ni eliminar una política administrada por AWS, pero puede asociarla o separarla de entidades de la organización según sea necesario.

Políticas AWS Organizations administradas para su uso conAWS Identity and Access Management (IAM)

Una política administrada de IAM la proporciona y mantiene AWS. Una política administrada proporciona permisos para tareas comunes que puede asignar a los usuarios adjuntando la política administrada al usuario o objeto de rol de IAM apropiado. No tiene que escribir la política usted mismo, y cuando AWS actualiza la política según corresponda para admitir nuevos servicios, obtendrá automáticamente e inmediatamente el beneficio de la actualización. Puede ver la lista de políticas administradas de AWS en la página Políticas en la consola de IAM. Use el menú de Filtrar políticas para seleccionar AWSadministrado.

Puede usar las siguientes políticas administradas para conceder permisos a usuarios y roles en su organización.

Nombre de la política	Descripción	ARN

AWSOrganizationsFullAccess	Proporciona todos los permisos necesarios para crear y administrar completamente una organización. El contenido de esta declaración de la política se muestra en el siguiente fragmento: <pre>{
	    "Version": "2012-10-17",
	    "Statement": [
	        {
	            "Sid": "AWSOrganizationsFullAccess",
	            "Effect": "Allow",
	            "Action": "organizations:*",
	            "Resource": "*"
	        },
	        {
	            "Sid": "AWSOrganizationsFullAccessAccount",
	            "Effect": "Allow",</pre>
		arn:aws:iam: :aws:policy/AWSOrganizationsFullAccess

Nombre de la política	Descripción	ARN

```
            "Action": [
                "account:
PutAlternateContact",
                "account:
DeleteAlternateContact",
                "account:
GetAlternateContact",
                "account:
GetContactInformation",
                "account:
PutContactInformation",
                "account:
ListRegions",
                "account:
EnableRegion",
                "account:
DisableRegion"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AWSOrgan
izationsFullAccessCreateSLR
",
            "Effect": "Allow",
            "Action":
 "iam:CreateServiceLinkedRol
e",
            "Resource": "*",
            "Condition": {
                "StringEq
uals": {
                    "iam:AWSS
erviceName": "organiza
tions.amazonaws.com"
                }
            }
        }
    ]
}
```

Nombre de la política	Descripción	ARN
AWSOrganizationsReadOnlyAccess	Proporciona acceso de solo lectura a la información acerca de la organización. No permite al usuario realizar ningún cambio. El contenido de esta declaración de la política se muestra en el siguiente fragmento: `{ "Version":"2012-10-17", "Statement":[{ "Sid": "AWSOrganizationsReadOnly", "Effect":"Allow", "Action":["organizations:Describe*", "organizations:List*"], "Resource": "*" }, { "Sid": "AWSOrganizationsReadOnlyAccount", "Effect":"Allow", "Action":["account:GetAlternateContact", "account:GetContactInformation", "account:ListRegions"], "Resource": "*" }] }`	arn:aws:iam: :aws:policy/AWSOrganizationsReadOnlyAccess

Actualizaciones para Organizations AWS Políticas administradas

La siguiente tabla muestra las actualizaciones de las políticas administradas de AWS debido a 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 la página de historial de documentos AWS Organizations.

Cambio	Descripción	Fecha
AWSOrganizationsFullAccess— actualizado para incluir elementos que describen la declaración de política. `Sid`	Las organizaciones agregaron `Sid` elementos para la política `AWSOrganizationsFullAccess` gestionada.	6 de febrero de 2024
AWSOrganizationsReadOnlyAccess— actualizado para incluir `Sid` elementos que describen la declaración de política.	Las organizaciones agregaron `Sid` elementos para la política `AWSOrganizationsReadOnlyAccess` gestionada.	6 de febrero de 2024
AWSOrganizationsFullAccess— se actualizó para permitir los permisos de API de la cuenta necesarios para habilitarlos o deshabilitarlos Regiones de AWS a través de la consola de Organizations.	Organizations ha añadido las acciones `account:ListRegions` , `account:EnableRegion` y `account:DisableRegion` a la política para permitir el acceso de escritura para habilitar o desactivar Regiones para una cuenta.	22 de diciembre de 2022
AWSOrganizationsReadOnlyAccess— se actualizó para permitir los permisos de API de las cuentas necesarios para publicar anuncios Regiones de AWS a través de la consola de Organizations.	Organizations ha añadido la acción `account:ListRegions` a la política para permitir el acceso a la visualización de Regiones para una cuenta.	22 de diciembre de 2022
AWSOrganizationsFullAccess— actualizado para permitir los permisos de la API de la cuenta necesarios para añadir o editar los	Se han agregado las acciones `account:GetContactInformation` y `account:PutContactInformation` a	21 de octubre de 2022

Cambio	Descripción	Fecha
contactos de la cuenta a través de la consola de Organizations.	la política para permitir el acceso de escritura para modificar los contactos de una cuenta en Organizations.	
AWSOrganizationsReadOnlyAccess— actualizado para permitir los permisos de API de la cuenta necesarios para ver los contactos de la cuenta a través de la consola de Organizations.	Se ha agregado la acción `account:GetContactInformation` a la política para permitir el acceso para ver los contactos de una cuenta en Organizations.	21 de octubre de 2022
AWSOrganizationsFullAccess— actualizado para permitir la creación de una organización.	Organizations agregó el permiso `CreateServiceLinkedRole` a la política para habilitar la creación del rol vinculado al servicio necesario para crear una organización. El permiso está restringido a la creación de un rol que solo puede ser utilizado por el servicio `organizations.amazonaws.com`	24 de agosto de 2022
AWSOrganizationsFullAccess— actualizado para permitir los permisos de la API de la cuenta necesarios para añadir, editar o eliminar contactos alternativos de la cuenta a través de la consola de Organizations.	Las Organizations han agregado el `account:GetAlternateContact` , `account:DeleteAlternateContact` , `account:PutAlternateContact` de acciones de la política para habilitar el acceso de escritura para modificar contactos alternativos de una cuenta.	7 de febrero de 2022

Cambio	Descripción	Fecha
AWSOrganizationsReadOnlyAccess— actualizado para permitir los permisos de API de la cuenta necesarios para ver los contactos alternativos de la cuenta a través de la consola de Organizations.	Las Organizations han agregado el `account:GetAlternateContact` de acción de la política para permitir el acceso para ver contactos alternativos de una cuenta.	7 de febrero de 2022

Políticas de control de servicios administradas por AWS Organizations

Las políticas de control de servicios (SCP) son similares a las políticas de permisos de IAM, pero son una característica de AWS Organizations, no 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 página Políticas de la consola de 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
Completo AWSAccess	Da acceso a la cuenta de administración de AWS Organizations 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
- Solución de problemas de políticas de AWS Organizations

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
- Aparece un mensaje de "acceso denegado" al realizar una solicitud con credenciales de seguridad temporales
- Obtengo un mensaje de "acceso denegado" cuando intento dejar una organización como cuenta miembro o eliminar una cuenta miembro como cuenta de administración.
- Obtengo un mensaje de "cuota superada" cuando intento agregar una cuenta a mi organización
- Aparece un mensaje que indica que "esta operación requiere un periodo de espera" al añadir o eliminar cuentas
- Obtengo un mensaje de "organización todavía inicializando" cuando intento añadir una cuenta a mi organización
- Aparece el mensaje "Invitations are disabled" cuando intento invitar a una cuenta a mi organización.
- Los cambios que realizo no están siempre visibles inmediatamente

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, grupo o rol. 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 de un usuario, grupo o rol consulte Trabajo con políticas en la Guía 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 la función de que está utilizando para realizar la solicitud tiene los permisos adecuados. Los permisos de credenciales de seguridad temporales se obtienen de un usuario o una función de y, por tanto, se limitan a los concedidos al usuario o la función de . Para obtener más información sobre cómo se determinan los permisos de las credenciales de seguridad temporales, consulte Controlar los permisos para credenciales de seguridad temporarias en la Guía 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 la documentación del conjunto de herramientas del SDK seleccionado o Uso de credenciales de seguridad temporales para solicitar acceso a los recursos de AWS en la Guía del usuario de IAM.
- Compruebe que sus credenciales de seguridad temporales no hayan caducado. Para obtener más información, consulte Solicitud de credenciales de seguridad temporales en la Guía 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 Acceder facturación en la cuenta miembro. Para obtener más información, consulte Activación del acceso a la consola de Billing and Cost Management en la Guía del usuario de AWS Billing.
- 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 desde su cuenta de miembro.

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 una Cuenta de AWS, elimínela de su organización para que no se siga contabilizando para la cuota.
- Para obtener más información sobre cómo solicitar un aumento de cuotas, consulte Valores mínimos y máximos.

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 tiene problemas con las cuotas de la cuenta al agregar o eliminar cuentas, consulte Valores mínimos y máximos para obtener información sobre cómo solicitar un aumento de cuota.

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. 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 datos en la Guía para desarrolladores de bases de datos Amazon Redshift
- Modelo de consistencia de datos de Amazon S3 en la Guía del usuario de Amazon Simple Storage Service
- Ensuring Consistency When Using Amazon S3 and Amazon Elastic MapReduce for ETL Workflows en el blog sobre macrodatos de AWS
- Consistencia final de EC2 en la Referencia de la 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

Las políticas de control de servicios (SCP) de AWS Organizations son 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. La gramática de las políticas de IAM se basa en la definición de nombres y valores que tengan significado y puedan ser entendidos por los servicios de AWS que usan políticas para conceder permisos.

AWS Organizations utiliza un subconjunto de la sintaxis y la gramática de IAM. Para obtener más información, consulte Sintaxis de SCP.

Errores de políticas comunes

- Más de un objeto de política
- Más de un elemento Statement
- El documento de política supera el tamaño máximo

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 5120 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 la Referencia de API AWS Organizations.

> **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 la Referencia de API AWS Organizations.

Temas

- puntos de conexión
- HTTPS obligatorio
- Firma de solicitudes API de AWS Organizations

puntos de conexión

AWS Organizations tiene un único punto de enlace de API global alojado en la región EE. UU. Este (Norte de Virginia).

Para obtener más información sobre AWS los puntos finales y las regiones de todos los servicios, consulte Puntos finales regionales en. Referencia general de AWS

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. Se recomienda encarecidamente no utilizar las credenciales de Usuario raíz de la cuenta de AWS para el trabajo diario con AWS Organizations. Puede utilizar las credenciales de un usuario o rol.

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

AWS Organizations no es compatible con versiones anteriores, como Signature Version 2.

Para obtener más información, consulte los siguientes temas:

- Credenciales de seguridad de AWS: ofrece información general acerca de los tipos de credenciales que puede utilizar para acceder a AWS.
- Prácticas de seguridad recomendadas en IAM: ofrece sugerencias acerca de cómo utilizar el servicio de IAM para ayudar a proteger sus recursos de AWS, incluidos los de AWS Organizations.
- Credenciales temporales de seguridad en IAM: describe cómo crear y utilizar las credenciales temporales de seguridad.

Historial de documentos de AWS Organizations

En la tabla siguiente se describen las actualizaciones principales de la documentación de AWS Organizations.

- Versión de API: 2016-11-28

Cambio	Descripción	Fecha
Declaraciones de política actualizadas	Se agregaron nuevos `Sid` elementos a las declaraciones de políticas AWS Organizations gestionadas.	6 de febrero de 2024
Nuevo tema de cierre de cuentas de gestión	Se agregaron enlaces a consideraciones y pasos detallados que explican cómo cerrar una cuenta de administración.	1 de febrero de 2024
Prácticas recomendadas actualizadas	Se agregó nueva información a la sección de prácticas recomendadas para ayudar a alinearse con las prácticas recomendadas de IAM.	12 de junio de 2023
Se actualizaron AWSOrganizationsFullAccess y AWSOrganizationsReadOnlyAccess gestionaron las políticas	Ambas políticas administradas se actualizaron para permitir el acceso de escritura o lectura a los contactos de las cuentas.	21 de octubre de 2022
Se actualizó la política AWSOrganizationsFullAccess gestionada	La política administrada se actualizó para permitir la creación de una organización agregando el permiso necesario para crear el rol	24 de agosto de 2022

	vinculado al servicio que necesita una organización nueva.	
Capacidad de cierre de la cuenta de Organizations desde la consola de AWS Organizations	Las entidades principales de la cuenta de administración pueden cerrar cuentas de miembro desde la consola de AWS Organizations y proteger las cuentas de los miembros del cierre accidental mediante el uso de las políticas de IAM.	29 de marzo de 2022
Anuncio actualizado para actualizar contactos alternativos con la consola de AWS Organizations	Organizations ahora proporciona la capacidad de actualizar los contactos alternativos para las cuentas dentro de su organización utilizando la consola AWS Organizations. Anuncie la nueva capacidad y señale a la referencia de administración de cuentas para obtener instrucciones.	8 de febrero de 2022
Actualizaciones de políticas administradas por Organizations: Actualización de una política existente	Se actualizaron las políticas AWSOrganizationsReadOnlyAccess administradas AWSOrganizationsFullAccess y las políticas para permitir los permisos de API de la cuenta necesarios para actualizar o ver los contactos alternativos de la cuenta a través de la AWS Organizations consola.	7 de febrero de 2022

Integración de las organizaciones con Amazon DevOps Guru	Puede integrar Amazon DevOps Guru AWS Organizations para supervisar el estado de las aplicaciones de forma integral en todas las cuentas de su organización y obtener información valiosa.	3 de enero de 2022
Integración de Organizations con Amazon Detective	Puede integrar Amazon Detective con AWS Organizations para garantizar que el gráfico de comportamiento de Detective proporcione visibilidad de la actividad de todas las cuentas de la organización.	16 de diciembre de 2021
La integración de Organizations con AWS Config ahora 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, consulte Acumulación de datos de varias cuentas y regiones en la Guía del desarrollador de AWS Config.	16 de junio de 2021

La integración de Organizations con AWS Firewall Manager ahora incluye la compatibilidad con 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 copia de seguridad de Organizations ahora admiten la copia de seguridad continua	Puede utilizar la característica de copias de seguridad AWS Backup continuas con las políticas de copia de seguridad de su organización.	10 de marzo de 2021
La integración de Organizations con AWS CloudFormation StackSets ahora incluye la compatibilidad con un administrador delegado	Ahora puede designar una cuenta de miembro de su organización para que sea la AWS CloudFormation StackSets administradora de 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 cuentas mientras habilita todas las características	AWS actualizó 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

Se presenta la versión 2.0 de la consola de AWS Organizations	AWS introdujo una nueva versión de la consola AWS. Toda la documentación se ha actualizado para reflejar la nueva forma de realizar las tareas.	21 de enero de 2021
Organizations ahora admite la integración con AWS Marketplace	A partir de ahora, puede habilitar AWS Marketplace para compartir con más facilidad las licencias de software en todas las cuentas de su organización.	3 de diciembre de 2020
Organizations ahora admite la integración con Amazon S3 Lens	Amazon S3 Lens admite el acceso de confianza y el administrador delegado con Organizations. Para obtener información detallada, consulte Amazon S3 Storage Lens en la Guía del usuario de Amazon Simple Storage Service.	18 de noviembre de 2020
Copias de seguridad entre cuentas	Cuando utiliza políticas 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

Las Regiones de AWS en China ahora admiten AWS Resource Access Manager como un servicio de confianza de Organizations	A partir de ahora, puede utilizar las características AWS RAM que se integran con Organizations como un servicio de confianza cuando utiliza Organizations y AWS RAM en China.	18 de noviembre de 2020
Organizations ahora admite 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	AWS Organizations cambió el nombre de la “cuenta maestra” a “cuenta de administración”. Solo se ha cambiado el nombre, 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 de AWS Organizations. La nueva sección incluye temas que tratan las prácticas recomenda das para los usuarios raíz de cuentas de administración y cuentas de miembro y administración de contraseñ as.	6 de octubre de 2020

Se ha agregado nueva sección de prácticas recomendadas y dos primeras páginas	Hay una nueva sección para temas que describen las prácticas recomendadas para AWS Organizations. Esta actualización incluye un tema sobre prácticas recomendadas para la cuenta de administr ación de una organización y un tema sobre prácticas recomendadas para cuentas de miembro.	2 de octubre de 2020
Las políticas de copia de seguridad de Organizations ahora admiten copias de seguridad coherentes con las aplicaciones en instancias de Windows EC2 mediante VSS (Volume Shadow Copy Service)	Las políticas de copia de seguridad admiten una nueva sección `advanced_backup_settings` “. La primera entrada de esta nueva sección es una configuración `ec2` llamada `WindowsVSS` que puede habilitar o desactivar. Para obtener más información, consulte Creación de una copia de seguridad de Windows habilitada para VSS en la Guía para desarroll adores de AWS Backup.	24 de septiembre de 2020

Organizations apoya tag-on-create y controla el acceso por etiquetas	Puede agregar etiquetas a los recursos de Organizations cuando los crea. Puede usar Políticas de etiquetas para estandarizar el uso de etiquetas en los recursos de Organizations. Puede usar Políticas de IAM para restringir el acceso solo a los recursos que tienen claves de etiqueta y valores especificados.	15 de septiembre de 2020
Se agregó AWS Health como un servicio de confianza	Puede agregar eventos AWS Health en todas las cuentas de su organización.	4 de agosto de 2020
Políticas de exclusión de servicios de inteligencia artificial (IA)	Puede usar las políticas de exclusión de servicios de IA para controlar si los servicios de IA AWS pueden almacenar y utilizar el contenido del cliente procesado por dichos servicios (contenido de IA) para el desarrollo y la mejora continua de Servicios y tecnologías de IA AWS.	8 de julio de 2020
Se agregaron políticas de copia de seguridad e integración con AWS Backup	Puede usar las 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

Compatibilidad con la administración delegada del Analizador de acceso de IAM	Permite delegar el acceso administrativo de Access Analyzer de su organización en una cuenta miembro designada.	30 de marzo de 2020
Integración con el 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 en todas las Cuentas de AWS en su organización en el explorador de Systems Manager.	26 de noviembre de 2019
leyes: PrincipalOrgPaths	La nueva clave de condición global comprueba la ruta de AWS Organizations para el usuario de IAM, el rol de IAM y el usuario raíz de la cuenta de Cuenta de AWS que realiza la solicitud.	20 de noviembre de 2019

Integración con reglas de AWS Config	Puede utilizar las operaciones de API de AWS Config para administrar las reglas de AWS Config en todas las cuentas de Cuentas de AWS de su 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 con el 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 Service Catalog se han agregado 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
CreateAccount notificaciones	`CreateAccount` las notificaciones se publican en los CloudTrail registros 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 para que los servicios de AWS seleccionados funcionen en las cuentas de la organizac ión. IAM Identity Center 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 compatibi lidad con el nuevo servicio AWS IAM Identity Center	AWS Organizations ahora es compatible con la integración con AWS IAM Identity Center (IAM Identity Center).	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	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

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.