Guía del usuario de

AWS Resource Access Manager

AWS Resource Access Manager: Guía del usuario de

Table of Contents

¿Qué es AWS Resource Access Manager?

AWS Resource Access Manager (AWS RAM) le ayuda a compartir de forma segura sus recursos entre Cuentas de AWS su organización o unidades organizativas (OUs) y con los roles y usuarios AWS Identity and Access Management (de IAM) en el caso de los tipos de recursos compatibles. Si tienes varios Cuentas de AWS, puedes crear un recurso una vez y usarlos AWS RAM para que esas otras cuentas puedan utilizarlo. Si tu cuenta está gestionada por AWS Organizations, puedes compartir los recursos con todas las demás cuentas de la organización o solo con las cuentas que pertenezcan a una o más unidades organizativas específicas (OUs). También puedes compartirlos con un identificador Cuentas de AWS de cuenta específico, independientemente de si la cuenta forma parte de una organización. Ciertos tipos de recursos admitidos también le permiten compartir con roles y usuarios de IAM específicos.

Contenido

Descripción general de los vídeos

En el siguiente vídeo se proporciona una breve introducción AWS RAM y se describe cómo crear un recurso compartido. Para obtener más información, consulte ???.

En el siguiente vídeo se muestra cómo aplicar los permisos AWS gestionados a AWS los recursos. Para obtener más información, consulte ???.

En este vídeo se ofrece una demostración de cómo crear y asociar permisos administrados por el cliente siguiendo las prácticas recomendadas de privilegio mínimo. Para obtener más información, consulte, ???.

Ventajas de AWS RAM

¿Por qué usarlo AWS RAM? Ofrece las siguientes ventajas:

- Reduce los gastos operativos: crea un recurso una vez y úsalo AWS RAM para compartirlo con otras cuentas. De esta forma, se elimina la necesidad de aprovisionar recursos duplicados en cada cuenta, lo que reduce la sobrecarga operativa. Dentro de la cuenta propietaria del recurso, se AWS RAM simplifica la concesión de acceso a todos los roles y usuarios de esa cuenta sin tener que usar políticas de permisos basadas en la identidad.
- Proporciona seguridad y coherencia: simplifique la administración de la seguridad de sus recursos compartidos utilizando un único conjunto de políticas y permisos. Si, en lugar de eso, creara recursos duplicados en todas sus cuentas independientes, tendría que implementar políticas y permisos idénticos y, después, tendría que mantenerlos de forma idéntica en todas esas cuentas. En su lugar, todos los usuarios de un AWS RAM recurso compartido se administran mediante un único conjunto de políticas y permisos. AWS RAM ofrece una experiencia coherente para compartir diferentes tipos de AWS recursos.
- Proporciona visibilidad y capacidad de auditoría: consulte los detalles de uso de sus recursos compartidos mediante la integración AWS RAM de Amazon CloudWatch y AWS CloudTrail. AWS RAM proporciona una visibilidad completa de los recursos y cuentas compartidos.

¿Qué hay del acceso entre cuentas con políticas basadas en recursos?

Puede compartir algunos tipos de AWS recursos con otros Cuentas de AWS si adjunta una política basada en recursos que identifique a los principales (IAM) AWS Identity and Access Management (funciones y usuarios de IAM) ajenos a los suyos. Cuenta de AWS Sin embargo, compartir un recurso adjuntando una política no aprovecha las ventajas adicionales que ofrece. AWS RAM Al usarlo AWS RAM , obtienes las siguientes funciones:

- Puede compartir con una organización o una unidad organizativa (OU) sin tener que enumerar cada una de Cuenta de AWS IDs ellas.
- Los usuarios pueden ver los recursos que se comparten con ellos directamente en la consola de Servicio de AWS que los origina y en las operaciones de la API, como si tales recursos estuvieran directamente en la cuenta del usuario. Por ejemplo, si suele AWS RAM compartir una subred de Amazon VPC con otra cuenta, los usuarios de esa cuenta pueden ver la subred en la consola de

Amazon VPC y en los resultados de las operaciones de la API de Amazon VPC realizadas en esa cuenta. Los recursos compartidos adjuntando una política basada en recursos no están visibles de este modo; en su lugar, debe detectar el recurso y hacer referencia a él explícitamente por su nombre de recurso de Amazon (ARN).

- Los propietarios de un recurso pueden ver qué entidades principales tienen acceso a cada recurso individual que han compartido.
- Si comparte recursos con una cuenta que no forma parte de su organización, inicia AWS RAM un proceso de invitación. El destinatario debe aceptar la invitación para que la entidad principal pueda acceder a los recursos compartidos. Una vez que activa la capacidad para compartir dentro de la organización, compartir con las cuentas de la organización no requiere invitación.

Si tienes recursos que has compartido mediante una política de permisos basada en recursos, puedes convertirlos en recursos totalmente AWS RAM gestionados de la siguiente manera:

- Use la operación PromoteResourceShareCreatedFromPolicy de la API.
- Usa el equivalente de la operación de la API, que es el comando AWS Command Line Interface (AWS CLI). promote-resource-share-created-from-policy

Cómo funciona el uso compartido de recursos

Cuando compartes un recurso de la cuenta propietaria con otra Cuenta de AWS, la cuenta consumidora, estás concediendo acceso al recurso compartido a los principales de la cuenta consumidora. Todas las políticas y permisos que se aplican a roles y usuarios de la cuenta consumidora se aplican también al recurso compartido. Los recursos del recurso compartido parecen recursos nativos en el lugar con el Cuentas de AWS que los has compartido.

Puede compartir tanto recursos globales como regionales. Para obtener más información, consulte Compartir recursos regionales frente a recursos globales.

Compartir recursos de su propiedad

Con AWS RAM, compartes los recursos que te pertenecen mediante la creación de un recurso compartido. Para crear un recurso compartido, especifique lo siguiente:

- El Región de AWS lugar en el que desea crear el recurso compartido. En la consola, selecciónela en el menú desplegable Región que aparece en la esquina superior derecha de la consola. En el AWS CLI, se utiliza el `--region` parámetro.

  - Un recurso compartido solo puede contener recursos regionales que pertenezcan a la misma Región de AWS que el recurso compartido.
  - Un recurso compartido puede contener recursos globales solo si se encuentra en la región de origen designada para los recursos globales, Este de EE. UU. (Norte de Virginia), `us-east-1`.
- Asigne un nombre al recurso compartido.
- La lista de recursos a los que desea conceder acceso como parte de este recurso compartido.
- Las entidades principales a las que concede acceso al recurso compartido. Los directores pueden ser individuales Cuentas de AWS, las cuentas de una organización o una unidad organizativa (OU) AWS Organizations, o funciones o usuarios individuales AWS Identity and Access Management (IAM).

  > **Note**
  >
  > No todos los tipos de recursos se pueden compartir con roles y los usuarios de IAM. Para obtener información sobre los recursos que puede compartir con estas entidades principales, consulte Recursos que se pueden compartir AWS.

- Un permiso administrado que asociar a cada tipo de recurso incluido en el recurso compartido. El permiso administrado determina lo que las entidades principales de las demás cuentas pueden hacer en relación con los recursos del recurso compartido.

  El comportamiento del permiso depende del tipo de entidad principal:

  - Si la entidad principal está en una cuenta diferente de la cuenta propietaria del recurso, los permisos adjuntos al recurso compartido serán los permisos máximos disponibles para conceder a roles y usuarios de esas cuentas. El administrador de dichas cuentas debe entonces conceder acceso a roles y usuarios individuales al recurso compartido mediante políticas de permisos basadas en la identidad de IAM. Los permisos concedidos en esas políticas no pueden superar los definidos en los permisos adjuntos al recurso compartido.

La cuenta propietaria de los recursos conserva la propiedad total de los recursos que comparte.

Usar recursos compartidos

Cuando el propietario de un recurso lo comparte con su cuenta, puede obtener acceso al recurso compartido del mismo modo que lo haría si este fuera propiedad de su cuenta. Puede acceder al recurso mediante la consola, los AWS CLI comandos y las operaciones de API del servicio

correspondiente. Las operaciones de API que las entidades principales de su cuenta pueden realizar varían en función del tipo de recurso y se especifican en el permiso AWS RAM adjunto al recurso compartido. También se siguen aplicando todas las políticas de IAM y políticas de control del servicios configuradas en su cuenta, lo que le permite aprovechar las inversiones existentes en controles de seguridad y gobernanza.

Cuando accedes a un recurso compartido mediante el servicio de ese recurso, tienes las mismas capacidades y limitaciones Cuenta de AWS que el propietario del recurso.

- Si el recurso es regional, solo podrá acceder a él desde la Región de AWS en la que existe la cuenta propietaria.
- Si el recurso es global, puede acceder a él desde cualquier Región de AWS compatible con la consola de servicio y las herramientas del recurso. Puede ver y administrar el recurso compartido y sus recursos globales en la AWS RAM consola y las herramientas solo en la región de origen designada, EE. UU. Este (Virginia del Norte)`us-east-1`.

Accediendo AWS RAM

Puede trabajar con él AWS RAM de cualquiera de las siguientes maneras:

AWS RAM consola

AWS RAM proporciona una interfaz de usuario basada en la web, la AWS RAM consola. Si te has registrado en una Cuenta de AWS, puedes acceder a la AWS RAM consola iniciando sesión en la página de inicio AWS RAM de la consola Consola de administración de AWSy eligiendo una opción.

También puede usar un navegador para ir directamente a la consola de AWS RAM. Si todavía no se ha registrado, se le pedirá que lo haga antes de que aparezca la consola.

AWS CLI y Herramientas para Windows PowerShell

AWS CLI Y Herramientas de AWS para PowerShell proporcionan acceso directo a las operaciones de la API AWS RAM pública. AWS admite estas herramientas en WindowsmacOS, yLinux. Para obtener más información acerca de cómo empezar, consulte la Guía del usuario de la AWS Command Line Interface o la Guía del usuario de AWS Tools for Windows PowerShell. Para obtener más información sobre los comandos de AWS RAM, consulte la Referencia de AWS CLI comandos o la Referencia de AWS Tools for Windows PowerShell cmdlets.

AWS SDKs

AWS proporciona comandos de API para un amplio conjunto de lenguajes de programación. Para obtener más información sobre cómo empezar, consulta la Guía de referencia de herramientas AWS SDKs y herramientas.

API de consulta

Si no utilizas uno de los lenguajes de programación compatibles, la API de consulta AWS RAM HTTPS te proporciona acceso programático a AWS RAM y AWS. Con la AWS RAM API, puedes enviar solicitudes HTTPS directamente al servicio. Cuando utilices la AWS RAM API, debes incluir un código para firmar digitalmente las solicitudes con tus credenciales. Para obtener más información, consulte la Referencia de la API de AWS RAM.

Precios para AWS RAM

No se cobran cargos adicionales por el uso AWS RAM o la creación de recursos compartidos ni por compartir tus recursos entre cuentas. Los cargos por el uso de recursos varían en función del tipo de recurso. Para obtener más información sobre cómo se AWS facturan los recursos compartibles, consulte la documentación del servicio de propiedad del recurso.

Conformidad y estándares internacionales

PCI DSS

AWS RAM admite el procesamiento, el almacenamiento y la transmisión de los datos de las tarjetas de crédito por parte de un comerciante o proveedor de servicios, y se ha comprobado que cumple con el estándar de seguridad de datos (DSS) de la industria de tarjetas de pago (PCI).

Para obtener más información acerca de PCI DSS, incluido cómo solicitar una copia del Paquete de conformidad con PCI de AWS , consulte PCI DSS Nivel 1.

FedRAMP

AWS RAM está autorizado como FedRAMP Moderado en las Regiones de AWS siguientes áreas: EE.UU. Este (Norte de Virginia), EE.UU. Este (Ohio), EE.UU. Oeste (Norte de California) y EE.UU. Oeste (Oregón).

AWS RAM está autorizado como FedRAMP High en los Regiones de AWS siguientes lugares AWS GovCloud : (EE. UU. Oeste) y (EE. UU. Este). AWS GovCloud

El Programa Federal de Administración de Riesgos y Autorizaciones (FedRAMP) es un amplio programa gubernamental de EE. UU. que ofrece un enfoque estandarizado para la supervisión continua, la autorización y la evaluación de la seguridad de servicios y productos en la nube.

Para obtener más información acerca de la conformidad con FedRAMP, consulte FedRAMP.

SOC e ISO

AWS RAM se puede utilizar para cargas de trabajo sujetas al cumplimiento del Control Organizativo de Servicios (SOC) y a las normas ISO 9001, ISO 27001, ISO 27017, ISO 27018 e ISO 27701 de la Organización Internacional de Normalización (ISO). Los clientes de los sectores financiero, de la salud y otros sectores regulados pueden obtener información sobre los procesos y controles de seguridad que protegen los datos de los clientes, y que está disponible en los informes de SOC y en los certificados ISO y CSA STAR de AWS en AWS Artifact.

Para obtener más información sobre conformidad, consulte SOC.

Para obtener más información sobre la conformidad ISO, consulte ISO 9001, ISO 27001, ISO 27017, ISO 27018 e ISO 27701.

Empezar con AWS RAM

Con AWS Resource Access Manager, puede compartir los recursos que le pertenecen con otras personas Cuentas de AWS. Si su cuenta está gestionada por AWS Organizations, también puede compartir recursos con las demás cuentas de su organización. También puede usar los recursos que otras Cuentas de AWS hayan compartido con usted.

Si no habilitas el uso compartido interno AWS Organizations, no podrás compartir los recursos con tu organización ni con las unidades organizativas (OU) de tu organización. Sin embargo, puedes seguir compartiendo recursos con personas Cuentas de AWS de tu organización. Cuando se trate de tipos de recursos compatibles, también puede compartir los recursos con funciones o usuarios individuales de AWS Identity and Access Management (IAM) de su organización. En este caso, tales entidades principales se tratan como cuentas externas y no como parte de la organización. Reciben una invitación para unirse al recurso compartido, y deben aceptar la invitación para obtener acceso a los recursos compartidos.

Contenido

Términos y conceptos para AWS RAM

Los siguientes conceptos ayudan a explicar cómo puedes usar AWS Resource Access Manager (AWS RAM) para compartir tus recursos.

Uso compartido de recursos

Los recursos se comparten AWS RAM mediante la creación de un recurso compartido. Un recurso compartido consta de los tres elementos siguientes:

- Una lista de uno o más AWS recursos para compartir.
- Una lista de una o más entidades principales a las que se concede acceso.
- Un permiso administrado para cada tipo de recurso que se incluya en el recurso compartido. Cada permiso administrado se aplica a todos los recursos de ese tipo en ese recurso compartido.

Después de AWS RAM crear un recurso compartido, las entidades principales especificadas en el recurso compartido pueden tener acceso a los recursos del recurso compartido.

- Si activas el AWS RAM uso compartido y los directores con AWS Organizations los que compartes pertenecen a la misma organización que la cuenta compartida, dichos directores podrán recibir acceso en cuanto el administrador de la cuenta les conceda permisos para usar los recursos mediante una política de permisos AWS Identity and Access Management (IAM).
- Si no activas el uso AWS RAM compartido con Organizations, puedes seguir compartiendo los recursos con Cuentas de AWS las personas de tu organización. El administrador de la cuenta consumidora recibe una invitación para unirse al recurso compartido, y debe aceptarla para que las entidades principales especificadas en el recurso compartido puedan acceder a los recursos compartidos.
- También puede compartir con cuentas externas a su organización, si el tipo de recurso lo admite. El administrador de la cuenta consumidora recibe una invitación para unirse al recurso compartido, y debe aceptarla para que las entidades principales especificadas en el recurso compartido puedan acceder a los recursos compartidos. Para obtener información sobre los tipos de recursos que admiten este tipo de uso compartido, consulte Recursos que se pueden compartir AWS y fíjese en la columna Puede compartir con cuentas externas a su organización.

Cuentas que comparte

La cuenta de uso compartido contiene el recurso que se comparte y en la que el AWS RAM administrador crea el AWS recurso compartido mediante AWS RAM.

Un AWS RAM administrador es un director de IAM que tiene permisos para crear y configurar recursos compartidos en. Cuenta de AWS Como AWS RAM su función consiste en adjuntar una política basada en recursos a los recursos de un recurso compartido, el AWS RAM administrador también debe tener permisos para llamar a la `PutResourcePolicy` operación en cada tipo de recurso incluido en un recurso compartido. Servicio de AWS

Entidades principales consumidoras

La cuenta consumidora es aquella Cuenta de AWS con la que se comparte un recurso. El recurso compartido puede especificar una cuenta completa como entidad principal o, en el caso de ciertos tipos de recursos, roles o usuarios individuales de la cuenta. Para obtener información sobre los tipos de recursos que admiten este tipo de uso compartido, consulte Recursos que se pueden compartir AWS y fíjese en la columna Puede compartir con roles y usuarios de IAM.

AWS RAM también apoya a los directores de servicio como consumidores de recursos compartidos. Para obtener información sobre los tipos de recursos que admiten este tipo de uso compartido, consulte Recursos que se pueden compartir AWS y fíjese en la columna Puede compartir con entidades principales de servicio.

Las entidades principales de la cuenta consumidora pueden realizar solo las acciones permitidas por los dos permisos siguientes:

- Los permisos administrados adjuntos al recurso compartido. Especifican los permisos máximos que se pueden conceder a las entidades principales de la cuenta consumidora.
- Las políticas basadas en la identidad de IAM adjuntadas a roles o usuarios individuales por el administrador de IAM en la cuenta consumidora. Esas políticas deben conceder acceso `Allow` a acciones específicas y al nombre de recurso de Amazon (ARN) de un recurso de la cuenta que comparte.

AWS RAM admite los siguientes tipos principales de IAM como consumidores de recursos compartidos:

- Otro Cuenta de AWS: el recurso compartido hace que los recursos incluidos en la cuenta de uso compartido estén disponibles para la cuenta consumidora.
- Roles o usuarios individuales de IAM en otra cuenta: algunos tipos de recursos permiten compartir directamente con roles o usuarios individuales de IAM. Identifique este tipo de entidad principal por su ARN.
  - Rol de IAM: `arn:aws:iam::123456789012:role/rolename`
  - Usuario de IAM: `arn:aws:iam::123456789012:user/username`
- Principal de servicio: comparte un recurso con un AWS servicio para conceder al servicio acceso a un recurso compartido. Compartir el principal del AWS servicio permite que un servicio tome medidas en su nombre para aliviar la carga operativa.

  Para compartir con una entidad principal de servicio, seleccione que desea permitir el uso compartido con cualquiera y, a continuación, en Seleccione el tipo de entidad principal, elija Entidad principal de servicio en la lista desplegable. Especifique el nombre de la entidad principal de servicio con el siguiente formato:

  - *`service-id`*`.amazonaws.com`

  Para reducir el riesgo del suplente confuso, la política de recursos muestra el ID de cuenta del propietario del recurso en la clave de condición `aws:SourceAccount`.

- Cuentas de una organización: si la cuenta compartida está gestionada por AWS Organizations, el recurso compartido puede especificar el identificador de la organización para compartirlo con todas las cuentas de la organización. Como alternativa, el recurso compartido también puede especificar un ID de unidad organizativa (OU) para compartirlo con todas las cuentas de esa OU. Una cuenta compartida solo puede compartir con su propia organización o unidad organizativa IDs dentro de su propia organización. Especifique las cuentas de una organización por el ARN de la organización o de la OU.
  - Todas las cuentas de una organización: a continuación se muestra un ejemplo del ARN de una organización de AWS Organizations:

    ```
    arn:aws:organizations::123456789012:organization/o-<orgid>
    ```

  - Todas las cuentas de una unidad organizativa: a continuación se muestra un ejemplo del ARN de un ID de OU:

    ```
    arn:aws:organizations::123456789012:organization/o-<orgid>/ou-<rootid>-<ouid>
    ```

> **Important**
>
> Cuando comparte con una organización o unidad organizativa, y ese ámbito incluye la cuenta propietaria del recurso compartido, todas las entidades principales de la cuenta compartida automáticamente obtienen acceso a los recursos del recurso compartido. El acceso concedido viene definido por los permisos administrados asociados al recurso compartido. Esto se debe a que la política basada en los recursos que se AWS RAM adjunta a cada recurso del recurso compartido utiliza `"Principal": "*"` Para obtener más información, consulte Implicaciones del uso de "Principal": "*" en una política basada en recursos.
>
> Las entidades principales de las demás cuentas consumidoras no obtienen acceso a los recursos del recurso compartido de inmediato. Los administradores de las demás cuentas primero deben adjuntar políticas de permisos basados en identidad a las entidades principales correspondientes. Esas políticas deben conceder el `Allow` acceso a los recursos individuales ARNs del recurso compartido. Los permisos de dichas políticas no pueden superar los especificados en el permiso administrado asociado al recurso compartido.

Política basada en los recursos

Las políticas basadas en recursos son documentos de texto JSON que implementan el lenguaje de políticas de IAM. A diferencia de las políticas basadas en la identidad que se asocian al principal, como un rol o un usuario de IAM, las políticas basadas en recursos se asocian al recurso. AWS RAM crea políticas basadas en los recursos en su nombre en función de la información que proporciona para su uso compartido de recursos. Debe especificar un elemento de política de `Principal` que determine quién puede acceder al recurso. Para obtener más información, consulte Políticas basadas en identidad y políticas basadas en recursos en la Guía del usuario de IAM.

Las políticas basadas en recursos generadas por se AWS RAM evalúan junto con todos los demás tipos de políticas de IAM. Esto incluye cualquier política de IAM basada en la identidad asociada a los principales que intenten acceder al recurso, así como las políticas de control de servicios (SCPs) que puedan aplicarse al recurso. AWS Organizations Cuenta de AWS Las políticas basadas en recursos generadas por ellas AWS RAM participan en la misma lógica de evaluación de políticas que todas las demás políticas de IAM. Para obtener detalles completos sobre la evaluación de políticas y sobre cómo determinar los permisos resultantes, consulte Lógica de evaluación de políticas en la Guía del usuario de IAM.

AWS RAM proporciona una experiencia de intercambio de recursos sencilla y segura al proporcionar políticas easy-to-use abstractas basadas en los recursos.

Para los tipos de recursos que respaldan las políticas basadas en los recursos, crea y administra AWS RAM automáticamente las políticas basadas en los recursos por usted. Para un recurso determinado, AWS RAM crea la política basada en recursos combinando la información de todos los recursos compartidos que incluyen dicho recurso. Por ejemplo, piensa en una canalización de Amazon SageMaker AI que compartes utilizando AWS RAM e incluyendo en dos recursos compartidos diferentes. Podría utilizar un recurso compartido para proporcionar acceso de solo lectura a toda la organización. A continuación, podría utilizar el otro recurso compartido para conceder únicamente permisos de ejecución de SageMaker IA a una sola cuenta. AWS RAM combina automáticamente esos dos conjuntos diferentes de permisos en una única política de recursos con varias declaraciones. A continuación, adjunta la política combinada basada en recursos al recurso de la canalización. Puede ver esta política de recursos subyacente llamando a la GetResourcePolicyoperación. Servicios de AWS a continuación, utilice esa política basada en los recursos para autorizar a cualquier director que intente realizar una acción en el recurso compartido.

Si bien puede crear políticas basadas en recursos manualmente y adjuntarlas a sus recursos llamando a `PutResourcePolicy`, le recomendamos que utilice AWS RAM , ya que ofrece las siguientes ventajas:

- Capacidad de descubrimiento para los consumidores de recursos compartidos: si compartes los recursos mediante el uso AWS RAM, los usuarios pueden ver todos los recursos compartidos con ellos directamente en la consola del servicio propietario del recurso y en las operaciones de API, como si esos recursos estuvieran directamente en la cuenta del usuario. Por ejemplo, si compartes un AWS CodeBuild proyecto con otra cuenta, los usuarios de la cuenta consumidora pueden ver el proyecto en la CodeBuild consola y ver los resultados de las operaciones de CodeBuild API realizadas. Los recursos que se comparten adjuntando directamente una política basada en recursos no están visibles de este modo. En su lugar, debe detectar el recurso y hacer referencia a él explícitamente por su ARN.
- Capacidad de administración para los propietarios de acciones: si compartes los recursos mediante el uso AWS RAM, los propietarios de los recursos de la cuenta compartida pueden ver de forma centralizada qué otras cuentas tienen acceso a sus recursos. Si comparte un recurso utilizando una política basada en recursos, solo podrá ver las cuentas consumidoras examinando la política de los recursos individuales en la consola de servicio o API correspondiente.
- Eficiencia: si compartes los recursos mediante el uso AWS RAM, puedes compartir varios recursos y administrarlos como una unidad. Los recursos que se comparten mediante el uso exclusivo de políticas basadas en recursos requieren que se adjunten políticas individuales a cada recurso que se comparte.
- Simplicidad: con AWS RAM esto, no necesita entender el lenguaje de políticas de IAM basado en JSON. AWS RAM proporciona permisos ready-to-use AWS gestionados entre los que puede elegir para adjuntarlos a sus recursos compartidos.

Al utilizarlos AWS RAM, puede incluso compartir algunos tipos de recursos que aún no son compatibles con las políticas basadas en recursos. Para estos tipos de recursos, genera AWS RAM automáticamente una política basada en los recursos como representación de los permisos reales. Los usuarios pueden ver esta representación llamando a GetResourcePolicy. Esto incluye los siguientes tipos de recursos:

- Amazon Aurora: clústeres de base de datos (DB)
- Amazon EC2: reservas de capacidad y hosts dedicados
- AWS License Manager — Configuraciones de licencia
- AWS Outposts — Tablas de rutas, puestos de avanzada y sitios de las pasarelas de enlace locales

- Amazon Route 53: reglas de reenvío
- Amazon Virtual Private Cloud: IPv4 direcciones, listas de prefijos, subredes, destinos de espejo de tráfico, pasarelas de tránsito y dominios de multidifusión de pasarelas de tránsito propiedad de los clientes

AWS RAM Ejemplos de políticas generadas basadas en recursos

Si comparte un recurso de imagen de EC2 Image Builder con una cuenta individual AWS RAM , genera una política similar al ejemplo siguiente y la adjunta a todos los recursos de imagen que estén incluidos en el recurso compartido.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:root"
            },
            "Action": [
                "imagebuilder:GetImage",
                "imagebuilder:ListImages"
            ],
            "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
        }
    ]
}
```

Si comparte un recurso de imagen de EC2 Image Builder con un rol o usuario de IAM Cuenta de AWS diferente AWS RAM , genera una política similar al ejemplo siguiente y la adjunta a todos los recursos de imagen que estén incluidos en el recurso compartido.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:role/MySampleRole"
            },
            "Action": [
                "imagebuilder:GetImage",
                "imagebuilder:ListImages"
            ],
            "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
        }
    ]
}
```

Si comparte un recurso de imagen de EC2 Image Builder con todas las cuentas de una organización o con las cuentas de una unidad organizativa AWS RAM , genera una política similar al ejemplo siguiente y la adjunta a todos los recursos de imagen que estén incluidos en el recurso compartido.

> **Note**
>
> Esta política usa `"Principal": "*"` y luego usa el elemento `"Condition"` para restringir los permisos a las identidades que coincidan con los `PrincipalOrgID` especificados. Para obtener más información, consulte Implicaciones del uso de "Principal": "*" en una política basada en recursos.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "imagebuilder:GetImage",
                "imagebuilder:ListImages"
```

```
            ],
            "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-123456789"
                }
            }
        }
    ]
}
```

Implicaciones del uso de "Principal": "*" en una política basada en recursos

Cuando se incluye `"Principal": "*"` en una política basada en recursos, la política concede acceso a todas las entidades principales de IAM de la cuenta que contiene el recurso, con sujeción a las restricciones que imponga un elemento `Condition`, si existe. Las instrucciones `Deny` explícitas de cualquier política que se aplique a la entidad principal de llamada anulan los permisos otorgados por esta política. Sin embargo, una instrucción `Deny` implícita (es decir, en ausencia de una instrucción `Allow` explícita) en cualquier política de identidad, política de límite de permisos o política de sesión aplicable no da como resultado una instrucción `Deny` a las entidades principales a las que dicha política basada en recursos concede acceso a una determinada acción.

Si este comportamiento no es deseable en su caso, puede limitarlo añadiendo una instrucción `Deny` explícita a una política de identidad, límite de permisos o política de sesión que afecte a los roles y usuarios pertinentes.

Permisos administrados

Los permisos administrados definen qué acciones pueden realizar las entidades principales, y en qué condiciones, para los tipos de recursos admitidos en un recurso compartido. Al crear un recurso compartido, debe especificar qué permiso administrado desea usar para cada tipo de recurso que esté incluido en el recurso compartido. Un permiso administrado enumera el conjunto `actions` y las condiciones que los directores pueden ejecutar con el recurso compartido. AWS RAM

Puede adjuntar un solo permiso administrado por cada tipo de recurso de un recurso compartido. No puede crear un recurso compartido en el que algunos recursos de un determinado tipo usen un permiso administrado y otros recursos del mismo tipo usen un permiso administrado diferente. Para ello, tendría que crear dos recursos compartidos diferentes y dividir los recursos entre ellos,

atribuyendo a cada conjunto un permiso administrado diferente. Existen dos tipos diferentes de permisos administrados:

AWS permisos gestionados

AWS Los permisos gestionados los crean y mantienen los permisos, AWS y los conceden para situaciones comunes de los clientes. AWS RAM define al menos un permiso AWS administrado para cada tipo de recurso compatible. Algunos tipos de recursos admiten más de un permiso AWS administrado, con un permiso administrado designado como AWS predeterminado. El permiso AWS administrado predeterminado está asociado a menos que especifique lo contrario.

Permisos administrados por el cliente

Los permisos administrados por el cliente son permisos administrados que usted crea y mantiene especificando con precisión qué acciones se pueden realizar en los recursos que se comparten con AWS RAM y en qué condiciones. Por ejemplo, digamos que desea limitar el acceso de lectura a sus grupos del Administrador de direcciones IP (IPAM) de Amazon VPC, que le ayudan a administrar sus direcciones IP a gran escala. Puede crear permisos administrados por el cliente para que sus desarrolladores asignen direcciones IP, pero no ver el rango de direcciones IP que asignan otras cuentas de desarrollador. Puede seguir las prácticas recomendadas de privilegio mínimo para conceder únicamente los permisos necesarios para realizar tareas en los recursos compartidos.

Puede definir su propio permiso para un tipo de recurso de un recurso compartido, con la opción de añadir condiciones tales como claves de contexto globales y claves específica de servicio para especificar las condiciones en las que las entidades principales tienen acceso al recurso. Estos permisos se pueden usar en uno o más AWS RAM recursos compartidos. Los permisos administrados por el cliente son específicos de una región.

AWS RAM utiliza los permisos gestionados como entrada para crear las políticas basadas en recursos para los recursos que compartes.

Versión del permiso administrado

Cualquier cambio en un permiso administrado se representa como una nueva versión de ese permiso administrado. La nueva versión es la predeterminada para todos los recursos compartidos nuevos. Cada permiso administrado siempre tiene una versión designada como versión predeterminada. Al crear o AWS crear una nueva versión de permisos administrados, debe actualizar de forma explícita el permiso administrado para cada recurso compartido existente. Puede evaluar

los cambios antes de aplicarlos al recurso compartido en este paso. Todos los recursos compartidos nuevos utilizarán automáticamente la nueva versión del permiso administrado para el tipo de recurso correspondiente.

AWS versiones de permisos gestionados

AWS gestiona todos los cambios en los permisos AWS gestionados. Estos cambios abordan nuevas funcionalidades o eliminan deficiencias detectadas. Solo puede aplicar la versión predeterminada de un permiso administrado a sus recursos compartidos.

Versiones de los permisos administrados por el cliente

Usted se encarga de gestionar todos los cambios en los permisos administrados por el cliente. Puede crear una nueva versión predeterminada, establecer una versión anterior como predeterminada o eliminar las versiones que ya no estén asociadas a ningún recurso compartido. Puede haber hasta cinco versiones de cada permiso administrado por el cliente.

Al crear o actualizar un recurso compartido, solo puede adjuntar la versión predeterminada del permiso administrado especificado. Para obtener más información, consulte Actualización de los permisos AWS gestionados a una versión más reciente.

Compartir sus AWS recursos

Para compartir un recurso de su propiedad mediante el uso AWS RAM, haga lo siguiente:

- Habilite el uso compartido de recursos dentro AWS Organizations (opcional)
- Crear un recurso compartido

Notas

- Compartir un recurso con entidades ajenas al propietario del Cuenta de AWS recurso no cambia los permisos ni las cuotas que se aplican al recurso dentro de la cuenta que lo creó.
- AWS RAM es un servicio regional. Los principales con los que comparte recursos solo pueden acceder a los recursos compartidos en el lugar Regiones de AWS en el que se crearon los recursos.

- Algunos recursos tienen consideraciones y requisitos previos especiales para su uso compartido. Para obtener más información, consulte Recursos que se pueden compartir AWS.

Habilite el uso compartido de recursos dentro AWS Organizations

Cuando su cuenta esté gestionada por AWS Organizations, podrá aprovecharla para compartir recursos con mayor facilidad. Con o sin organizaciones, un usuario puede compartir con cuentas individuales. Sin embargo, si su cuenta pertenece a una organización, puede compartir con cuentas individuales, así como con todas las cuentas de la organización o de una OU, sin necesidad de enumerar cada cuenta.

Para compartir recursos dentro de una organización, primero debes usar la AWS RAM consola o AWS Command Line Interface (AWS CLI) para habilitar el uso compartido con AWS Organizations. Cuando compartes recursos en tu organización, AWS RAM no envía invitaciones a los directores. Las entidades principales de su organización obtienen acceso a los recursos compartidos sin necesidad de intercambiar invitaciones.

Cuando habilitas el uso compartido de recursos en tu organización, AWS RAM crea un rol vinculado a un servicio denominado. **`AWSServiceRoleForResourceAccessManager`** Solo el AWS RAM servicio puede asumir este rol y otorga AWS RAM permiso para recuperar información sobre la organización de la que es miembro mediante la política AWS administrada. `AWSResourceAccessManagerServiceRolePolicy`

> **Note**
>
> De forma predeterminada, si habilitas el uso compartido con AWS Organizations, el uso compartido de recursos dentro de tu organización restringe el acceso a los consumidores de la misma organización. Si una cuenta de consumidor abandona la organización, esa cuenta pierde el acceso a los recursos del recurso compartido. Esta restricción se aplica tanto si comparte los recursos con una unidad organizativa, con toda la organización o con una cuenta individual de la organización.
> Para account-to-account compartir dentro de su organización,
> puede conservar el acceso compartido cuando las cuentas `True` se `RetainSharingOnAccountLeaveOrganization` vayan configurando cuando cree un nuevo recurso compartido. Con esta configuración habilitada, AWS RAM envía una invitación

a la cuenta consumidora (similar a compartir con cuentas externas). La cuenta conserva el acceso a los recursos compartidos incluso si abandona la organización.
La `RetainSharingOnAccountLeaveOrganization` configuración tiene los siguientes requisitos y limitaciones:

- Requiere `allowExternalPrincipals` ser `True`
- Solo se puede configurar al crear nuevos recursos compartidos
- No se aplica al uso compartido con la organización OUs o con toda la organización
- Cuando `RetainSharingOnAccountLeaveOrganization` está establecido en`True`, no puede usar recursos compartidos para compartir recursos que solo se pueden compartir dentro de una organización.

Si ya no necesita compartir recursos con toda la organización OUs, puede deshabilitar el uso compartido de recursos. Para obtener más información, consulte Deshabilitar el uso compartido de recursos con AWS Organizations.

Permisos mínimos

Para ejecutar los procedimientos que se describen a continuación, debe iniciar sesión como entidad principal en la cuenta de administración de la organización que tenga los siguientes permisos:

- `ram:EnableSharingWithAwsOrganization`
- `iam:CreateServiceLinkedRole`
- `organizations:enableAWSServiceAccess`
- `organizations:DescribeOrganization`

Requisitos

- Solo puede realizar estos pasos si ha iniciado sesión como entidad principal en la cuenta de administración de la organización.
- La organización debe tener todas las características habilitadas. Para obtener más información, consulte Habilitar todas las características en la organización en la Guía del usuario de AWS Organizations .

> **Important**
>
> Debe habilitar el uso compartido con AWS Organizations mediante la AWS RAM consola o el AWS CLI comando enable-sharing-with-aws-organization. Así se asegurará de crear el rol vinculado al servicio `AWSServiceRoleForResourceAccessManager`. Si habilitas el acceso de confianza AWS Organizations mediante la AWS Organizations consola o el enable-aws-service-access AWS CLI comando, no se crea el rol `AWSServiceRoleForResourceAccessManager` vinculado al servicio y no puedes compartir recursos dentro de tu organización.

Console

Para habilitar el uso compartido de recursos dentro de la organización

1. Abre la página de configuración en la AWS RAM consola.
2. Selecciona Activar compartir con y AWS Organizations, a continuación, selecciona Guardar configuración.

AWS CLI

Para habilitar el uso compartido de recursos dentro de la organización

Usa el comando enable-sharing-with-aws-organization.

Este comando se puede utilizar en cualquier Región de AWS lugar y permite compartir con todas las regiones AWS Organizations en las que AWS RAM se admite.

```
$ aws ram enable-sharing-with-aws-organization
{
    "returnValue": true
}
```

Crear un recurso compartido

Para compartir recursos de su propiedad, debe crear un recurso compartido. A continuación se ofrece información general sobre el proceso:

1. Añada los recursos que desea compartir.

2. Para cada tipo de recurso que incluya en el recurso compartido, especifique el permiso administrado que se debe utilizar para dicho tipo de recurso.
   - Puede elegir uno de los permisos AWS gestionados disponibles, un permiso gestionado por el cliente existente o crear uno nuevo gestionado por el cliente.
   - AWS Los permisos gestionados se crean AWS para cubrir los casos de uso estándar.
   - Los permisos administrados por el cliente le permiten personalizar sus propios permisos administrados para adaptarlos a sus necesidades empresariales y de seguridad.

   > **Note**
   >
   > Si el permiso administrado seleccionado tiene varias versiones, se adjunta AWS RAM automáticamente la versión predeterminada. Solo es posible adjuntar la versión designada como predeterminada.

3. Especifique las entidades principales que desea que tengan acceso a los recursos.

Consideraciones

- Si más adelante necesita eliminar un AWS recurso que haya incluido en un recurso compartido, le recomendamos que primero elimine el recurso de cualquier recurso compartido que lo incluya o que elimine el recurso compartido.
- Puede ver una lista de los tipos de recursos que se pueden incluir en un recurso compartido en Recursos que se pueden compartir AWS.
- Solo puede compartir los recursos que sean de su propiedad. No puede compartir recursos que se hayan compartido con usted.
- AWS RAM es un servicio regional. Al compartir un recurso con entidades principales de otras Cuentas de AWS, dichas entidades principales deben acceder a cada recurso desde la misma Región de AWS en la que se creó. Para acceder a los recursos globales compatibles, puede acceder a esos recursos desde cualquiera de los Región de AWS que sean compatibles con la consola de servicio y las herramientas de ese recurso. Puede ver tales recursos compartidos y sus recursos globales en la consola y en las herramientas de AWS RAM únicamente en la región de origen designada, Este de EE. UU. (Norte de Virginia), `us-east-1`. Para obtener más información AWS RAM y recursos globales, consulteCompartir recursos regionales frente a recursos globales.
- Si la cuenta desde la que compartes forma parte de una organización AWS Organizations y la opción de compartir dentro de tu organización está habilitada, todos los responsables de la organización con los que compartas recursos tendrán acceso automáticamente a los recursos

compartidos sin necesidad de utilizar invitaciones. Una entidad principal de una cuenta con la que comparte fuera del contexto de una organización recibe una invitación para unirse al recurso compartido y solo obtiene acceso a los recursos compartidos tras aceptar la invitación.

- Si comparte con una entidad principal de servicio, no podrá asociar ninguna otra entidad principal al recurso compartido.
- Si el uso compartido es entre cuentas o entidades principales que forman parte de una organización, cualquier cambio en la pertenencia a la organización afectará de manera dinámica al acceso al recurso compartido.
  - Si agrega una cuenta Cuenta de AWS a la organización o una unidad organizativa que tenga acceso a un recurso compartido, esa nueva cuenta de miembro tendrá acceso automáticamente al recurso compartido. El administrador de la cuenta con la que ha compartido puede entonces conceder a determinadas entidades principales de dicha cuenta acceso a los recursos del ese recurso compartido.
  - Si elimina una cuenta de la organización o una OU que tenga acceso a un recurso compartido, las entidades principales de dicha cuenta pierden automáticamente el acceso a los recursos a los que se accedía a través del recurso compartido.
  - Si ha compartido directamente con una cuenta de miembro o con roles o usuarios de IAM de la cuenta de miembro y, a continuación, la elimina de la organización, las entidades principales de esa cuenta pierden el acceso a los recursos a los que se accedía a través del recurso compartido.

> **Important**
>
> Cuando comparte con una organización o OU, y ese ámbito incluye la cuenta propietaria del recurso compartido, todas las entidades principales de la cuenta compartida automáticamente obtienen acceso a los recursos del recurso compartido. El acceso concedido viene definido por los permisos administrados asociados al recurso compartido. Esto se debe a que la política basada en los recursos que se AWS RAM adjunta a cada recurso del recurso compartido utiliza `"Principal": "*"` Para obtener más información, consulte Implicaciones del uso de "Principal": "*" en una política basada en recursos.
> Las entidades principales de las demás cuentas consumidoras no obtienen acceso a los recursos del recurso compartido de inmediato. Los administradores de las demás cuentas primero deben adjuntar políticas de permisos basados en identidad a las entidades principales correspondientes. Esas políticas deben conceder el `Allow` acceso a los recursos individuales ARNs del recurso compartido. Los permisos de dichas políticas

no pueden superar los especificados en el permiso administrado asociado al recurso compartido.

- Solo puede agregar la organización de la que forma parte su cuenta y OUs desde esa organización a sus recursos compartidos. No puede agregar OUs ni organizaciones ajenas a la suya a un recurso compartido como entidades principales. Sin embargo, puedes añadir funciones y usuarios de IAM individuales Cuentas de AWS o, en el caso de los servicios compatibles, ajenos a la organización como directores de un recurso compartido.

> **Note**
>
> No todos los tipos de recursos se pueden compartir con roles y los usuarios de IAM. Para obtener información sobre los recursos que puede compartir con estas entidades principales, consulte Recursos que se pueden compartir AWS.

- Para los siguientes tipos de recursos, dispone de siete días para aceptar la invitación a unirse al recurso compartido para los siguientes tipos de recursos. Si no acepta la invitación antes de que caduque, esta se rechazará automáticamente.

> **Important**
>
> En el caso de los tipos de recursos compartidos que no figuran en la lista siguiente, dispone de 12 horas para aceptar la invitación a unirse al recurso compartido. Transcurridas 12 horas, la invitación caduca y se elimina la asociación de la entidad principal de usuario final del recurso compartido. Los usuarios finales ya no pueden aceptar la invitación.

  - Amazon Aurora: clústeres de base de datos (DB)
  - Amazon EC2: reservas de capacidad y hosts dedicados
  - AWS License Manager — Configuraciones de licencia
  - AWS Outposts — Tablas de rutas, puestos de avanzada y sitios de las pasarelas de enlace locales
  - Amazon Route 53: reglas de reenvío
  - Amazon VPC: IPv4 direcciones propiedad de los clientes, listas de prefijos, subredes, objetivos de espejo de tráfico, pasarelas de tránsito, dominios de multidifusión de pasarelas de tránsito

Console

Para crear un recurso compartido

1. Abra la consola de AWS RAM.
2. Como AWS RAM los recursos compartidos existen de forma específica Regiones de AWS, elija el recurso correspondiente en la lista desplegable situada en la esquina superior derecha Región de AWS de la consola. Para ver los recursos compartidos que contienen recursos globales, debe establecer en EE.UU. Este (Norte de Virginia), (). Región de AWS `us-east-1` Para obtener más información sobre cómo compartir recursos globales, consulte Compartir recursos regionales frente a recursos globales. Si desea incluir recursos globales en el recurso compartido, debe elegir la región de origen designada, Este de EE. UU. (Norte de Virginia),`us-east-1`.
3. Si es la primera vez que lo AWS RAM hace, elija Crear un recurso compartido en la página de inicio. De lo contrario, elija Crear recurso compartido en la página Compartidos por mí: recursos compartidos.
4. En Paso 1: Especifique los detalles del recurso compartido, haga lo siguiente:

   a. En Nombre, introduzca un nombre descriptivo para el recurso compartido.

   b. En Recursos, elija los recursos que desea añadir al recurso compartido de la siguiente manera:

      - En Seleccionar tipo de recurso, elija el tipo de recurso que desea compartir. Esta acción filtra la lista de recursos que se pueden compartir y muestra solo los recursos del tipo seleccionado.
      - En la lista de recursos resultante, seleccione las casillas de verificación situadas junto a los recursos individuales que desee compartir. Los recursos seleccionados se mueven a Recursos seleccionados.

        Si va a compartir recursos asociados a una zona de disponibilidad concreta, usar el ID de zona de disponibilidad (ID de AZ) le ayudará a determinar la ubicación relativa de los recursos en las distintas cuentas. Para obtener más información, consulte ID de zona de disponibilidad para sus recursos de AWS.

   c. (Opcional) Para adjuntar etiquetas al recurso compartido, en Etiquetas, introduzca una clave y un valor de etiqueta. Para añadir otras, elija Añadir nueva etiqueta. Repita este paso tantas veces como sea necesario. Estas etiquetas se aplican únicamente al recurso compartido propiamente dicho, no a los recursos que este contiene.

5. Elija Siguiente.
6. En el paso 2: asocie un permiso administrado a cada tipo de recurso, puede elegir asociar un permiso administrado creado por AWS al tipo de recurso, elegir un permiso administrado por el cliente existente o crear su propio permiso administrado por el cliente para los tipos de recursos compatibles. Para obtener más información, consulte Tipos de permisos administrados.

   Elija Crear permiso administrado por el cliente para crear un permiso administrado por el cliente que cumpla los requisitos de su caso de uso compartido. Para obtener más información, consulte Crear un permiso administrado por el cliente. Una vez que haya completado el proceso, elija

   y, a continuación, podrá seleccionar el nuevo permiso administrado por el cliente en la lista desplegable Permisos administrados.

   > **Note**
   >
   > Si el permiso administrado seleccionado tiene varias versiones, AWS RAM adjunta automáticamente la versión predeterminada. Solo es posible adjuntar la versión designada como predeterminada.

   Para mostrar las acciones que permite el permiso administrado, expanda Ver la plantilla de política de este permiso administrado.
7. Elija Siguiente.
8. En Paso 3: Otorgar acceso a entidades principales, haga lo siguiente:

   a. De forma predeterminada, está seleccionada la opción Permitir el uso compartido con cualquier persona, lo que significa que, en el caso de los tipos de recursos Cuentas de AWS que lo admiten, puede compartir recursos con personas ajenas a su organización. Esto no afecta a los tipos de recursos que solo se pueden compartir dentro de una organización, como las subredes de Amazon VPC. También puede compartir algunos tipos de recursos compatibles con roles y usuarios de IAM.

      Para restringir la capacidad de compartir recursos solo a las cuentas y entidades principales de su organización, elija Permitir compartir solo dentro de la organización.

b. En Entidades principales, haga lo siguiente:

- Para añadir la organización, una unidad organizativa (OU) o una Cuenta de AWS que forme parte de una organización, activa Mostrar estructura organizativa. Se muestra una vista en árbol de la organización. A continuación, seleccione la casilla de verificación situada junto a cada entidad principal que desee añadir.

> **Important**
>
> Cuando comparte con una organización o OU, y ese ámbito incluye la cuenta propietaria del recurso compartido, todas las entidades principales de la cuenta compartida automáticamente obtienen acceso a los recursos del recurso compartido. El acceso concedido viene definido por los permisos administrados asociados al recurso compartido. Esto se debe a que la política basada en los recursos que se AWS RAM adjunta a cada recurso del recurso compartido utiliza `"Principal": "*"` Para obtener más información, consulte Implicaciones del uso de "Principal": "*" en una política basada en recursos.
>
> Las entidades principales de las demás cuentas consumidoras no obtienen acceso a los recursos del recurso compartido de inmediato. Los administradores de las demás cuentas primero deben adjuntar políticas de permisos basados en identidad a las entidades principales correspondientes. Esas políticas deben conceder el `Allow` acceso a los recursos individuales ARNs del recurso compartido. Los permisos de dichas políticas no pueden superar los especificados en el permiso administrado asociado al recurso compartido.

- Si selecciona la organización (el ID comienza por `o-`), las entidades principales de todas las Cuentas de AWS de la organización podrán acceder al recurso compartido.
- Si selecciona una unidad organizativa (el identificador comienza por`ou-`), los directores de toda Cuentas de AWS la unidad organizativa y su unidad secundaria OUs pueden acceder al recurso compartido.
- Si selecciona una persona Cuenta de AWS, solo los directores de esa cuenta pueden acceder al recurso compartido.

> **Note**
>
> La opción Mostrar estructura organizativa aparece solo si la opción de compartir con AWS Organizations está habilitada y si se ha iniciado sesión en la cuenta de administración de la organización.
> No puede usar este método para especificar una Cuenta de AWS externa a la organización o un rol o usuario de IAM. En su lugar, debe desactivar la opción Mostrar estructura organizativa y usar la lista desplegable y el cuadro de texto para introducir el ID o el ARN.

- Para especificar una entidad principal mediante el ID o el ARN, incluidos las entidades principales externas a la organización, seleccione el tipo de entidad principal en cada caso. A continuación, introduzca el ID (para una Cuenta de AWS organización o una OU) o el ARN (para un rol o un usuario de IAM) y, a continuación, seleccione Agregar. Los tipos de entidades principales y los formatos de ID y ARN disponibles son los siguientes:
  - Cuenta de AWS— Para añadir un Cuenta de AWS, introduzca el ID de cuenta de 12 dígitos. Por ejemplo:

    ```
    123456789012
    ```

  - Organización: para añadir todos los elementos Cuentas de AWS de su organización, introduzca el ID de la organización. Por ejemplo:

    ```
    o-abcd1234
    ```

  - Unidad organizativa (OU): para añadir una OU, introduzca el ID de la OU. Por ejemplo:

    ```
    ou-abcd-1234efgh
    ```

  - Rol de IAM: para añadir un rol de IAM, introduzca el ARN del rol. Utilice la siguiente sintaxis:

    ```
    arn:partition:iam::account:role/role-name
    ```

    Por ejemplo:

    ```
    arn:aws:iam::123456789012:role/MyS3AccessRole
    ```

> **Note**
>
> Para obtener el ARN único de un rol de IAM, consulte la lista de roles en la consola de IAM, utilice el comando get-role AWS CLI o la acción de la API. GetRole

- Usuario de IAM: para añadir un usuario de IAM, introduzca el ARN del usuario. Utilice la siguiente sintaxis:

  `arn:`*`partition`*`:iam::`*`account`*`:user/`*`user-name`*

  Por ejemplo:

  `arn:aws:iam::123456789012:user/bob`

> **Note**
>
> Para obtener el ARN único de un usuario de IAM, consulte la lista de usuarios en la consola de IAM, utilice el get-user AWS CLI comando o la acción de la API. GetUser

- Entidad principal de servicio: para añadir una entidad principal de servicio, elija Entidad principal de servicio en el cuadro desplegable Seleccionar tipo de entidad principal. Introduzca el nombre de la entidad principal de servicio de AWS . Utilice la siguiente sintaxis:
  - *`service-id`*`.amazonaws.com`

    Por ejemplo:

    `pca-connector-ad.amazonaws.com`

c. En Entidades principales seleccionadas, compruebe que las entidades principales que ha especificado figuran en la lista.

9. Elija Siguiente.
10. En Paso 4: Revisión y creación, revise los detalles de configuración del recurso compartido. Para cambiar la configuración de cualquier paso, elija el enlace correspondiente al paso al que desea volver y realice los cambios necesarios.

11. Cuando haya terminado de revisar el recurso compartido, elija Crear recurso compartido.

    La asociación del recurso y la entidad principal puede tardar unos minutos en completarse. Espere a que finalice el proceso antes de intentar utilizar el recurso compartido.

12. Puede añadir y eliminar recursos y entidades principales, o aplicar etiquetas personalizadas al recurso compartido en cualquier momento. Puede cambiar el permiso administrado de los tipos de recursos que se incluyen en el recurso compartido para aquellos tipos que admitan más permisos que el permiso administrado predeterminado. Puede eliminar el recurso compartido cuando ya no desee compartir los recursos. Para obtener más información, consulte Compartir AWS recursos de su propiedad.

AWS CLI

Para crear un recurso compartido

Utilice el comando create-resource-share. El siguiente comando crea un recurso compartido que se comparte con todos los miembros de la organización Cuentas de AWS . El recurso compartido contiene una configuración de AWS License Manager licencia y concede los permisos administrados predeterminados para ese tipo de recurso.

> **Note**
>
> Si desea usar un permiso administrado por el cliente con un tipo de recurso en este recurso compartido, puede usar uno existente o crear uno nuevo. Anote el ARN del permiso administrado por el cliente y, a continuación, cree el recurso compartido. Para obtener más información, consulte Crear un permiso administrado por el cliente.

```
$ aws ram create-resource-share \
    --region us-east-1 \
    --name MyLicenseConfigShare \
    --permission-arns arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionLicenseConfiguration \
    --resource-arns arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-abc123 \
    --principals arn:aws:organizations::123456789012:organization/o-1234abcd
{
    "resourceShare": {
```

```
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
        "name": "MyLicenseConfigShare",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": true,
        "status": "ACTIVE",
        "creationTime": "2021-09-14T20:42:40.266000-07:00",
        "lastUpdatedTime": "2021-09-14T20:42:40.266000-07:00"
    }
}
```

Uso de AWS recursos compartidos

Para empezar a usar los recursos que se compartieron con su cuenta utilizando AWS Resource Access Manager, complete las siguientes tareas.

Tareas

- Responder a la invitación al recurso compartido
- Usar los recursos que se han compartido con usted

Responder a la invitación al recurso compartido

Si recibe una invitación para unirse a un recurso compartido, debe aceptarla para obtener acceso a los recursos compartidos.

No se utilizan invitaciones en las situaciones siguientes:

- Si formas parte de una organización AWS Organizations y el uso compartido en tu organización está activado, los directores de la organización tendrán acceso automáticamente a los recursos compartidos sin necesidad de invitaciones.
- Si compartes con el Cuenta de AWS propietario del recurso, los directores de esa cuenta tendrán acceso automáticamente a los recursos compartidos sin necesidad de invitaciones.

Console

Para responder a una invitación

1. Abra la página Compartidos conmigo: recursos compartidos de la consola de AWS RAM .

> **Note**
>
> Un recurso compartido solo está visible en el lugar Región de AWS en el que se creó. Si el recurso compartido esperado no aparece en la consola, puede que tengas que cambiarlo a otro Región de AWS mediante el control desplegable situado en la esquina superior derecha.

2. Revise la lista de recursos compartidos a los que se le ha concedido acceso.

   La columna Estado indica su estado de participación actual en el recurso compartido. El estado `Pending` indica que se le ha añadido a un recurso compartido, pero que aún no ha aceptado o rechazado la invitación.

3. Para responder a la invitación al recurso compartido, seleccione el ID del recurso compartido y elija Aceptar recurso compartido para aceptar la invitación, o Rechazar recurso compartido para rechazarla. Si rechaza la invitación, no obtendrá acceso a los recursos. Si acepta la invitación, obtendrá acceso a los recursos.

AWS CLI

Para empezar, obtenga una lista de las invitaciones a recursos compartidos que están a su disposición. El siguiente comando de ejemplo se ejecutó en la región `us-west-2`, y muestra que hay un recurso compartido disponible con el estado `PENDING`.

```
$ aws ram get-resource-share-invitations
{
    "resourceShareInvitations": [
        {
            "resourceShareInvitationArn": "arn:aws:ram:us-
west-2:111122223333:resource-share-invitation/1234abcd-ef12-9876-5432-aaaaaa111111",
            "resourceShareName": "MyNewResourceShare",
            "resourceShareArn": "arn:aws:ram:us-west-2:111122223333:resource-
share/1234abcd-ef12-9876-5432-bbbbbb222222",
            "senderAccountId": "111122223333",
            "receiverAccountId": "444455556666",
            "invitationTimestamp": "2021-09-15T15:00:32.568000-07:00",
            "status": "PENDING"
        }
    ]
```

```
}
```

Puede usar el nombre de recurso de Amazon (ARN) de la invitación del comando anterior como parámetro en el siguiente comando para aceptar la invitación.

```
$ aws ram accept-resource-share-invitation \
    --resource-share-invitation-arn arn:aws:ram:us-west-2:111122223333:resource-
share-invitation/1234abcd-ef12-9876-5432-aaaaaa111111
{
    "resourceShareInvitation": {
        "resourceShareInvitationArn": "arn:aws:ram:us-west-2:111122223333:resource-
share-invitation/1234abcd-ef12-9876-5432-aaaaaa111111",
        "resourceShareName": "MyNewResourceShare",
        "resourceShareArn": "arn:aws:ram:us-west-2:111122223333:resource-
share/1234abcd-ef12-9876-5432-bbbbbb222222",
        "senderAccountId": "111122223333",
        "receiverAccountId": "444455556666",
        "invitationTimestamp": "2021-09-15T15:14:12.580000-07:00",
        "status": "ACCEPTED"
    }
}
```

El resultado muestra que el `status` ha cambiado a `ACCEPTED`. Los recursos incluidos en ese recurso compartido ahora están disponibles para las entidades principales de la cuenta que los acepta.

Usar los recursos que se han compartido con usted

Una vez que acepte la invitación para unirse a un recurso compartido, podrá realizar determinadas acciones en los recursos compartidos. Estas acciones varían según el tipo de recurso. Para obtener más información, consulte Recursos que se pueden compartir AWS. Los recursos están disponibles directamente en la consola de servicio y API/CLI en las operaciones de cada recurso. Si el recurso es regional, debe utilizar el comando correcto Región de AWS en la consola de servicio o la API/CLI. Si el recurso es global, debe usar la región de origen designada, EE. UU. Este (Virginia del Norte). `us-east-1` Para ver el recurso AWS RAM, debe abrir la AWS RAM consola en la Región de AWS que se creó el recurso compartido.

Trabajar con recursos compartidos de AWS

Puede usar AWS Resource Access Manager (AWS RAM) para compartir recursos de AWS de su propiedad y obtener acceso a los recursos de AWS que se comparten con usted.

Contenido

Compartir recursos regionales frente a recursos globales

En este tema se analizan las diferencias en la forma en que AWS Resource Access Manager (AWS RAM) funciona con los recursos regionales y globales.

Los recursos pueden ser regionales o globales. Puede usar el cuarto campo del nombre de recurso de Amazon (ARN) para identificar si un recurso es regional o global. Los recursos regionales muestran la Región de AWS. Si este campo está en blanco, significa que el recurso es global.

¿En qué se diferencian los recursos regionales y globales?

Recursos regionales

La mayoría de los recursos con los que puede compartir AWS RAM son regionales. Los puede crear en una Región de AWS específica y, a continuación, existen en esa región. Para ver esos recursos o interactuar con ellos, debe dirigir sus operaciones hacia esa región. Por ejemplo, para crear una instancia de Amazon Elastic Compute Cloud (Amazon EC2) con, eliges Consola de administración de AWS la instancia en Región de AWS la que quieres crear la instancia. Si utilizas AWS Command Line Interface (AWS CLI) para crear la instancia, incluyes el `--region` parámetro. AWS SDKs Cada uno tiene su propio mecanismo equivalente para especificar la región que utiliza la operación.

Existen varios motivos para utilizar los recursos regionales. Una buena razón es asegurarse de que los recursos y los puntos de conexión de servicio que se utilizan para acceder a ellos estén lo más cerca posible del cliente. Esto mejora el rendimiento al minimizar la latencia. Otra razón es proporcionar un límite de aislamiento. Esto permite crear copias independientes de los recursos en varias regiones para distribuir la carga y mejorar la escalabilidad. Al mismo tiempo, aísla los recursos unos de otros para mejorar la disponibilidad.

Si especificas otro Región de AWS en la consola o en un AWS CLI comando, ya no podrás ver ni interactuar con los recursos que veías en la región anterior.

Cuando consulta el nombre de recurso de Amazon (ARN) de un recurso regional, la región que contiene el recurso se especifica como el cuarto campo del ARN. Por ejemplo, una instancia de Amazon EC2 es un recurso regional. Estos recursos tienen ARNs un aspecto similar al siguiente ejemplo para una VPC que existe en la `us-east-1` región.

```
arn:aws:ec2:us-east-1:123456789012:instance/i-0a6f30921424d3eee
```

Recursos globales

Algunos AWS servicios admiten recursos a los que puede acceder de forma global, lo que significa que puede utilizar el recurso desde cualquier lugar. No se especifica ninguno Región de AWS en la consola de un servicio global. Para acceder a un recurso global, no se especifica un `--region` parámetro cuando se utilizan las operaciones del servicio AWS CLI y del AWS SDK.

Los recursos globales admiten casos en los que es fundamental que solo pueda existir una instancia de un determinado recurso en cada momento dado. En estos casos, la replicación o sincronización entre copias en diferentes regiones no son adecuadas. Tener que acceder a un único punto de conexión global, con el posible aumento de la latencia, se considera aceptable para garantizar que cualquier cambio sea visible de forma instantánea para los consumidores del recurso. Por ejemplo, cuando creas una red principal de WAN AWS en la nube como recurso global, es coherente para todos los usuarios. Aparece como un único clúster global y continuo en todas las regiones.

El nombre de recurso de Amazon (ARN) de un recurso global no incluye una región. El cuarto campo del ARN está vacío, como se muestra en el siguiente ejemplo de ARN de una red central WAN en la nube.

```
arn:aws:networkmanager::123456789012:core-network/core-network-0514d38fa6f796cea
```

Recursos compartidos y sus regiones

AWS RAM es un servicio regional y un recurso compartido es regional. Por lo tanto, un recurso compartido puede contener recursos del Región de AWS mismo recurso compartido y cualquier recurso global compatible. La región en la que se crea el recurso compartido se denomina su región de origen.

> **Important**
>
> En la actualidad, se pueden crear recursos compartidos con recursos globales únicamente en la región de origen designada Este de EE. UU. (Norte de Virginia), `us-east-1`. Si bien puede crear el recurso compartido solo en esa única región de origen, cualquier recurso global compartido aparecerá como un recurso global estándar al visualizarlo en la consola de ese servicio o en las operaciones de CLI y SDK. La restricción a la región de origen se aplica únicamente al recurso compartido, no a los recursos que contiene.

Para compartir un recurso regional que haya creado en la `us-west-2` región, debe configurar la AWS RAM consola para usar `us-west-2` y crear el recurso compartido allí. No puede crear un recurso compartido que incluya recursos regionales de diferentes Regiones de AWS. Esto significa que, para compartir recursos de `us-west-2` y de `eu-north-1`, debe crear dos recursos

compartidos diferentes. No puede combinar recursos de dos regiones diferentes en un mismo recurso compartido.

Para compartir un recurso global en la AWS RAM consola, debe configurarla para que utilice la AWS RAM región de origen designada, EE. UU. Este (Norte de Virginia)`us-east-1`. A continuación, cree el recurso compartido en la región de origen designada. Solo puede combinar recursos globales en un recurso compartido con recursos de la región `us-east-1`.

Aunque el recurso global solo se puede ver en un AWS RAM recurso compartido en la región de origen designada, sigue siendo un recurso global después de compartirlo. Puedes acceder a él en el entorno compartido Cuentas de AWS desde cualquier región desde la que pudieras acceder a él en la versión original Cuenta de AWS.

Consideraciones

- Para crear un recurso compartido en la AWS RAM consola, debe usar la región que contiene los recursos que desea compartir. Si desea incluir un recurso global, debe usar la región de origen designada para crear el recurso compartido. Por ejemplo, para compartir una red principal de WAN en la AWS nube, debes crear el recurso compartido en la `us-east-1` región.
- Para ver o modificar un recurso compartido en la AWS RAM consola, debes usar la región que contiene el recurso compartido. Del mismo modo, las operaciones AWS RAM AWS CLI y las del SDK le permiten interactuar únicamente con los recursos compartidos que se encuentren en la región que especifique en la operación. Para ver o modificar recursos compartidos que contengan recursos globales, debe usar la región de origen designada, Este de EE. UU. (Norte de Virginia), `us-east-1`.
- Para ver un recurso regional en la AWS RAM consola e incluirlo en un recurso compartido, debe usar la región que contiene el recurso regional.
- Para ver un recurso global en la AWS RAM consola e incluirlo en un recurso compartido, debe usar la región de origen designada, EE. UU. Este (Norte de Virginia)`us-east-1`.
- Solo puede crear un recurso compartido con recursos regionales y globales a la vez en la región de origen designada, Este de EE. UU. (Norte de Virginia), `us-east-1`.

Compartir AWS recursos de su propiedad

Puede usar AWS Resource Access Manager (AWS RAM) para compartir los recursos que especifique con las entidades principales que especifique. En esta sección se describe cómo puede

crear nuevos recursos compartidos, modificar recursos compartidos existentes y eliminar recursos compartidos que ya no necesite.

Temas

Ver los recursos compartidos que ha creado en AWS RAM

Puede ver una lista de los recursos compartidos que ha creado. Puede ver qué recursos está compartiendo, así como las entidades principales con las que los comparte.

Console

Para ver sus recursos compartidos

1. Abra la página Compartidos por mí: recursos compartidos en la consola de AWS RAM.
2. Puesto que los recursos compartidos de AWS RAM son específicos de las diferentes Regiones de AWS, elija la Región de AWS que corresponda en la lista desplegable de la esquina superior derecha de la consola. Para ver los recursos compartidos que contienen recursos globales, debe definir la Región de AWS como Este de EE. UU. (Norte de Virginia), (`us-east-1`). Para obtener más información sobre cómo compartir recursos globales, consulte Compartir recursos regionales frente a recursos globales.
3. Si alguno de los permisos administrados que utilizan los recursos compartidos en los resultados tiene una nueva versión designada como predeterminada, la página le advertirá de ello mediante un banner. Puede optar por actualizar todas las versiones de los permisos administrados a la vez. Para ello, seleccione Revisar y actualizar todo en la parte superior de la página.

   Como alternativa, cuando se trate de recursos compartidos individuales con una o más versiones nuevas de los permisos administrados, la columna Estado mostrará la opción Actualización disponible. Al seleccionar ese enlace, se inicia el proceso de revisión de las

versiones actualizadas de los permisos administrados, lo que le permitirá asignarlas como versiones para los tipos de recursos pertinentes de dicho recurso compartido.

4. (Opcional) Aplique un filtro si desea buscar recursos compartidos específicos. Puede aplicar varios filtros para delimitar en mayor medida la búsqueda. Puede escribir una palabra clave (por ejemplo, parte del nombre de un recurso compartido) para que se muestren solo los recursos compartidos cuyo nombre incluya el texto especificado. Resalte el cuadro de texto para ver una lista desplegable de campos de atributo sugeridos. Una vez que elija uno, podrá elegir de la lista de valores disponibles para dicho campo. Puede añadir otros atributos o palabras clave hasta que encuentre el recurso que busca.
5. Elija el nombre del recurso compartido que desea revisar. La consola muestra la siguiente información sobre el recurso compartido:

   - Resumen: muestra el nombre, el ID, el propietario, el nombre de recurso de Amazon (ARN), la fecha de creación y el estado actual del recurso compartido, e indica si este se puede o no compartir con cuentas externas.
   - Permisos administrados: muestra una lista de los permisos administrados asociados al recurso compartido. Puede haber, como máximo, un permiso administrado por cada tipo de recurso incluido en el recurso compartido. Cada permiso administrado muestra la versión de dicho permiso que está asociada al recurso compartido. Si no se trata de la versión predeterminada, la consola muestra el enlace Actualizar a la versión predeterminada. Al seleccionar dicho enlace, tendrá la posibilidad de actualizar el recurso compartido para que utilice la versión predeterminada.
   - Recursos compartidos: muestra una lista de los recursos individuales que se incluyen en el recurso compartido. Elija el ID de un recurso para abrir una nueva pestaña del navegador y ver el recurso en la consola de su servicio nativo.
   - Entidades principales compartidas: muestra una lista de las entidades principales con las que se comparten los recursos.
   - Etiquetas: muestra una lista de los pares de clave-valor de etiqueta asociados al recurso compartido propiamente dicho; no se trata de las etiquetas asociadas a los recursos individuales incluidos en el recurso compartido.

AWS CLI

Para ver sus recursos compartidos

Puede usar el comando get-resource-shares con el parámetro `--resource-owner` definido como `SELF` para que se muestren los detalles de los recursos compartidos creados en su Cuenta de AWS.

En el siguiente ejemplo, se muestran los recursos compartidos que se comparten en la Región de AWS actual (`us-east-1`) para la Cuenta de AWS que realiza la llamada. Para obtener los recursos compartidos creados en otra región, use el parámetro `--region` *<region-code>*. Para incluir los recursos compartidos que contengan recursos globales, debe especificar la región Este de EE. UU. (Norte de Virginia), `us-east-1`.

```
$  aws ram get-resource-shares \
    --resource-owner SELF
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/2ebe77d7-4156-4a93-87a4-228568d04425",
            "name": "MySubnetShare",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-10T15:38:54.449000-07:00",
            "lastUpdatedTime": "2021-09-10T15:38:54.449000-07:00",
            "featureSet": "STANDARD"
        },
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/818d71dd-7512-4f71-99c6-2ae57aa010bc",
            "name": "MyLicenseConfigShare",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-14T20:42:40.266000-07:00",
            "lastUpdatedTime": "2021-09-14T20:42:40.266000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
```

Crear un recurso compartido en AWS RAM

Para compartir recursos de su propiedad, debe crear un recurso compartido. A continuación se ofrece información general sobre el proceso:

1. Añada los recursos que desea compartir.
2. Para cada tipo de recurso que incluya en el recurso compartido, especifique el permiso administrado que se debe utilizar para dicho tipo de recurso.
   - Puede elegir uno de los permisos administrados de AWS disponibles, un permiso administrado por el cliente existente, o bien crear un nuevo permiso administrado por el cliente.
   - AWS crea permisos administrados de AWS para cubrir los casos de uso más habituales.
   - Los permisos administrados por el cliente le permiten personalizar sus propios permisos administrados para adaptarlos a sus necesidades empresariales y de seguridad.

   > **Note**
   >
   > Si el permiso administrado seleccionado tiene varias versiones, AWS RAM adjunta automáticamente la versión predeterminada. Solo es posible adjuntar la versión designada como predeterminada.

3. Especifique las entidades principales que desea que tengan acceso a los recursos.

Consideraciones

- Si más adelante necesita eliminar un recurso de AWS que haya incluido en un recurso compartido, le recomendamos que elimine primero el recurso de cualquier recurso compartido que lo incluya, o bien que elimine el recurso compartido en su totalidad.
- Puede ver una lista de los tipos de recursos que se pueden incluir en un recurso compartido en Recursos que se pueden compartir AWS.
- Solo puede compartir los recursos que sean de su propiedad. No puede compartir recursos que se hayan compartido con usted.
- AWS RAM es un servicio regional. Al compartir un recurso con entidades principales de otras Cuentas de AWS, dichas entidades principales deben acceder a cada recurso desde la misma Región de AWS en la que se creó. En el caso de los recursos globales compatibles, puede acceder a dichos recursos desde cualquier Región de AWS que sea compatible con la consola de servicio y las herramientas del recurso. Puede ver tales recursos compartidos y sus recursos

globales en la consola y en las herramientas de AWS RAM únicamente en la región de origen designada, Este de EE. UU. (Norte de Virginia), `us-east-1`. Para obtener más información sobre AWS RAM y los recursos globales, consulte Compartir recursos regionales frente a recursos globales.

- Si la cuenta desde la que comparte forma parte de una organización de AWS Organizations y el uso compartido está habilitado dentro de la organización, todas las entidades principales de la organización con las que comparte obtienen automáticamente acceso a los recursos compartidos, sin necesidad de usar invitaciones. Una entidad principal de una cuenta con la que comparte fuera del contexto de una organización recibe una invitación para unirse al recurso compartido y solo obtiene acceso a los recursos compartidos tras aceptar la invitación.
- Si comparte con una entidad principal de servicio, no podrá asociar ninguna otra entidad principal al recurso compartido.
- Si el uso compartido es entre cuentas o entidades principales que forman parte de una organización, cualquier cambio en la pertenencia a la organización afectará de manera dinámica al acceso al recurso compartido.
  - Si añade una Cuenta de AWS a la organización o una OU que tenga acceso a un recurso compartido, la nueva cuenta de miembro obtiene acceso al recurso compartido automáticamente. El administrador de la cuenta con la que ha compartido puede entonces conceder a determinadas entidades principales de dicha cuenta acceso a los recursos del ese recurso compartido.
  - Si elimina una cuenta de la organización o una OU que tenga acceso a un recurso compartido, las entidades principales de dicha cuenta pierden automáticamente el acceso a los recursos a los que se accedía a través del recurso compartido.
  - Si ha compartido directamente con una cuenta de miembro o con roles o usuarios de IAM de la cuenta de miembro y, a continuación, la elimina de la organización, las entidades principales de esa cuenta pierden el acceso a los recursos a los que se accedía a través del recurso compartido.

> **Important**
>
> Cuando comparte con una organización o OU, y ese ámbito incluye la cuenta propietaria del recurso compartido, todas las entidades principales de la cuenta compartida automáticamente obtienen acceso a los recursos del recurso compartido. El acceso concedido viene definido por los permisos administrados asociados al recurso compartido. Esto se debe a que la política basada en recursos que AWS RAM adjunta a cada recurso

del recurso compartido utiliza `"Principal": "*"`. Para obtener más información, consulte Implicaciones del uso de "Principal": "*" en una política basada en recursos. Las entidades principales de las demás cuentas consumidoras no obtienen acceso a los recursos del recurso compartido de inmediato. Los administradores de las demás cuentas primero deben adjuntar políticas de permisos basados en identidad a las entidades principales correspondientes. Tales políticas deben conceder acceso `Allow` a los ARN de los recursos individuales del recurso compartido. Los permisos de dichas políticas no pueden superar los especificados en el permiso administrado asociado al recurso compartido.

- Solo puede añadir la organización a la que pertenece su cuenta y las OU de dicha organización a sus recursos compartidos. No puede añadir como entidades principales a un recurso compartido OU ni organizaciones que no pertenezcan a su propia organización. Sin embargo, sí puede añadir Cuentas de AWS individuales o, en el caso de los servicios compatibles, roles y usuarios de IAM de fuera de la organización como entidades principales a un recurso compartido.

> **Note**
>
> No todos los tipos de recursos se pueden compartir con roles y los usuarios de IAM. Para obtener información sobre los recursos que puede compartir con estas entidades principales, consulte Recursos que se pueden compartir AWS.

- Para los siguientes tipos de recursos, dispone de siete días para aceptar la invitación a unirse al recurso compartido para los siguientes tipos de recursos. Si no acepta la invitación antes de que caduque, esta se rechazará automáticamente.

> **Important**
>
> En el caso de los tipos de recursos compartidos que no figuran en la lista siguiente, dispone de 12 horas para aceptar la invitación a unirse al recurso compartido. Transcurridas 12 horas, la invitación caduca y se elimina la asociación de la entidad principal de usuario final del recurso compartido. Los usuarios finales ya no pueden aceptar la invitación.

  - Amazon Aurora: clústeres de base de datos (DB)
  - Amazon EC2: reservas de capacidad y hosts dedicados

- AWS License Manager: configuraciones de licencias
- AWS Outposts: tablas de enrutamiento de puerta de enlace, outposts y sitios
- Amazon Route 53: reglas de reenvío
- Amazon VPC: direcciones IPv4 propiedad del cliente, listas de prefijos, subredes, destinos de reflejo de tráfico, puertas de enlace de tránsito, dominios de multidifusión de puerta de enlace de tránsito

Console

Para crear un recurso compartido

1. Abra la consola de AWS RAM.
2. Puesto que los recursos compartidos de AWS RAM son específicos de las diferentes Regiones de AWS, elija la Región de AWS que corresponda en la lista desplegable de la esquina superior derecha de la consola. Para ver los recursos compartidos que contienen recursos globales, debe definir la Región de AWS como Este de EE. UU. (Norte de Virginia), (`us-east-1`). Para obtener más información sobre cómo compartir recursos globales, consulte Compartir recursos regionales frente a recursos globales. Si desea incluir recursos globales en el recurso compartido, debe elegir la región de origen designada, Este de EE. UU. (Norte de Virginia),`us-east-1`.
3. Si es la primera vez que utiliza AWS RAM, elija Crear un recurso compartido desde la página de inicio. De lo contrario, elija Crear recurso compartido en la página Compartidos por mí: recursos compartidos.
4. En Paso 1: Especifique los detalles del recurso compartido, haga lo siguiente:
   a. En Nombre, introduzca un nombre descriptivo para el recurso compartido.
   b. En Recursos, elija los recursos que desea añadir al recurso compartido de la siguiente manera:
      - En Seleccionar tipo de recurso, elija el tipo de recurso que desea compartir. Esta acción filtra la lista de recursos que se pueden compartir y muestra solo los recursos del tipo seleccionado.
      - En la lista de recursos resultante, seleccione las casillas de verificación situadas junto a los recursos individuales que desee compartir. Los recursos seleccionados se mueven a Recursos seleccionados.

Si va a compartir recursos asociados a una zona de disponibilidad concreta, usar el ID de zona de disponibilidad (ID de AZ) le ayudará a determinar la ubicación relativa de los recursos en las distintas cuentas. Para obtener más información, consulte ID de zona de disponibilidad para sus recursos de AWS.

c. (Opcional) Para adjuntar etiquetas al recurso compartido, en Etiquetas, introduzca una clave y un valor de etiqueta. Para añadir otras, elija Añadir nueva etiqueta. Repita este paso tantas veces como sea necesario. Estas etiquetas se aplican únicamente al recurso compartido propiamente dicho, no a los recursos que este contiene.

5. Elija Siguiente.

6. En Paso 2: Asociar un permiso administrado a cada tipo de recurso, puede optar por asociar un permiso administrado creado por AWS al tipo de recurso, elegir un permiso administrado por el cliente existente o crear su propio permiso administrado por el cliente para los tipos de recursos compatibles. Para obtener más información, consulte Tipos de permisos administrados.

   Elija Crear permiso administrado por el cliente para crear un permiso administrado por el cliente que cumpla los requisitos de su caso de uso compartido. Para obtener más información consulte () Crear un permiso administrado por el cliente. Una vez que haya completado el proceso, elija

   y, a continuación, podrá seleccionar el nuevo permiso administrado por el cliente en la lista desplegable Permisos administrados.

   > **Note**
   >
   > Si el permiso administrado seleccionado tiene varias versiones, AWS RAM adjunta automáticamente la versión predeterminada. Solo es posible adjuntar la versión designada como predeterminada.

   Para mostrar las acciones que permite el permiso administrado, expanda Ver la plantilla de política de este permiso administrado.

7. Elija Siguiente.

8. En Paso 3: Otorgar acceso a entidades principales, haga lo siguiente:

a. De manera predeterminada, está seleccionada la opción Permitir compartir con cualquiera, lo que significa que, en el caso de los tipos de recursos que lo admiten, puede compartir recursos con Cuentas de AWS externas a la organización. Esto no afecta a los tipos de recursos que solo se pueden compartir dentro de una organización, como las subredes de Amazon VPC. También puede compartir algunos tipos de recursos compatibles con roles y usuarios de IAM.

   Para restringir la capacidad de compartir recursos solo a las cuentas y entidades principales de su organización, elija Permitir compartir solo dentro de la organización.

b. En Entidades principales, haga lo siguiente:

   - Para añadir la organización, una unidad organizativa (OU) o una Cuenta de AWS que forme parte de una organización, active Mostrar estructura organizativa. Se muestra una vista en árbol de la organización. A continuación, seleccione la casilla de verificación situada junto a cada entidad principal que desee añadir.

     > **Important**
     >
     > Cuando comparte con una organización o OU, y ese ámbito incluye la cuenta propietaria del recurso compartido, todas las entidades principales de la cuenta compartida automáticamente obtienen acceso a los recursos del recurso compartido. El acceso concedido viene definido por los permisos administrados asociados al recurso compartido. Esto se debe a que la política basada en recursos que AWS RAM adjunta a cada recurso del recurso compartido utiliza `"Principal": "*"`. Para obtener más información, consulte Implicaciones del uso de "Principal": "*" en una política basada en recursos.
     >
     > Las entidades principales de las demás cuentas consumidoras no obtienen acceso a los recursos del recurso compartido de inmediato. Los administradores de las demás cuentas primero deben adjuntar políticas de permisos basados en identidad a las entidades principales correspondientes. Tales políticas deben conceder acceso `Allow` a los ARN de los recursos individuales del recurso compartido. Los permisos de dichas políticas no pueden superar los especificados en el permiso administrado asociado al recurso compartido.

- Si selecciona la organización (el ID comienza por `o-`), las entidades principales de todas las Cuentas de AWS de la organización podrán acceder al recurso compartido.
- Si selecciona una OU (el ID comienza por `ou-`), las entidades principales de todas las Cuentas de AWS de dicha unidad organizativa y sus unidades organizativas secundarias podrán acceder al recurso compartido.
- Si selecciona una Cuenta de AWS individual, solo las entidades principales de dicha cuenta podrán acceder al recurso compartido.

> **Note**
>
> La opción Mostrar estructura organizativa aparece solo si la opción de compartir con AWS Organizations está habilitada y si se ha iniciado sesión en la cuenta de administración de la organización.
> No puede usar este método para especificar una Cuenta de AWS externa a la organización o un rol o usuario de IAM. En su lugar, debe desactivar la opción Mostrar estructura organizativa y usar la lista desplegable y el cuadro de texto para introducir el ID o el ARN.

- Para especificar una entidad principal mediante el ID o el ARN, incluidos las entidades principales externas a la organización, seleccione el tipo de entidad principal en cada caso. A continuación, introduzca el ID (si se trata de una Cuenta de AWS, una organización o una OU) o el ARN (si se trata de un rol o un usuario de IAM) y, a continuación, elija Añadir. Los tipos de entidades principales y los formatos de ID y ARN disponibles son los siguientes:
  - Cuenta de AWS: para añadir una Cuenta de AWS, introduzca el ID de 12 dígitos de la cuenta. Por ejemplo:

    ```
    123456789012
    ```

  - Organización: para añadir todas las Cuentas de AWS de la organización, introduzca el ID de la organización. Por ejemplo:

    ```
    o-abcd1234
    ```

  - Unidad organizativa (OU): para añadir una OU, introduzca el ID de la OU. Por ejemplo:

`ou-abcd-1234efgh`

- Rol de IAM: para añadir un rol de IAM, introduzca el ARN del rol. Utilice la siguiente sintaxis:

  `arn:partition:iam::account:role/role-name`

  Por ejemplo:

  `arn:aws:iam::123456789012:role/MyS3AccessRole`

  > **Note**
  >
  > Para obtener el ARN único de un rol de IAM, consulte la lista de roles en la consola de IAM y utilice el comando get-role de la AWS CLI o la acción GetRole de la API.

- Usuario de IAM: para añadir un usuario de IAM, introduzca el ARN del usuario. Utilice la siguiente sintaxis:

  `arn:partition:iam::account:user/user-name`

  Por ejemplo:

  `arn:aws:iam::123456789012:user/bob`

  > **Note**
  >
  > Para obtener el ARN único de un usuario de IAM, consulte la lista de usuarios en la consola de IAM y utilice el comando get-user de la AWS CLI o la acción GetUser de la API.

- Entidad principal de servicio: para añadir una entidad principal de servicio, elija Entidad principal de servicio en el cuadro desplegable Seleccionar tipo de entidad principal. Introduzca el nombre de la entidad principal de servicio de AWS. Utilice la siguiente sintaxis:
  - `service-id.amazonaws.com`

Por ejemplo:

```
pca-connector-ad.amazonaws.com
```

c. En Entidades principales seleccionadas, compruebe que las entidades principales que ha especificado figuran en la lista.

9. Elija Siguiente.
10. En Paso 4: Revisión y creación, revise los detalles de configuración del recurso compartido. Para cambiar la configuración de cualquier paso, elija el enlace correspondiente al paso al que desea volver y realice los cambios necesarios.
11. Cuando haya terminado de revisar el recurso compartido, elija Crear recurso compartido.

    La asociación del recurso y la entidad principal puede tardar unos minutos en completarse. Espere a que finalice el proceso antes de intentar utilizar el recurso compartido.
12. Puede añadir y eliminar recursos y entidades principales, o aplicar etiquetas personalizadas al recurso compartido en cualquier momento. Puede cambiar el permiso administrado de los tipos de recursos que se incluyen en el recurso compartido para aquellos tipos que admitan más permisos que el permiso administrado predeterminado. Puede eliminar el recurso compartido cuando ya no desee compartir los recursos. Para obtener más información, consulte Compartir AWS recursos de su propiedad.

AWS CLI

Para crear un recurso compartido

Utilice el comando create-resource-share. El siguiente comando crea un recurso compartido que se comparte con todas las Cuentas de AWS de la organización. El recurso compartido contiene una configuración de licencia de AWS License Manager y concede los permisos administrados predeterminados para ese tipo de recurso.

> **Note**
>
> Si desea usar un permiso administrado por el cliente con un tipo de recurso en este recurso compartido, puede usar uno existente o crear uno nuevo. Anote el ARN del permiso administrado por el cliente y, a continuación, cree el recurso compartido. Para obtener más información, consulte Crear un permiso administrado por el cliente.

```
$ aws ram create-resource-share \
    --region us-east-1 \
    --name MyLicenseConfigShare \
    --permission-arns arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionLicenseConfiguration \
    --resource-arns arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-abc123 \
    --principals arn:aws:organizations::123456789012:organization/o-1234abcd
{
    "resourceShare": {
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
        "name": "MyLicenseConfigShare",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": true,
        "status": "ACTIVE",
        "creationTime": "2021-09-14T20:42:40.266000-07:00",
        "lastUpdatedTime": "2021-09-14T20:42:40.266000-07:00"
    }
}
```

Actualizar un recurso compartido en AWS RAM

Puede actualizar un recurso compartido en AWS RAM en cualquier momento de las siguientes maneras:

- Puede añadir entidades principales, recursos o etiquetas a un recurso compartido que haya creado.
- En el caso de los tipos de recursos que admiten más permisos que el permiso administrado predeterminado de AWS, puede elegir qué permiso administrado se aplica a los recursos de cada tipo.
- Cuando un permiso administrado adjunto al recurso compartido tiene una nueva versión predeterminada, puede actualizar el permiso administrado para que utilice la nueva versión.
- Puede revocar el acceso a los recursos compartidos eliminando entidades principales o recursos de un recurso compartido. Si revoca el acceso, las entidades principales ya no tendrán acceso a los recursos compartidos.

> **Note**
>
> Las entidades principales con las que comparte recursos pueden abandonar su recurso compartido si este está vacío o contiene solo tipos de recursos que permiten abandonar un recurso compartido. Si el recurso compartido contiene tipos de recursos que no admiten el abandono, aparece un mensaje que informa a las entidades principales que deben ponerse en contacto con el propietario del recurso compartido. En este caso, usted, como propietario del recurso compartido, debe eliminar las entidades principales del recurso compartido. Para obtener una lista de los tipos de recursos que no admiten esta acción, consulte Requisitos previos para abandonar un recurso compartido.

Console

Para actualizar un recurso compartido

1. Vaya a la página Compartidos por mí: recursos compartidos de la consola de AWS RAM.
2. Puesto que los recursos compartidos de AWS RAM son específicos de las diferentes Regiones de AWS, elija la Región de AWS que corresponda en la lista desplegable de la esquina superior derecha de la consola. Para ver los recursos compartidos que contienen recursos globales, debe definir la Región de AWS como Este de EE. UU. (Norte de Virginia), (`us-east-1`). Para obtener información sobre cómo compartir recursos globales, consulte Compartir recursos regionales frente a recursos globales.
3. Seleccione el recurso compartido y, a continuación, elija Modificar.
4. En Paso 1: Especifique los detalles del recurso compartido, revise los detalles del recurso compartido y, si es necesario, actualice cualquiera de los siguientes elementos:

   a. (Opcional) Para cambiar el nombre del recurso compartido, edite el Nombre.

   b. (Opcional) Para añadir un recurso al recurso compartido, en Recursos, seleccione el tipo de recurso y, a continuación, active la casilla de verificación situada junto a él para añadirlo al recurso compartido. Los recursos globales aparecen solo si configura la región como Este de EE. UU. (Norte de Virginia), (`us-east-1`) en la Consola de administración de AWS.

   c. (Opcional) Para eliminar un recurso del recurso compartido, localice el recurso en Recursos seleccionados y, a continuación, pulse la X situada junto al ID del recurso.

d. (Opcional) Para añadir una etiqueta al recurso compartido, en Etiquetas, ingrese una clave y un valor de etiqueta en los cuadros de texto vacíos. Para añadir más de un par de clave y valor de etiqueta, elija Añadir nueva etiqueta. Puede añadir hasta 50 etiquetas.

e. Para eliminar una etiqueta del recurso compartido, en Etiquetas, localice la etiqueta y elija la opción Eliminar que aparece junto a ella.

5. Elija Siguiente.

6. (Opcional) En Paso 2: Asociar un permiso administrado a cada tipo de recurso, puede optar por asociar un permiso administrado creado por AWS al tipo de recurso, elegir un permiso administrado por el cliente existente o crear su propio permiso administrado por el cliente. Para obtener más información, consulte Tipos de permisos administrados.

   También puede elegir Crear permiso administrado por el cliente para crear un permiso administrado por el cliente que cumpla los requisitos de su caso de uso compartido. Para obtener más información, consulte Crear un permiso administrado por el cliente. Una vez que haya completado el proceso, elija

   y, a continuación, podrá seleccionar el nuevo permiso administrado por el cliente en la lista desplegable Permiso administrado.

   Para que se muestren las acciones que permite el permiso administrado, expanda Ver la plantilla de política de este permiso administrado.

7. Si la versión del permiso administrado actualmente asignada al recurso compartido no es la versión predeterminada actual, puede actualizar a la versión predeterminada seleccionando Actualizar a la versión predeterminada.

   > **Note**
   >
   > Hasta que guarde los cambios en el recurso compartido después del último paso, puede cancelar la actualización de la versión seleccionando Restablecer la versión anterior. Sin embargo, en el caso de los permisos administrados de AWS, una vez guardado el recurso compartido, el cambio será definitivo y ya no podrá volver a la versión anterior.

8. Elija Siguiente.

9. En Paso 3: Elija las entidades principales a las que se permite el acceso, revise las entidades principales seleccionadas y, si es necesario, actualice cualquiera de los elementos siguientes:

   a. (Opcional) Para cambiar si la opción de compartir está habilitada con las entidades principales internas o externas a la organización, elija una de las siguientes opciones:

      - Para compartir recursos con roles o usuarios individuales de Cuentas de AWS externos a la organización, seleccione Permitir compartir con entidades principales externas.
      - Para restringir la capacidad de compartir recursos solo a las entidades principales de su organización en AWS Organizations, elija Permitir compartir solo dentro de la organización.

   b. En Entidades principales, haga lo siguiente:

      - (Opcional) Para añadir una organización, una unidad organizativa (OU) o una Cuenta de AWS miembro de su organización, active Mostrar estructura organizativa para que se muestre una vista de árbol de la organización. A continuación, seleccione la casilla de verificación situada junto a cada entidad principal que desee añadir.

        > **Important**
        >
        > Cuando comparte con una organización o OU, y ese ámbito incluye la cuenta propietaria del recurso compartido, todas las entidades principales de la cuenta compartida automáticamente obtienen acceso a los recursos del recurso compartido. El acceso concedido viene definido por los permisos administrados asociados al recurso compartido. Esto se debe a que la política basada en recursos que AWS RAM adjunta a cada recurso del recurso compartido utiliza `"Principal": "*"`. Para obtener más información, consulte Implicaciones del uso de "Principal": "*" en una política basada en recursos.
        >
        > Las entidades principales de las demás cuentas consumidoras no obtienen acceso a los recursos del recurso compartido de inmediato. Los administradores de las demás cuentas primero deben adjuntar políticas de permisos basados en identidad a las entidades principales correspondientes. Tales políticas deben conceder acceso `Allow` a los ARN de los recursos individuales del recurso compartido. Los permisos de dichas políticas no

pueden superar los especificados en el permiso administrado asociado al recurso compartido.

> **Note**
>
> La opción Mostrar estructura organizativa aparece solo si la opción de compartir con AWS Organizations está habilitada y si se ha iniciado sesión como entidad principal en la cuenta de administración de la organización. No puede usar este método para especificar una Cuenta de AWS externa a la organización o un rol o usuario de IAM. En su lugar, debe añadir estas entidades principales introduciendo sus identificadores, que se muestran en el cuadro de texto situado debajo del conmutador Mostrar estructura organizativa. Consulte el punto siguiente.

- (Opcional) Para añadir una entidad principal por su identificador, elija el tipo de entidad principal en la lista desplegable y, a continuación, introduzca el ID o el ARN de la entidad principal. Por último, seleccione Añadir.

  Si selecciona una Cuenta de AWS individual, solo dicha cuenta podrá acceder al recurso compartido. Puede elegir cualquiera de las opciones siguientes.

  - Otra Cuenta de AWS (distinta del propietario del recurso): hace que el recurso esté disponible para la otra cuenta. El administrador de esa cuenta debe completar el proceso concediendo acceso al recurso compartido a roles y usuarios individuales mediante políticas de permisos basadas en la identidad. Esos permisos no pueden superar los definidos en los permisos administrados adjuntos al recurso compartido.
  - Esta Cuenta de AWS (propietario del recurso): todos los roles y usuarios de la cuenta propietaria del recurso reciben automáticamente el acceso definido por los permisos administrados adjunto al recurso compartido.
- La adición aparece de inmediato en la lista Entidades principales seleccionadas.

  A continuación, puede añadir otras cuentas, unidades organizativas o la organización repitiendo este paso.
- (Opcional) Para eliminar una entidad principal, localícela en Entidades principales seleccionadas, seleccione la casilla de verificación que le corresponda y elija Anular selección.

10. Elija Siguiente.
11. En Paso 4: Revisión y actualización, revise los detalles de configuración del recurso compartido.
12. Para cambiar la configuración de cualquier paso, elija el enlace correspondiente al paso al que desea volver y haga los cambios necesarios.

    Si algún permiso administrado sigue utilizando versiones distintas de la predeterminada, tiene otra oportunidad de solucionarlo seleccionando Actualizar a la versión predeterminada.
13. Cuando haya terminado de hacer cambios, elija Actualizar recurso compartido.

AWS CLI

Para actualizar un recurso compartido

Puede usar los siguientes comandos de la AWS CLI para modificar un recurso compartido:

- Para cambiar el nombre de un recurso compartido o si se permiten las entidades principales externas, utilice el comando update-resource-share. En el siguiente ejemplo, se cambia el nombre del recurso compartido especificado y se configura el recurso para que solo permita las entidades principales de su organización. Debe usar el punto de conexión del servicio para la Región de AWS que contiene el recurso compartido.

```
$ aws ram update-resource-share \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE \
    --name "my-renamed-resource-share" \
    --no-allow-external-principals
{
    "resourceShare": {
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
        "name": "my-renamed-resource-share",
        "owningAccountId": "123456789012",
        "allowExternalPrincipals": false,
        "status": "ACTIVE",
        "creationTime": 1565295733.282,
        "lastUpdatedTime": 1565303080.023
    }
}
```

- Para añadir un recurso a un recurso compartido, utilice el comando associate-resource-share. En el siguiente ejemplo, se añade una subred al recurso compartido especificado.

```
$ aws ram associate-resource-share \
    --region us-east-1 \
    --resource-arns arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE
{
    "resourceShareAssociations": [
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
        "associatedEntity": "arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235",
        "associationType": "RESOURCE",
        "status": "ASSOCIATING",
        "external": false
    ]
}
```

- Para añadir o reemplazar un permiso administrado para un tipo de recurso en un recurso compartido, use los comandos list-permissions y associate-resource-share-permission. Puede asignar un solo permiso administrado por tipo de recurso de un recurso compartido. Si intenta añadir un permiso administrado a un tipo de recurso que ya tiene un permiso administrado, debe incluir la opción `--replace` o el comando fallará y se producirá un error.

  El siguiente comando de ejemplo muestra los ARN de los permisos administrados disponibles para una subred de Amazon Elastic Compute Cloud (Amazon EC2) y, a continuación, usa uno de esos ARN para reemplazar el permiso administrado de AWS actualmente asignado a ese tipo de recurso en el recurso compartido especificado.

```
$ aws ram list-permissions \
    --resource-type ec2:Subnet
{
    "permissions": [
        {
            "arn": "arn:aws:ram::aws:permission/AWSRAMDefaultPermissionSubnet",
            "version": "1",
            "defaultVersion": true,
            "name": "AWSRAMDefaultPermissionSubnet",
            "resourceType": "ec2:Subnet",
```

```
            "creationTime": "2020-02-27T11:38:26.727000-08:00",
            "lastUpdatedTime": "2020-02-27T11:38:26.727000-08:00"
        }
    ]
}
$ aws ram associate-resource-share-permission \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
    --permission-arn arn:aws:ram::aws:permission/AWSRAMDefaultPermissionSubnet
{
    "returnValue": true
}
```

- Para eliminar un recurso de un recurso compartido, use el comando disassociate-resource-share. El siguiente ejemplo elimina la subred Amazon EC2 con el ARN especificado del recurso compartido especificado.

```
$ aws ram disassociate-resource-share \
    --region us-east-1 \
    --resource-arns arn:aws:ec2:us-east-1:123456789012:subnet/
subnet-0250c25a1f4e15235 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE
{
    "resourceShareAssociations": [
        "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/7ab63972-b505-7e2a-420d-6f5d3EXAMPLE",
        "associatedEntity": "arn:aws:ec2:us-east-1:ubnet/
subnet-0250c25a1f4e15235",
        "associationType": "RESOURCE",
        "status": "DISASSOCIATING",
        "external": false
    ]
}
```

- Para modificar las etiquetas adjuntas a un recurso compartido, use los comandos tag-resource y untag-resource. En el siguiente ejemplo, se añade la etiqueta `project=lima` al recurso compartido especificado.

```
$ aws ram tag-resource \
    --region us-east-1 \
```

```
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
    --tags key=project,value=lima
```

En el siguiente ejemplo, se elimina la etiqueta con una clave `project` de del recurso compartido especificado.

```
$ aws ram untag-resource \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-share/
f1d72a60-da19-4765-b4f9-e27b658b15b8 \
    --tag-keys=project
```

Los comandos de etiquetado no generan ningún resultado si se ejecutan correctamente.

Ver los recursos compartidos en AWS RAM

Puede ver la lista de recursos individuales que ha compartido del conjunto de recursos compartidos. La lista lo ayuda a determinar qué recursos está compartiendo actualmente, el número de recursos compartidos de los proceden y el número de entidades principales que tienen acceso a ellos.

Console

Para ver los recursos que está compartiendo actualmente

1. Abra la página Compartidos por mí: recursos compartidos en la consola de AWS RAM .
2. Como AWS RAM los recursos compartidos existen de forma específica Regiones de AWS, elige el recurso correspondiente Región de AWS en la lista desplegable situada en la esquina superior derecha de la consola. Para ver los recursos compartidos que contienen recursos globales, debe establecer en EE.UU. Este (Norte de Virginia), (). Región de AWS `us-east-1` Para obtener información sobre cómo compartir recursos globales, consulte Compartir recursos regionales frente a recursos globales.
3. Se muestra la siguiente información para cada recurso compartido:

   - ID de recurso: el identificador del recurso. Elija el ID de un recurso para abrir una nueva pestaña del navegador y ver el recurso en su consola de servicio nativa.
   - Tipo de recurso: el tipo de recurso.
   - Compartido por última vez: la fecha en la que se compartió el recurso por última vez.

- Recursos compartidos: el número de recursos compartidos que incluyen el recurso. Para ver la lista de recursos compartidos, elija el número.
- Entidades principales: el número de entidades principales que pueden acceder al recurso. Elija el valor para ver las entidades principales.

AWS CLI

Para ver los recursos que está compartiendo actualmente

Puede usar el comando list-resources con el parámetro `--resource-owner` definido como `SELF` para que se muestren los detalles de los recursos que comparte actualmente.

En el siguiente ejemplo, se muestran los recursos que están incluidos en los recursos compartidos de la Región de AWS (`us-east-1`) para la Cuenta de AWS que realiza la llamada. Para obtener los recursos que comparte en otra región, use el parámetro `--region` *<region-code>*.

```
$ aws ram list-resources \
    --region us-east-1 \
    --resource-owner SELF
{
    "resources": [
        {
            "arn": "arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-ecbd5574fd92cb0d312baea260e4cece",
            "type": "license-manager:LicenseConfiguration",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/818d71dd-7512-4f71-99c6-2ae57aa010bc",
            "creationTime": "2021-09-14T20:42:40.266000-07:00",
            "lastUpdatedTime": "2021-09-14T20:42:41.081000-07:00"
        },
        {
            "arn": "arn:aws:license-manager:us-east-1:123456789012:license-
configuration:lic-ecbd5574fd92cb0d312baea260e4cece",
            "type": "license-manager:LicenseConfiguration",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-share/
a477f3b2-4001-4dcb-bd54-7c8d23b4f07d",
            "creationTime": "2021-07-22T11:48:11.104000-07:00",
            "lastUpdatedTime": "2021-07-22T11:48:11.971000-07:00"
        }
    ]
```

```
}
```

Ver los directores con los que compartes recursos en AWS RAM

Puede ver las entidades principales con las que comparte recursos de su propiedad en todos los recursos compartidos. Ver esta lista de entidades principales le ayuda a determinar quién tiene acceso a sus recursos compartidos.

Console

Para ver las entidades principales con las que comparte recursos

1. Vaya a la página Compartidos por mí: entidades principales en la consola de AWS RAM .
2. Como AWS RAM los recursos compartidos existen de forma específica Regiones de AWS, elige el recurso correspondiente Región de AWS en la lista desplegable situada en la esquina superior derecha de la consola. Para ver los recursos compartidos que contienen recursos globales, debe establecer en EE.UU. Este (Norte de Virginia), (). Región de AWS `us-east-1` Para obtener más información sobre cómo compartir recursos globales, consulte Compartir recursos regionales frente a recursos globales.
3. Para buscar entidades principales concretas, ayúdese de los filtros. Puede aplicar varios filtros para delimitar en mayor medida la búsqueda. Resalte el cuadro de texto para ver una lista desplegable de campos de atributo sugeridos. Una vez que elija uno, podrá elegir de la lista de valores disponibles para dicho campo. Puede añadir otros atributos o palabras clave hasta encontrar el recurso que busca.
4. La consola muestra la siguiente información para cada entidad principal de la lista:
   - ID de entidad principal: el identificador de la entidad principal. Elija el ID para abrir una nueva pestaña del navegador y ver la entidad principal en su consola nativa.
   - Recursos compartidos: el número de recursos compartidos que ha compartido con la entidad principal especificada. Pulse en el número para ver la lista de recursos compartidos.
   - Recursos: el número de recursos que ha compartido con la entidad principal. Pulse en el número para ver la lista de recursos compartidos.

AWS CLI

Para ver las entidades principales con las que comparte recursos

Puede usar el comando list-principals para obtener una lista de los principales a los que hace referencia en los recursos compartidos que creó en la cuenta actual Región de AWS para la cuenta llamante.

En el siguiente ejemplo, se enumeran las entidades principales que tienen acceso a los recursos compartidos creados en la región predeterminada para la cuenta de llamada. En este ejemplo, los principales son la organización de la cuenta llamante y un recurso compartido independiente Cuenta de AWS, que forma parte de dos recursos diferentes. Debe usar el punto final del servicio Región de AWS que contiene el recurso compartido.

```
$ aws ram list-principals \
    --region us-east-1 \
    --resource-owner SELF
{
    "principals": [
        {
            "id": "arn:aws:organizations::123456789012:organization/o-a1b2c3dr",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-share/
a477f3b2-4001-4dcb-bd54-7c8d23b4f07d",
            "creationTime": "2021-09-14T20:40:58.532000-07:00",
            "lastUpdatedTime": "2021-09-14T20:40:59.610000-07:00",
            "external": false
        },
        {
            "id": "111111111111",
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/6405fa7c-0786-4e15-8c9f-8aec02802f18",
            "creationTime": "2021-09-15T15:00:31.601000-07:00",
            "lastUpdatedTime": "2021-09-15T15:14:13.618000-07:00",
            "external": true
        }
    ]
}
```

Eliminar un recurso compartido en AWS RAM

Puede eliminar un recurso compartido en cualquier momento. Cuando se elimina un recurso compartido, todas las entidades principales que estaban asociadas al recurso compartido pierden el acceso a los recursos compartidos. La eliminación de un recurso compartido no implica la eliminación de los recursos compartidos individuales que este contiene.

> **Para eliminar un AWS recurso**
>
> Si necesita eliminar un AWS recurso que ha incluido en un recurso compartido, le AWS recomienda que primero se asegure de eliminar el recurso de cualquier recurso compartido que lo incluya o de eliminar el recurso compartido.

El recurso compartido eliminado permanece visible en la AWS RAM consola durante un breve período después de la eliminación, pero su estado cambia a`Deleted`.

Console

Para eliminar un recurso compartido

1. Abra la página Compartidos por mí: recursos compartidos en la consola de AWS RAM .
2. Como AWS RAM los recursos compartidos existen de forma específica Regiones de AWS, elija el recurso correspondiente Región de AWS en la lista desplegable situada en la esquina superior derecha de la consola. Para ver los recursos compartidos que contienen recursos globales, debe establecer en EE.UU. Este (Norte de Virginia), (). Región de AWS `us-east-1` Para obtener más información sobre cómo compartir recursos globales, consulte Compartir recursos regionales frente a recursos globales.
3. Seleccione los recursos compartidos que desea eliminar.

   > **Warning**
   >
   > Asegúrese de seleccionar el recurso compartido correcto. Una vez que lo elimine, no podrá recuperarlo.

4. Elija Eliminar y, en el mensaje de confirmación, elija nuevamente Eliminar.
5. El recurso compartido eliminado desaparece pasadas dos horas. Hasta entonces, permanece visible en la consola con el estado eliminado.

AWS CLI

Para eliminar un recurso compartido

Puede usar el delete-resource-sharecomando para eliminar un recurso compartido que ya no necesite.

En el siguiente ejemplo, primero se utiliza el get-resource-sharescomando para obtener el nombre de recurso de Amazon (ARN) del recurso compartido que se desea eliminar. A continuación, se utiliza delete-resource-sharepara eliminar el recurso compartido especificado.

```
$  aws ram get-resource-shares \
    --region us-east-1 \
    --resource-owner SELF
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:123456789012:resource-
share/2ebe77d7-4156-4a93-87a4-228568d04425",
            "name": "MySubnetShare",
            "owningAccountId": "123456789012",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-10T15:38:54.449000-07:00",
            "lastUpdatedTime": "2021-09-10T15:38:54.449000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
$ aws ram delete-resource-share \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:123456789012:resource-
share/2ebe77d7-4156-4a93-87a4-228568d04425
{
    "returnValue": true
}
```

Acceder a los recursos de AWS compartidos con usted

AWS Resource Access Manager (AWS RAM) le permite ver los recursos compartidos a los que se le ha añadido, los recursos compartidos a los que puede acceder y las cuentas de Cuentas de

AWS que tienen recursos compartidos con usted. También puede abandonar un recurso compartido cuando ya no necesite acceder a su contenido.

Contenido

Aceptar y rechazar invitaciones a recursos compartidos

Para acceder a un recurso compartido, el propietario del recurso compartido debe añadirle como entidad principal. El propietario puede añadir a cualquiera de los siguientes como entidad principal al recurso compartido.

- La organización a la que pertenece su cuenta
- Una unidad organizativa (OU) que contenga su cuenta
- Su cuenta individual
- En el caso de los tipos de recursos compatibles, su rol o usuario específicos de IAM

Si se le agrega al recurso compartido a través de un miembro de una organización y está habilitado el uso compartido dentro de la organización, obtendrá acceso automáticamente a los recursos compartidos sin tener que aceptar una invitación. Cuenta de AWS AWS Organizations Las entidades principales de servicio también tienen acceso automático a los recursos compartidos sin aceptar una invitación. Si la cuenta a través de la cual recibe acceso se elimina posteriormente de la organización, todas las entidades principales de dicha cuenta pierden automáticamente el acceso a los recursos a los que accedía a través de dicho recurso compartido.

Si se le añade a un recurso compartido a través de uno de los siguientes, recibirá una invitación para unirse al recurso compartido:

- Una cuenta ajena a tu organización en AWS Organizations
- Una cuenta de tu organización con la que no AWS Organizations está habilitada la función de compartir

Si recibe una invitación para unirse a un recurso compartido, debe aceptarla para obtener acceso a los recursos compartidos que este contiene. Si rechaza la invitación, no podrá acceder a los recursos compartidos.

Para los siguientes tipos de recursos, dispone de siete días para aceptar la invitación a unirse al recurso compartido para los siguientes tipos de recursos. Si no acepta la invitación antes de que caduque, esta se rechazará automáticamente.

> **Important**
>
> En el caso de los tipos de recursos compartidos que no figuran en la lista siguiente, dispone de 12 horas para aceptar la invitación a unirse al recurso compartido. Transcurridas 12 horas, la invitación caduca y se elimina la asociación de la entidad principal de usuario final del recurso compartido. Los usuarios finales ya no pueden aceptar la invitación.

- Amazon Aurora: clústeres de base de datos (DB)
- Amazon EC2: reservas de capacidad y hosts dedicados
- AWS License Manager — Configuraciones de licencia
- AWS Outposts — Tablas de rutas, puestos de avanzada y sitios de las pasarelas de enlace locales
- Amazon Route 53: reglas de reenvío
- Amazon VPC: IPv4 direcciones propiedad de los clientes, listas de prefijos, subredes, objetivos de espejo de tráfico, pasarelas de tránsito, dominios de multidifusión de pasarelas de tránsito

Console

Para responder a una invitación a un recurso compartido

1. Ve a la página Compartido conmigo: recursos compartidos en la consola. AWS RAM
2. Como AWS RAM los recursos compartidos existen de forma específica Regiones de AWS, elige el recurso correspondiente Región de AWS en la lista desplegable situada en la esquina superior derecha de la consola. Para ver los recursos compartidos que contienen recursos globales, debe establecer en EE.UU. Este (Norte de Virginia), (). Región de AWS `us-east-1` Para obtener más información sobre cómo compartir recursos globales, consulte Compartir recursos regionales frente a recursos globales.
3. Revise la lista de recursos compartidos a los que se le ha añadido.

La columna Estado indica su estado de participación actual en el recurso compartido. El estado `Pending` indica que se le ha añadido a un recurso compartido, pero que aún no ha aceptado o rechazado la invitación.

4. Para responder a la invitación al recurso compartido, seleccione el ID del recurso compartido y elija Aceptar recurso compartido para aceptar la invitación, o Rechazar recurso compartido para rechazarla. Si rechaza la invitación, no obtendrá acceso a los recursos. Si acepta la invitación, obtendrá acceso a los recursos.

AWS CLI

Para responder a una invitación a un recurso compartido

Puede usar los siguientes comandos para aceptar o rechazar invitaciones a un recurso compartido:

- get-resource-share-invitations
- accept-resource-share-invitation
- reject-resource-share-invitation

1. El siguiente ejemplo comienza con el get-resource-share-invitationscomando para recuperar una lista de todas las invitaciones disponibles para el usuario Cuenta de AWS. El AWS CLI `query` parámetro permite restringir la salida únicamente a las invitaciones que tengan el valor `status` establecido en`PENDING`. Este ejemplo muestra que existe una invitación de la cuenta `111111111111` aún `PENDING` para la cuenta `123456789012` de la Región de AWS especificada.

```
$ aws ram get-resource-share-invitations \
    --region us-east-1 \
    --query 'resourceShareInvitations[?status==`PENDING`]'
{
    "resourceShareInvitations": [
        {
            "resourceShareInvitationArn": "arn:aws:ram:us-
east-1:111111111111:resource-share-invitation/3b3bc051-
fbf6-4336-8377-06c559dfee49",
            "resourceShareName": "Test TrngAcct Resource Share",
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/c4506c70-df75-4e6c-ac30-42ca03295a37",
```

```
            "senderAccountId": "111111111111",
            "receiverAccountId": "123456789012",
            "invitationTimestamp": "2021-09-21T08:56:24.977000-07:00",
            "status": "PENDING"
        }
    ]
}
```

2. Una vez que encuentre la invitación que desea aceptar, anote el `resourceShareInvitationArn` que aparece en el resultado para usarlo en el siguiente comando para aceptar la invitación.

```
$ aws ram accept-resource-share-invitation \
    --region us-east-1 \
    --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/3b3bc051-fbf6-4336-8377-06c559dfee49
{
    "resourceShareInvitation": {
        "resourceShareInvitationArn": "arn:aws:ram:us-
east-1:111111111111:resource-share-invitation/3b3bc051-
fbf6-4336-8377-06c559dfee49",
        "resourceShareName": "Test TrngAcct Resource Share",
        "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-share/
c4506c70-df75-4e6c-ac30-42ca03295a37",
        "senderAccountId": "111111111111",
        "receiverAccountId": "123456789012",
        "invitationTimestamp": "2021-09-21T09:18:24.545000-07:00",
        "status": "ACCEPTED"
    }
}
```

   Si se realiza correctamente, la respuesta muestra que el `status` ha cambiado de `PENDING` a `ACCEPTED`.

Si, por el contrario, desea rechazar la invitación, ejecute el reject-resource-share-invitationcomando con los mismos parámetros.

```
$ aws ram reject-resource-share-invitation \
    --region us-east-1 \
    --resource-share-invitation-arn arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/3b3bc051-fbf6-4336-8377-06c559dfee49
```

```
{
    "resourceShareInvitation": {
        "resourceShareInvitationArn": "arn:aws:ram:us-east-1:111111111111:resource-
share-invitation/3b3bc051-fbf6-4336-8377-06c559dfee49",
        "resourceShareName": "Test TrngAcct Resource Share",
        "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-share/
c4506c70-df75-4e6c-ac30-42ca03295a37",
        "senderAccountId": "111111111111",
        "receiverAccountId": "123456789012",
        "invitationTimestamp": "2021-09-21T09:18:24.545000-07:00",
        "status": "REJECTED"
    }
}
```

Ver los recursos compartidos que se comparten con usted

Puede ver los recursos compartidos a los que tiene acceso. Puede ver que entidades principales comparten recursos con usted y cuáles son esos recursos.

Console

Para ver los recursos compartidos

1. Vaya a la página Compartidos conmigo: recursos compartidos de la consola de AWS RAM .
2. Dado que AWS RAM los recursos compartidos existen de Regiones de AWS forma específica, elija el correspondiente Región de AWS en la lista desplegable de la esquina superior derecha de la consola. Para ver los recursos compartidos que contienen recursos globales, debe establecer en EE.UU. Este (Norte de Virginia), (). Región de AWS `us-east-1` Para obtener más información sobre cómo compartir recursos globales, consulte Compartir recursos regionales frente a recursos globales.
3. (Opcional) Aplique un filtro si desea buscar recursos compartidos específicos. Puede aplicar varios filtros para delimitar en mayor medida la búsqueda. Puede escribir una palabra clave (por ejemplo, parte del nombre de un recurso compartido) para que se muestren solo los recursos compartidos cuyo nombre incluya el texto especificado. Resalte el cuadro de texto para ver una lista desplegable de campos de atributo sugeridos. Una vez que elija uno, podrá elegir de la lista de valores disponibles para dicho campo. Puede añadir otros atributos o palabras clave hasta que encuentre el recurso que busca.
4. La AWS RAM consola muestra la siguiente información:

- Nombre: el nombre del recurso compartido.
- ID: el ID del recurso compartido. Elija el ID para ver la página de detalles del recurso compartido.
- Propietario: el ID de la Cuenta de AWS que creó el recurso compartido.
- Estado: el estado actual del recurso compartido. Los valores posibles son:
  - `Active`: el recurso compartido está activo y disponible para su uso.
  - `Deleted`: el recurso compartido se ha eliminado y ya no está disponible para su uso.
  - `Pending`: hay una invitación para aceptar el recurso compartido a la espera de una respuesta.

AWS CLI

Para ver los recursos compartidos

Utilice el get-resource-sharescomando con el `--resource-owner` parámetro establecido en`OTHER-ACCOUNTS`.

En el siguiente ejemplo, se muestra la lista de recursos compartidos por otras personas en la cuenta especificada Región de AWS con la cuenta de llamada Cuentas de AWS.

```
$ aws ram get-resource-shares \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "name": "Prod Env Shared Licenses",
            "owningAccountId": "111111111111",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T08:50:41.308000-07:00",
            "featureSet": "STANDARD"
        },
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:222222222222:resource-share/
c4506c70-df75-4e6c-ac30-42ca03295a37",
```

```
            "name": "Prod Env Shared Subnets",
            "owningAccountId": "222222222222",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-21T08:56:24.737000-07:00",
            "lastUpdatedTime": "2021-09-21T08:56:24.737000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
```


Ver los recursos compartidos con usted

Puede ver los recursos compartidos a los que tiene acceso. Puede ver qué entidades principales han compartido los recursos con usted y en qué recursos compartidos están incluidos.

Console

Para ver los recursos compartidos con usted

1. Vaya a la página Compartidos conmigo: recursos compartidos de la consola de AWS RAM.
2. Puesto que los recursos compartidos de AWS RAM son específicos de las diferentes Regiones de AWS, elija la Región de AWS que corresponda en la lista desplegable de la esquina superior derecha de la consola. Para ver los recursos compartidos que contienen recursos globales, debe definir la Región de AWS como Este de EE. UU. (Norte de Virginia), (`us-east-1`). Para obtener más información sobre cómo compartir recursos globales, consulte Compartir recursos regionales frente a recursos globales.
3. Ayúdese de los filtros para buscar recursos compartidos específicos. Puede aplicar varios filtros para delimitar en mayor medida la búsqueda.
4. Está disponible la siguiente información:

   - ID de recurso: el identificador del recurso. Seleccione el ID de recurso para verlo en su servicio.
   - Tipo de recurso: el tipo de recurso.
   - Compartido por última vez: la fecha en la que se compartió el recurso con usted.
   - Recursos compartidos: el número de recursos compartidos en los que está incluido el recurso. Seleccione el valor para ver los recursos compartidos.

- ID del propietario: el identificador de la entidad principal a la que pertenece el recurso.

AWS CLI

Para ver los recursos compartidos con usted

Puede usar el comando list-resources para ver los recursos que se comparten con usted.

El siguiente comando de ejemplo muestra detalles sobre el recurso al que se puede acceder a través de un recurso compartido en la Región de AWS especificada desde otra Cuenta de AWS.

```
$ aws ram list-resources \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "resources": [
        {
            "arn": "arn:aws:license-manager:us-east-1:111111111111:license-
configuration:lic-36be0485f5ae379cc74cf8e9242ab143",
            "type": "license-manager:LicenseConfiguration",
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "status": "AVAILABLE",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T08:50:42.517000-07:00"
        }
    ]
}
```

Ver las entidades principales que comparten recursos con usted

Puede ver una lista de todas las entidades principales que comparten recursos con usted. Puede ver qué recursos y recursos compartidos están compartiendo con usted.

Console

Para ver las entidades principales que comparten recursos con usted

1. Abre la AWS RAM consola en https://console.aws.amazon.com/ram/casa.

2. Como AWS RAM los recursos compartidos existen de forma específica Regiones de AWS, elige el recurso correspondiente Región de AWS en la lista desplegable situada en la esquina superior derecha de la consola. Para ver los recursos compartidos que contienen recursos globales, debe establecer en EE.UU. Este (Norte de Virginia), (). Región de AWS `us-east-1` Para obtener más información sobre cómo compartir recursos globales, consulte Compartir recursos regionales frente a recursos globales.
3. En el panel de navegación, elija Compartidos conmigo, Entidades principales.
4. (Opcional) Puede ayudarse de los filtros para encontrar entidades principales específicas. Puede aplicar varios filtros para delimitar en mayor medida la búsqueda.
5. La consola muestra la siguiente información:

   - ID principal: el identificador de la entidad principal que comparte con usted.
   - Recursos compartidos: el número de recursos compartidos a los que la entidad principal le ha añadido. Pulse en el número para ver la lista de recursos compartidos.
   - Recursos: el número de recursos que la entidad principal comparte con usted. Pulse en el valor para ver la lista de recursos.

AWS CLI

Para ver las entidades principales que comparten recursos con usted

Puede usar el comando list-principals para recuperar la lista de los principales que comparten recursos con el suyo. Cuenta de AWS

El siguiente comando de ejemplo muestra detalles sobre la persona Cuenta de AWS que compartió un recurso compartido con la cuenta utilizada para llamar a la operación en la cuenta especificada. Región de AWS

```
$  aws ram list-principals \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "principals": [
        {
            "id": "111111111111",
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T09:06:25.545000-07:00",
```

```
            "external": true
        }
    ]
}
```

Abandonar un recurso compartido

Si ya no necesita acceder a recursos que se han compartido con usted, puede abandonar un recurso compartido en cualquier momento. Al abandonar un recurso compartido, pierde el acceso a los recursos compartidos que contiene.

Requisitos previos para abandonar un recurso compartido

- Puede abandonar un recurso compartido solo si este se compartió con usted como Cuenta de AWS individual, y no en el contexto de una organización. No puedes abandonar un recurso compartido si alguien de tu organización te ha agregado y AWS Organizations está activado el uso compartido con él. Cuenta de AWS El acceso a los recursos compartidos dentro de una organización es automático.
- Para abandonar un recurso compartido, asegúrese de que el recurso en cuestión está vacío o de que contiene solo los tipos de recursos que permiten abandonar un recurso compartido.

  Los siguientes son los únicos tipos de recursos que permiten abandonar un recurso compartido.

Servicio	Tipo de recurso
Amazon Aurora	`rds:Cluster`
Amazon EC2	`ec2:CapacityReservation` `ec2:DedicatedHost`
AWS License Manager	`license-manager:LicenseConfiguration`

AWS Outposts	`ec2:LocalGatewayRouteTable`
	`outposts:Outpost`
	`outposts:Site`

Servicio	Tipo de recurso
Amazon Route 53	`route53resolver:ResolverRule`

Amazon VPC	`ec2:CoipPool`
	`ec2:PrefixList`
	`ec2:Subnet`
	`ec2:TrafficMirrorTarget`
	`ec2:TransitGateway`
	`ec2:TransitGatewayMulticastDomain`

Cómo abandonar un recurso compartido

Console

Para abandonar un recurso compartido

1. Vaya a la página Compartidos conmigo: recursos compartidos de la consola de AWS RAM .
2. Como AWS RAM los recursos compartidos existen de forma específica Regiones de AWS, elige el recurso correspondiente Región de AWS en la lista desplegable situada en la esquina superior derecha de la consola. Para ver los recursos compartidos que contienen recursos globales, debe establecer en EE.UU. Este (Norte de Virginia), (). Región de AWS `us-east-1` Para obtener más información sobre cómo compartir recursos globales, consulte Compartir recursos regionales frente a recursos globales.
3. Seleccione el recurso compartido que desea abandonar.
4. Seleccione Abandonar recurso compartido y, en el cuadro de diálogo de confirmación, seleccione Abandonar.

AWS CLI

Para abandonar un recurso compartido

Puede usar el disassociate-resource-sharecomando para dejar un recurso compartido.

Los siguientes comandos de ejemplo hacen Cuenta de AWS que el comando que llama al comando pierda el acceso a los recursos compartidos por el recurso compartido especificado por el ARN. Debe dirigir la solicitud al punto de conexión del servicio de la Región de AWS que contiene el recurso compartido que desea abandonar.

1. En primer lugar, recupere la lista de recursos compartidos para recuperar el ARN del recurso compartido que desea abandonar.

```
$ aws ram get-resource-shares \
    --region us-east-1 \
    --resource-owner OTHER-ACCOUNTS
{
    "resourceShares": [
        {
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "name": "Prod Environment Shared Licenses",
            "owningAccountId": "111111111111",
            "allowExternalPrincipals": true,
            "status": "ACTIVE",
            "creationTime": "2021-09-21T08:50:41.308000-07:00",
            "lastUpdatedTime": "2021-09-21T08:50:41.308000-07:00",
            "featureSet": "STANDARD"
        }
    ]
}
```

2. A continuación, puede ejecutar el comando para abandonar ese recurso compartido. Tenga en cuenta que también debe especificar el ID de su cuenta, 123456789012, como entidad principal para desvincularse del recurso compartido especificado, compartido por la cuenta 111111111111.

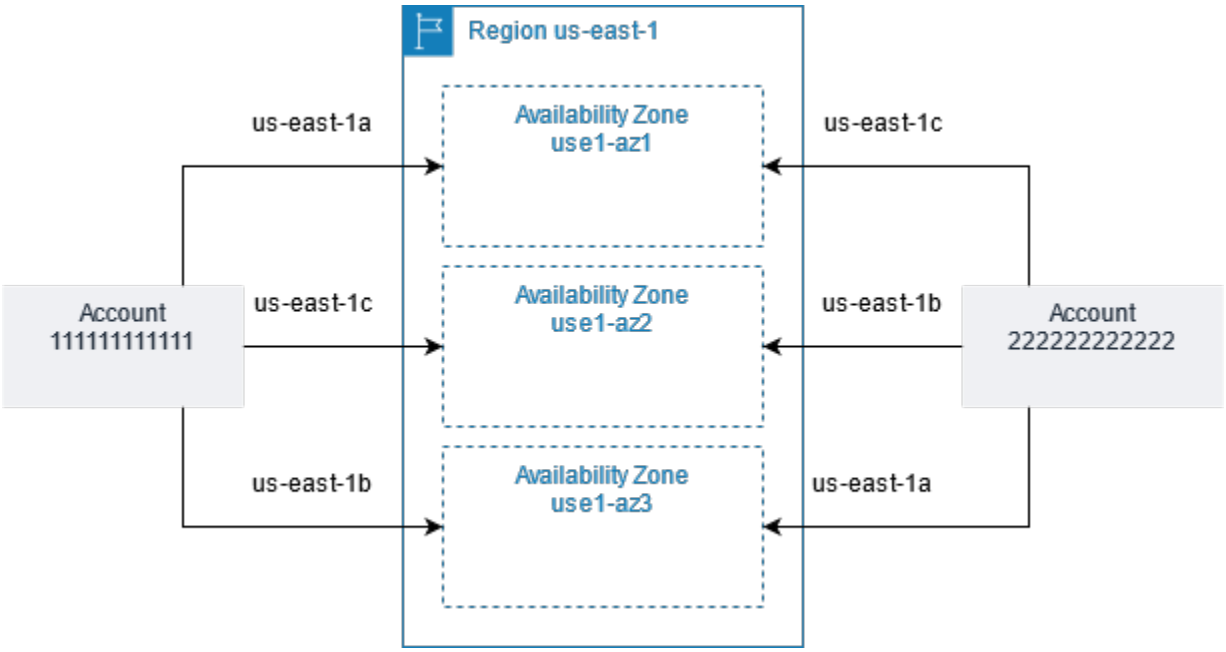
```
$ aws ram disassociate-resource-share \
    --region us-east-1 \
    --resource-share-arn arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e \
    --principals 123456789012
                        {
    "resourceShareAssociations": [
        {
```

```
            "resourceShareArn": "arn:aws:ram:us-east-1:111111111111:resource-
share/8b831ba0-63df-4608-be3c-19096b1ee16e",
            "associatedEntity": "123456789012",
            "associationType": "PRINCIPAL",
            "status": "DISASSOCIATING",
            "external": false
        }
    ]
}
```

ID de zona de disponibilidad para sus recursos de AWS

AWS asigna las zonas de disponibilidad física aleatoriamente a los nombres de las zonas de disponibilidad de cada Cuenta de AWS. Este enfoque facilita la distribución de los recursos entre las zonas de disponibilidad de una Región de AWS, para reducir la probabilidad de que los recursos se concentren en la zona de disponibilidad "a" de cada región. Como resultado, es posible que la zona de disponibilidad `us-east-1a` de su cuenta de AWS no se refiera a la misma ubicación física que la zona `us-east-1a` de otra cuenta de AWS. Para obtener más información, consulte Regiones y zonas de disponibilidad en la Guía del usuario de Amazon EC2.

En la siguiente ilustración, se muestra cómo los ID de zona de disponibilidad son los mismos para todas las cuentas, a pesar de los nombres de las zonas de disponibilidad pueden asignarse de forma diferente para cada cuenta.



En el caso de ciertos recursos, debe identificar no solo la Región de AWS, sino también la zona de disponibilidad. Por ejemplo, una subred de Amazon VPC. Dentro de una misma cuenta, la asignación de una zona de disponibilidad a un determinado nombre no es importante. Sin embargo, cuando se utiliza AWS RAM para compartir un recurso con otras Cuentas de AWS, la asignación sí es importante. Esta asignación aleatoria complica la capacidad de la cuenta de acceder al recurso compartido para saber a qué zona de disponibilidad debe hacer referencia. Para facilitar esta tarea, estos recursos también le permiten identificar la ubicación real de sus recursos respecto de sus cuentas utilizando el ID de AZ. El ID de AZ es un identificador único y coherente que designa a una zona de disponibilidad en todas las Cuentas de AWS. Por ejemplo, `use1-az1` es el ID de AZ de una zona de disponibilidad de la región `us-east-1`, y representa la misma ubicación física en todas las cuentas de AWS.

Puede usar ID de zona de disponibilidad para determinar la ubicación de los recursos de una cuenta respecto de los recursos de otra. Por ejemplo, si comparte una subred en la zona de disponibilidad con el ID de AZ `use1-az2` con otra cuenta, esta subred está disponible para dicha cuenta de la zona de disponibilidad cuyo ID de zona de disponibilidad es también `use1-az2`. El ID de zona de disponibilidad de cada subred se muestra en la consola de Amazon VPC, y se puede consultar con la AWS CLI.

Console

Para ver los ID de AZ de las zonas de disponibilidad de su cuenta

1. Vaya a la página de la consola de AWS RAM en la consola de AWS RAM.
2. Puede ver los ID de AZ de la Región de AWS actual en Su ID de zona de disponibilidad.

AWS CLI

Para ver los ID de AZ de las zonas de disponibilidad de su cuenta

El siguiente comando de ejemplo muestra los ID de AZ de las zonas de disponibilidad de la región Oeste de EE. UU. 2 y cómo estos se asignan para las Cuenta de AWS de llamada.

```
$ aws ec2 describe-availability-zones \
    --region us-west-2
{
    "AvailabilityZones": [
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
```

```
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2a",
            "ZoneId": "usw2-az2",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        },
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2b",
            "ZoneId": "usw2-az1",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        },
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2c",
            "ZoneId": "usw2-az3",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        },
        {
            "State": "available",
            "OptInStatus": "opt-in-not-required",
            "Messages": [],
            "RegionName": "us-west-2",
            "ZoneName": "us-west-2d",
            "ZoneId": "usw2-az4",
            "GroupName": "us-west-2",
            "NetworkBorderGroup": "us-west-2",
            "ZoneType": "availability-zone"
        }
    ]
}
```

Recursos que se pueden compartir AWS

Con AWS Resource Access Manager (AWS RAM), puedes compartir los recursos creados y administrados por otros Servicios de AWS. Puede compartir recursos con personas Cuentas de AWS. También puedes compartir recursos con las cuentas de una organización o unidades organizativas (OUs) de AWS Organizations. Algunos tipos de recursos compatibles también te permiten compartir recursos con funciones y usuarios individuales AWS Identity and Access Management (IAM).

En las siguientes secciones, se enumeran los tipos de recursos, agrupados por Servicio de AWS, que puede compartir mediante el uso AWS RAM. Las columnas de las tablas especifican qué características admite cada tipo de recurso:

Puede compartir con usuarios y roles de IAM	 puede compartir recursos de este tipo con funciones y usuarios individuales AWS Identity and Access Management (IAM), además de con cuentas.  solo puede compartir recursos de este tipo con cuentas.	Sí, No:
Puede compartir con cuentas externas a su organización	 solo puede compartir recursos de este tipo con cuentas individuales, dentro o fuera de la organización. Consulte Consideraciones para obtener más información.	Sí:

	 puede compartir recursos de este tipo solo con cuentas que sean miembros de la misma organización.	No:
Puede usar permisos administrados por el cliente	Todos los tipos de recursos que AWS RAM admiten los permisos AWS administrados son compatibles con los permisos administrados, pero un Sí en esta columna significa que los permisos administrados por el cliente también son compatibles con este tipo de recurso.	
	 los recursos de este tipo admiten el uso de permisos administrados por el cliente.	Sí:
	 los recursos de este tipo no admiten el uso de permisos administrados por el cliente.	No:
Puede compartir con entidades principales de servicio	 puede compartir recursos de este tipo con Servicios de AWS.	Sí:
	 no puede compartir recursos de este tipo con Servicios de AWS.	No:

AWS App Mesh

Puede compartir los siguientes AWS App Mesh recursos mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Mallas `appmesh:Mesh`	Cree y administre una malla de forma centralizada y compártala con otras Cuentas de AWS o con su organización. Una malla compartida permite que los recursos creados por diferentes Cuentas de AWS personas se comuniquen entre sí en la misma malla. Para obtener más información, consulte Usar mallas compartidas en la Guía del usuario de AWS App Mesh .	 S	 S Puede compartir con cualquier Cuenta de AWS.	 N	 No

AWS AppSync API GraphQL

Puedes compartir los siguientes recursos de la API de AWS AppSync GraphQL mediante. AWS RAM

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
AppSync GraphyQL APIs `appsync:Apis`	Gestiona AWS AppSync GraphQL de APIs forma centralizada y compártelos con otras personas Cuentas de AWS o con tu organización. Esto permite que varias cuentas se compartan AWS AppSync APIs como parte de la creación de una API AWS AppSync combinada unificada que puede acceder a los datos de varios subesquemas de APIs diferentes cuentas de la misma región. Para obtener más información, consulta Merged APIs en la Guía para AWS AppSync desarrolladores.	 S	 S Puede compartir con cualquier Cuenta de AWS.	 S	 No

Amazon API Gateway

Puede compartir los siguientes recursos de Amazon API Gateway mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Dominios personalizados privados de API Gateway `apigateway:Domainnames`	Cree y administre nombres de dominio de forma centralizada y compártalos con otras personas Cuentas de AWS o con su organización. Esto permite que varias cuentas invoquen tus nombres de dominio que están mapeados como privados. APIs Para obtener más información, consulte Nombres de dominio personalizados para uso privado APIs en API Gateway en la Guía para desarrolladores de Amazon API Gateway.	 No	 Sí Puede compartir con cualquier Cuenta de AWS.	 No	 No

Controlador de recuperación de aplicaciones (ARC) de Amazon

Puede compartir los siguientes recursos del Controlador de recuperación de aplicaciones de Amazon (ARC) mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Clústeres de Route 53 ARC `route53-recovery-control:Cluster`	Cree y gestione clústeres ARC de forma centralizada y compártalos con otras Cuentas de AWS personas o con su organización. Esto permite que varias cuentas creen paneles de control y controles de enrutamiento en un único clúster compartido, lo que reduce la complejidad y el número total de clústeres que precisa una organización. Para obtener más información, consulte Compartir clústeres entre cuentas en la Guía para desarrolladores del Controlad	 S	 S Puede compartir con cualquier Cuenta de AWS.	 S	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	or de recuperación de aplicaciones de Amazon (ARC).				
Planes de cambio de región de ARC `arc-region-switch:Plan`	Cree y administre planes de forma centralizada y compártalos con otras Cuentas de AWS o con su organización. Esto permite que varias cuentas utilicen recursos de una cuenta distinta de la que aloja el plan. Para obtener más información, consulte Cambio de región en la Guía para desarrolladores del Controlador de recuperación de aplicaciones de Amazon (ARC).	S	S Puede compartir con cualquier Cuenta de AWS.	S	No

Amazon Aurora

Puede compartir los siguientes recursos de Amazon Aurora utilizando AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Clústeres de base de datos de Aurora `rds:Cluster`	Cree y gestione un clúster de base de datos de forma centralizada y compártalo con otras Cuentas de AWS o con su organización. Esto permite a varias Cuentas de AWS clonar un clúster de base de datos compartido y administrado de forma centralizada. Para obtener más información, consulte Clonación multicuenta con AWS RAM Amazon Aurora en la Guía del usuario de Amazon Aurora.	N	S Puede compartir con cualquier Cuenta de AWS.	N	No

AWS Backup

Puede compartir los siguientes AWS Backup recursos utilizando. AWS RAM

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Almacenes de copias de seguridad `backup:BackupVault`	Cree y gestione de forma centralizada bóvedas aisladas de forma lógica y compártalas con otras personas o con su organización. Cuentas de AWS Esta opción permite a varias cuentas acceder a las copias de seguridad de los almacenes y restaurarlas. Para obtener más información, consulte Información general de los almacenes aislados lógicamente en la Guía para desarrolladores de AWS Backup .	S	S Puede compartir con cualquier Cuenta de AWS.	S	No

Amazon Bedrock

Puede compartir los siguientes recursos de Amazon Bedrock mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Modelo personalizado de Bedrock `bedrock:CustomModel`	Cree y administre un modelo personalizado de forma centralizada y compártalo con otras Cuentas de AWS o con su organización. Esto permite que varias cuentas utilicen el mismo modelo personalizado para las aplicaciones de IA generativa. Para obtener más información, consulte Cómo compartir un modelo para que lo use otra cuenta en la Guía del usuario de Amazon Bedrock.	S	N Puede compartir solo con Cuentas de AWS de su propia organización.	S	No

Administración de facturación y costos

Puede compartir los siguientes recursos de Administración de facturación y costos mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Paneles de Administración de facturación y costos `bcm-dashboards:dashboard`	Cree y administre paneles de Administración de facturación y costos y compártalos con otras Cuentas de AWS o fuera de su organización. Cuando se comparte un panel, solo se comparten las configuraciones del panel, no los datos subyacentes. Los destinatarios tienen acceso al diseño del panel y a las configuraciones de los widgets, y verán los datos en función de sus propios permisos de acceso. El uso compartido permite a las organizaciones establecer prácticas comunes de presentación de informes de costos y ayuda a los diferentes equipos a ver los datos de costos	N	S Puede compartir con cualquier Cuenta de AWS.	S	No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	de manera coherente. Para obtener más información, consulte Uso compartido de paneles en la Guía del usuario de Administración de facturación y costos.				

AWS Billing Ver servicio

Puede compartir los siguientes recursos de AWS Billing View Service mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Vistas de facturación `billing:billingview`	Cree y administre vistas de facturación personalizadas de forma centralizada y compártalas	N	N	S	No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	con otras personas Cuentas de AWS o con su organización. Esto permite a los propietarios de aplicaciones y unidades de negocio acceder a los gastos de AWS a nivel de unidad de negocio desde una cuenta de miembro. Para obtener más información, consulte Uso compartido de vistas de facturación personalizadas en la Guía del usuario de AWS Cost Management .		Puede compartir solo con Cuentas de AWS de su propia organización.		

AWS Cloud Map

Puede compartir los siguientes AWS Cloud Map recursos mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
AWS Cloud Map Espacios de nombres `servicediscovery:Namespace`	Cree y administre espacios de nombres de forma centralizada y compártalos con Cuentas de AWS en su organización. Esto permite que varias Cuentas de AWS descubran servicios e instancias en el espacio de nombres compartido sin necesidad de credenciales temporales. Para obtener más información, consulte Espacios de nombres de AWS Cloud Map compartidos en la Guía para desarrolladores de AWS Cloud Map .	 S	 N Puede compartir solo con Cuentas de AWS de su propia organización.	 S	 No

AWS WAN en la nube

Puedes compartir los siguientes recursos de AWS Cloud WAN mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Redes principales `networkmanager:CoreNetwork`	Crea y administra una red principal de Cloud WAN de forma centralizada y compártela con otros usuarios Cuentas de AWS. Esto permite el Cuentas de AWS acceso múltiple y el aprovisionamiento de hosts en una única red central de Cloud WAN. Para obtener más información, consulte Compartir una red central en la Guía del usuario de WAN en la nube de AWS .	S	S Puede compartir con cualquier Cuenta de AWS.	N	No

Amazon CloudFront

Puedes compartir los siguientes CloudFront recursos de Amazon utilizando AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Amazon CloudFront VpcOrigin `cloudfront:VpcOrigin`	Cree y gestione los orígenes de las CloudFront VPC de forma centralizada y compártalas con otras personas Cuentas de AWS o con su organización. Esto permite Cuentas de AWS utilizar varios orígenes de VPC compartidos para CloudFront distribuciones. Para obtener más información, consulte Trabajar con recursos compartidos CloudFront en la Guía para CloudFront desarrolladores de Amazon.	N	S Puede compartir con cualquier Cuenta de AWS.	N	No

AWS CloudHSM

Puede compartir los siguientes AWS CloudHSM recursos utilizando AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
AWS CloudHSM Respaldos `cloudhsm:Backup`	Gestione AWS CloudHSM las copias de seguridad de forma centralizada y compártalas con otras Cuentas de AWS personas o con su organización. Esto permite a varios Cuentas de AWS usuarios ver información sobre el Backup y utilizarla para restaurar un AWS CloudHSM clúster. Para obtener más información, consulte Administración de copias de seguridad de AWS CloudHSM en la Guía del usuario de AWS CloudHSM .	S	S	S	No

AWS CodeBuild

Puede compartir los siguientes AWS CodeBuild recursos mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
CodeBuild Proyectos `codebuild:Project`	Cree un proyecto y utilícelo para ejecutar compilaciones. Comparta el proyecto con otras personas Cuentas de AWS o con su organización. Esto permite que varias Cuentas de AWS y usuarios vean información sobre un proyecto y analicen sus compilaciones. Para obtener más información, consulte Uso de proyectos compartidos en la Guía del usuario de AWS CodeBuild .	S	S Puede compartir con cualquier Cuenta de AWS.	S	No
CodeBuild Denuncie grupos `codebuild:ReportGroup`	Cree un grupo de informes y utilícelo para crear informes a la hora de compilar un proyecto. Comparta el grupo de informes con otras personas Cuentas de AWS	S	S Puede compartir con cualquier	S	No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	o con su organización. Esto permite a varios Cuentas de AWS usuarios ver el grupo de informes y sus informes, así como los resultados de los casos de prueba de cada informe. Un informe se puede ver durante los 30 días siguientes a su creación. Pasado este periodo, caduca y deja de estar visible. Para obtener más información, consulte Uso de proyectos compartidos en la Guía del usuario de AWS CodeBuild .		Cuenta de AWS.		

AWS CodeConnections

Puede compartir los siguientes CodeConnections recursos mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Conexiones de código `codeconnections:Connection`	Administre la reutilización de las conexiones de código en varias cuentas. Es decir, al compartir conexiones de código, se reduce la carga de trabajo del administrador y la necesidad de acceso de administrador en todas las cuentas que requieren una conexión de código. Para obtener más información, consulte Compartir conexiones con Cuentas de AWS en la Guía del usuario de la consola de herramientas para desarrolladores.	N	S Puede compartir con cualquier Cuenta de AWS.	S	No

Amazon DataZone

Puede compartir los siguientes DataZone recursos utilizando AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
DataZone Dominios `datazone:Domain`	Cree y administre dominios de forma centralizada y compártalos con otras Cuentas de AWS o con su organización. Esto permite que varias cuentas creen DataZone dominios de Amazon. Para obtener más información, consulta Qué es Amazon DataZone en la Guía del DataZone usuario de Amazon.	N	S Puede compartir con cualquier Cuenta de AWS.	N	No

Amazon EC2

Puede compartir los siguientes recursos de Amazon EC2 utilizando AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Reservas de capacidad `ec2:CapacityReservation`	Cree y gestione las reservas de capacidad de forma centralizada y comparta la capacidad reservada con otras personas Cuentas de AWS o con su organización. Esto permite Cuentas de AWS lanzar varias instancias de Amazon EC2 en una capacidad reservada gestionada de forma centralizada. Para obtener más información, consulte Trabajar con Reservas de capacidad compartidas en la Guía del usuario de Amazon EC2. Comparta los bloques de capacidad para el aprendizaje automático (aún no UltraServer CBs se admiten)	N	Sí, para reservas de capacidad (se puede compartir con cualquier persona Cuenta de AWS). No para los bloques de capacidad (solo se pueden compartir con los Cuentas de AWS miembros de su propia	N	No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	con otras personas Cuentas de AWS o con su organización. Esta capacidad permite que las cargas de trabajo que se ejecutan en diferentes Cuentas de AWS ubicaciones puedan lanzar instancias de Amazon EC2 en bloques de capacidad propios, lo que le ayuda a utilizar mejor la capacidad reservada y a ahorrar costes. Para obtener más información, consulte Trabajar con bloques de capacidad compartidos en la Guía del usuario de Amazon EC2. **Important** Si no cumple todos los requisitos		organización).		

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	previos para compartir una reserva de capacidad, podría producirse un error al compartir. Si esto ocurre y un usuario intenta lanzar una instancia de Amazon EC2 en esa reserva de capacidad, esta se lanza como una instancia bajo demanda, lo que puede generar un mayor costo. Le recomendamos que compruebe que puede acceder a la reserva de capacidad				

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	compartida intentando visualizarla en la consola de Amazon EC2. También puede monitorizar los recursos compartidos con error para poder adoptar medidas correctivas antes de que los usuarios lancen las instancias de forma que aumenten sus costos. Para obtener más información, consulte Ejemplo: Alertar de errores en un recurso compartido.				

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Hosts dedicados `ec2:DedicatedHost`	Asigne y gestione los hosts dedicados de Amazon EC2 de forma centralizada y comparta la capacidad de instancias del host con otras personas Cuentas de AWS o con su organización. Esto permite Cuentas de AWS lanzar varias instancias de Amazon EC2 en hosts dedicados gestionados de forma centralizada. Para obtener más información, consulte Trabajar con hosts dedicados compartidos en la Guía del usuario de Amazon EC2.	 N	 S Puede compartir con cualquier Cuenta de AWS.	 N	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Grupos de ubicación `ec2:PlacementGroup`	Comparta los grupos de ubicación de los que dispone en toda su organización Cuentas de AWS, tanto dentro como fuera de ella. Puede lanzar instancias de Amazon EC2 desde cualquiera de las cuentas con las que comparte en un grupo de ubicación compartido. Para obtener más información, consulte Compartir un grupo con ubicación en la Guía del usuario de Amazon EC2.	 S	 S Puede compartir con cualquier Cuenta de AWS.	 N	 No

Generador de Imágenes de EC2

Puede compartir los siguientes recursos de Generador de imágenes de Amazon EC2 utilizando AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Componentes de Generador de imágenes `imagebuilder:Component`	Cree y administre grupos de componentes de forma centralizada y, compártalos con otras Cuentas de AWS o con su organización. Administre quién puede usar componentes predefinidos de compilación y prueba en sus recetas de imagen. Para obtener más información, consulte Compartir recursos del Generador de imágenes de EC2 en la Guía del usuario de Generador de imágenes de EC2.	 S	 S Puede compartir con cualquier Cuenta de AWS.	 S	 No
Recetas de contenedor de Generador de Imágenes `imagebuilder:ContainerRecipe`	Cree y gestione sus recetas en contenedores de forma centralizada y compártalas con otras personas Cuentas de AWS o con su organizac	 S	 S Puede compartir con cualquier	 S	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	ión. Esto le permite administrar quién puede usar documentos predefinidos para duplicar compilaciones de imágenes de contenedores. Para obtener más información, consulte Compartir recursos del Generador de imágenes de EC2 en la Guía del usuario del Generador de imágenes de EC2.		Cuenta de AWS.		

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Imágenes de Generador de imágenes `imagebuilder:Image`	Cree y gestione sus imágenes doradas de forma centralizada y compártalas con otras personas Cuentas de AWS o con su organización. Administre quién puede usar imágenes creadas con Generador de imágenes de EC2 en toda su organización. Para obtener más información, consulte Compartir recursos del Generador de imágenes de EC2 en la Guía del usuario del Generador de imágenes de EC2.	 S	 S Puede compartir con cualquier Cuenta de AWS.	 S	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Recetas de imágenes de Generador de Imágenes `imagebuilder:ImageRecipe`	Cree y gestione sus recetas de imágenes de forma centralizada y compártalas con otras personas Cuentas de AWS o con su organización. Esto le permite administrar quién puede usar documentos predefinidos para duplicar compilaciones de AMI. Para obtener más información, consulte Compartir recursos del Generador de imágenes de EC2 en la Guía del usuario del Generador de imágenes de EC2.	 S	 S Puede compartir con cualquier Cuenta de AWS.	 S	 No

Elastic Load Balancing

Puede compartir los siguientes recursos de Elastic Load Balancing mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Almacenes de confianza de ELB `elasticloadbalancing:TrustStore`	Cree y administre almacenes fiduciarios de Elastic Load Balancing de forma centralizada y compártalos con otras Cuentas de AWS personas o con su organización. Los administradores de seguridad pueden mantener un solo almacén de confianza, o un número reducido de ellos, y habilitar las configuraciones de TLS mutuas en los equilibradores de carga de aplicaciones. Para obtener información, consulte Cómo compartir el almacén de confianza de Elastic Load Balancing para los Equilibradores de carga de aplicación en la Guía del usuario para	 S	 S	 N	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	equilibradores de carga de aplicaciones.				

AWS End User Messaging SMS

Puede compartir el siguiente AWS End User Messaging SMS recurso mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
AWS SMS Listas de exclusión por voz `sms-voice:OptOutList`	Cree una lista de exclusión y compártala con otras Cuentas de AWS personas de su organización. Puede compartir la lista de exclusión para que las demás aplicaciones puedan excluir los números de teléfono del usuario procedent	N	S Puede compartir con cualquier Cuenta de AWS.	S	No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	es de otras Cuentas de AWS o para que puedan comprobar el estado del número de teléfono del usuario. Para obtener más información, consulte Trabajar con recursos compartidos en la Guía AWS End User Messaging SMS del usuario.				

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
AWS SMS Números de teléfono de voz `sms-voice:PhoneNumber`	Cree y administre números de teléfono para compartirlos con otras Cuentas de AWS o con su organización. Esto permite a varias Cuentas de AWS enviar mensajes utilizando el número de teléfono compartido. Para obtener más información, consulte Trabajar con recursos compartidos en la Guía AWS End User Messaging SMS del usuario.	 N	 S Puede compartir con cualquier Cuenta de AWS.	 S	 Sí

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
AWS SMS Grupo de voces `sms-voice:Pool`	Cree y administre grupos para compartir los con otras personas Cuentas de AWS o con su organización. Esto permite Cuentas de AWS enviar varios mensajes mediante el grupo compartido. Para obtener más información, consulte Trabajar con recursos compartidos en la Guía AWS End User Messaging SMS del usuario.	 N	 S Puede compartir con cualquier Cuenta de AWS.	 S	 Sí

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
AWS SMS Remitente de voz IDs `sms-voice:SenderId`	Crea y administra remitentes IDs y compártelos con otras personas Cuentas de AWS o con tu organización. Esto permite a varias Cuentas de AWS enviar mensajes mediante el identificador de remitente compartido. Para obtener más información, consulte Trabajar con recursos compartidos en la Guía AWS End User Messaging SMS del usuario.	 N	 S Puede compartir con cualquier Cuenta de AWS.	 S	 Sí

Amazon FSx para OpenZFS

Puede compartir los siguientes recursos de Amazon FSx for OpenZFS mediante. AWS RAM

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
FSx Volúmenes `fsx:Volume`	Cree y gestione FSx los volúmenes de OpenZFS de forma centralizada y compártalos con otras personas Cuentas de AWS o con su organización. Esto permite a varias cuentas realizar la replicación de datos mediante OpenZfs instantáneas en volúmenes compartidos mediante o. FSx APIs `CreateVolume` `CopySnapshotAndUpdateVolume` Para obtener más información, consulte Replicación de datos bajo demanda en la Guía del usuario de Amazon FSx for OpenZFS.	 S	 S Puede compartir con cualquier Cuenta de AWS.	 S	 No

AWS Glue

Puede compartir los siguientes AWS Glue recursos utilizando. AWS RAM

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
AWS Glue Catálogo `glue:Catalog`	Administre un catálogo de datos central y comparta metadatos sobre bases de datos y tablas con Cuentas de AWS su organización. Esto permite a los usuarios realizar consultas sobre datos de varias cuentas. Para obtener más información, consulte Uso compartido de tablas y bases de datos del catálogo de datos entre cuentas AWS en la Guía del desarrollador de AWS Lake Formation .	 N	 S Puede compartir con cualquier Cuenta de AWS.	 N	 No
AWS Glue bases de datos	Cree y administre bases de datos de catálogos de datos de forma centralizada	 N	 S	 N	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
`glue:Database`	y Cuentas de AWS compártalas con su organización. Las bases de datos son recopilaciones de tablas de catálogos de datos. Esto permite a los usuarios ejecutar consultas y trabajos de extracción, transformación y carga (ETL) que pueden combinar y consultar datos en varias cuentas. Para obtener más información, consulte Uso compartido de tablas y bases de datos del catálogo de datos entre cuentas AWS en la Guía del desarrollador de AWS Lake Formation .		Puede compartir con cualquier Cuenta de AWS.		

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
AWS Glue Tablas `glue:Table`	Cree y gestione las tablas del catálogo de datos de forma centralizada y compártalas con Cuentas de AWS su organización. Las tablas del catálogo de datos contienen metadatos relativos a tablas de datos de Amazon S3, orígenes de datos de JDBC, Amazon Redshift, fuentes de transmisión y otros almacenes de datos. Esto permite a los usuarios ejecutar consultas y trabajos ETL para combinar y consultar datos de varias cuentas. Para obtener más información, consulte Uso compartido de tablas y bases de datos del catálogo de datos entre cuentas de AWS en	 N	 S Puede compartir con cualquier Cuenta de AWS.	 N	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	la Guía del desarrollador de AWS Lake Formation .				

AWS License Manager

Puede compartir los siguientes AWS License Manager recursos mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Configuraciones de licencias `license-manager:LicenseConfiguration`	Cree y gestione las configuraciones de licencias de forma centralizada y compártalas con otras Cuentas de AWS personas o con su organización. Esto le permite aplicar reglas de licencias administr	N	S Puede compartir con cualquier Cuenta de AWS.	N	No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	adas de forma centralizada basándose en los términos de sus contratos empresariales entre varias Cuentas de AWS. Para obtener más información, consulte Configuraciones de licencias en License Manager en la Guía del usuario de License Manager.				

AWS Marketplace

Puede compartir los siguientes AWS Marketplace recursos mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Entidades de catálogo de Marketplace `aws-marketplace:Entity`	Cree, administre y comparta entidades en su organización Cuentas de AWS o dentro de ella en AWS Marketplace. Para obtener más información, consulte Compartir recursos en AWS RAM en la Referencia de AWS Marketplace Catalog API .	S	S Puede compartir con cualquier Cuenta de AWS.	N	No

AWS Migration Hub Refactor Spaces

Puede compartir los siguientes AWS Migration Hub Refactor Spaces recursos mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Entorno de Refactor Spaces `refactor-spaces:Environment`	Cree un entorno de Refactor Spaces y utilícelo para contener sus aplicaciones de Refactor Spaces. Comparta el entorno con otras Cuentas de AWS o con todas las cuentas de su organización. Esto permite a varios Cuentas de AWS usuarios ver información sobre el entorno y las aplicaciones que contiene. Para obtener más información, consulte Compartir entornos de Refactor Spaces con AWS RAM en la Guía del usuario de AWS Migration Hub Refactor Spaces .	 S	 S Puede compartir con cualquier Cuenta de AWS.	 S	 No

Aprobación multipartita

Puede compartir los siguientes recursos de aprobación de varias partes mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Equipo de aprobación de varias partes `mpa:ApprovalTeam`	Cree y administre equipos de aprobación y compártalos con otras Cuentas de AWS o con su organización. Esto permite a otras Cuentas de AWS utilizar un equipo de aprobación asociado con una operación protegida. Una operación protegida es una lista predefinida de operaciones que requieren la aprobación del equipo para poder ejecutarse. Para obtener más información, consulte Términos y conceptos en la Guía del usuario de la aprobación de varias partes.	 S	 S Puede compartir con cualquier Cuenta de AWS.	 S	 No

AWS Network Firewall

Puede compartir los siguientes AWS Network Firewall recursos mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Firewalls de red `network-firewall:Firewall`	Cree y administre firewalls de forma centralizada y compártalos con otras Cuentas de AWS para que puedan crear puntos de conexión de firewall. Esto permite que varias cuentas utilicen las protecciones de un único firewall. Para obtener más información, consulte Compartir AWS Network Firewall recursos en la Guía para AWS Network Firewall desarrolladores.	 S	 S Puede compartir con cualquier Cuenta de AWS.	 N	 No
Políticas de firewalls de red	Cree y gestione políticas de firewall de forma centraliz ada y compártalas	 S	 S	 N	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
`network-firewall:FirewallPolicy`	con otras Cuentas de AWS personas o con su organización. Esto permite que varias cuentas de una organización compartan un conjunto común de comportamientos de monitorización, protección y filtrado de la red. Para obtener más información, consulte Compartir AWS Network Firewall recursos en la Guía para AWS Network Firewall desarrolladores.		Puede compartir con cualquier Cuenta de AWS.		

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio

Grupos de reglas de firewalls de red
 	
`network-firewall:StatefulRuleGroup`
 	
`network-firewall:StatelessRuleGroup`
	Cree y gestione grupos de reglas sin estado y con estado de forma centralizada y compártalos con otras personas Cuentas de AWS o con su organización. Esto permite que varias cuentas de una organización compartan un conjunto de criterios para inspeccionar y gestionar el tráfico de la red. AWS Organizations Para obtener más información, consulte Compartir AWS Network Firewall recursos en la Guía para AWS Network Firewall desarrolladores.	 S	 S
			
			Puede compartir con cualquier Cuenta de AWS.
				 N	 No

Oracle Database@AWS

Puede compartir los siguientes Oracle Database@AWS recursos mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Oracle Database@AWS Infraestructura de Exadata `odb:CloudExadataInfrastructure`	Con ella Oracle Database@AWS, puede compartir su infraestructura de Exadata y su red ODB entre varias Cuentas de AWS unidades de la misma organización. AWS Podrá aprovisionar la infraestructura una sola vez y reutilizarla en cuentas de confianza, lo que le permite reducir los costos y separar las responsabilidades. Para obtener más información, consulte Uso compartido de recursos Oracle Database@AWS en la Guía del Oracle Database@AWS usuario.	N	N Puede compartir solo con Cuentas de AWS de su propia organización.	N	No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Oracle Database@AWS Red ODB `odb:OdbNetwork`	Con ella Oracle Database@AWS, puede compartir su infraestructura de Exadata y su red ODB entre varias Cuentas de AWS unidades de la misma organización. AWS Podrá aprovisionar la infraestructura una sola vez y reutilizarla en cuentas de confianza, lo que le permite reducir los costos y separar las responsabilidades. Para obtener más información, consulte Uso compartido de recursos Oracle Database@AWS en la Guía del Oracle Database@AWS usuario.	 N	 N Puede compartir solo con Cuentas de AWS de su propia organización.	 N	 No

AWS Outposts

Puede compartir los siguientes AWS Outposts recursos mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Outposts `outposts:Outpost`	Cree y administre Outposts de forma centralizada, y compártalos con otras Cuentas de AWS de su organización. Esto permite que varias cuentas creen subredes y volúmenes de EBS en sus Outposts compartidos y administrados de forma centralizada. Para obtener más información, consulta Cómo trabajar con recursos compartidos de AWS Outposts en la Guía del AWS Outposts usuario.	 N	 N Puede compartir solo con Cuentas de AWS de su propia organización.	 S	 No
Tabla de enrutamiento de la puerta de enlace local	Cree y gestione asociaciones de VPC a una puerta de enlace local de forma centraliz	 N	 N	 N	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
`ec2:LocalGatewayRouteTable`	ada y compártalas con otros miembros de su Cuentas de AWS organización. Esto permite a varias cuentas crear asociaciones de VPC con una puerta de enlace local y ver la tabla de enrutamiento y la configuración de la interfaz virtual. Para obtener más información, consulte Recursos de Outpost que se pueden compartir en la Guía del usuario de AWS Outposts .		Puede compartir solo con Cuentas de AWS de su propia organización.		

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Sitios de Outposts `outposts:Site`	Cree y administre sitios de Outpost y compártalos con otras Cuentas de AWS de su organización. Esto permite que varias cuentas creen y administren Outposts en el sitio compartido, y permite dividir el control entre los recursos de Outpost y el sitio. Para obtener más información, consulta Cómo trabajar con recursos compartidos de AWS Outposts en la Guía del AWS Outposts usuario.	N	S Puede compartir con cualquier Cuenta de AWS.	N	No

Amazon S3 en Outposts

Puede compartir el siguiente recurso de Amazon S3 en Outposts utilizando AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
S3 en Outposts `s3-outposts:Outpost`	Cree y administre buckets, puntos de acceso y puntos de conexión de Amazon S3 en Outpost. Esto permite que varias cuentas creen y administren Outposts en el sitio compartido, y permite dividir el control entre los recursos de Outpost y el sitio. Para obtener más información, consulta Cómo trabajar con recursos compartidos de AWS Outposts en la Guía del AWS Outposts usuario.	N	N Puede compartir solo con Cuentas de AWS de su propia organización.	S	No

AWS Private Certificate Authority

Puede compartir los siguientes Autoridad de certificación privada de AWS recursos mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Autoridad de certificación privada (CAs) `acm-pca:CertificateAuthority`	Cree y administre autoridades de certificación privadas (CAs) para la infraestructura de clave pública (PKI) interna de su organización y compártalas CAs con otras entidades Cuentas de AWS o con su organización. Esto permite a los usuarios de AWS Certificate Manager de otras cuentas emitir certificados X.509 firmados por la entidad de certificación compartida por usted. Para obtener más información, consulte Controlar el acceso a una CA privada en la Guía del usuario de AWS Private Certificate Authority .	 S	 S Puede compartir con cualquier Cuenta de AWS.	 N	 Sí

Explorador de recursos de AWS

Puede compartir los siguientes Explorador de recursos de AWS recursos mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Vistas de Resource Explorer `resource-explorer-2:View`	Cree y configure las vistas del Explorador de recursos de forma centralizada y compártalas con otras Cuentas de AWS personas de su organización. Esto permite a los roles y usuarios Cuentas de AWS buscar y descubrir los recursos a los que se puede acceder a través de la vista en múltiples ocasiones. Para obtener más información, consulte Compartir vistas de Resource Explorer en la Guía del usuario de Explorador de recursos de AWS .	 N	 N Puede compartir solo con Cuentas de AWS de su propia organización.	 N	 No

Grupos de recursos de AWS

Puede compartir los siguientes Grupos de recursos de AWS recursos mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Resource Groups `resource-groups:Group`	Cree y administre un grupo de recursos del anfitrión de forma centralizada y compártalo con otros Cuentas de AWS miembros de su organización. Esto permite que varias Cuentas de AWS compartan un grupo de hosts dedicados de Amazon EC2 creado con AWS License Manager. Para obtener más información, consulte Grupos de recursos de host en AWS License Manager en la Guía del usuario de AWS License Manager .	 N	 S Puede compartir con cualquier Cuenta de AWS.	 N	 No

Amazon Route 53

Puede compartir los siguientes recursos de Amazon Route 53 utilizando AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Grupos de reglas de firewall de Route 53 Resolver `route53resolver:FirewallRuleGroup`	Cree y administre grupos de reglas de Route 53 Resolver DNS Firewall de forma centralizada y compártalos con otras Cuentas de AWS personas o con su organización. Esto permite que varias cuentas compartan un conjunto de criterios para inspeccionar y gestionar las consultas de DNS salientes que pasan a través de Route 53 Resolver. Para obtener más información, consulte Compartir grupos de reglas de DNS Firewall de Route 53 Resolver entre Cuentas de AWS en la Guía	 S	 S Puede compartir con cualquier Cuenta de AWS.	 N	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	del desarrollador de Amazon Route 53.				
Route 53 Profiles `route53profiles:Profile`	Cree y administre Route 53 de Profiles forma centralizada y compártala con otras personas Cuentas de AWS o con su organización. Esto permite que varias cuentas apliquen las configuraciones de DNS especificadas en Route 53 Profiles a varias VPCs. Para obtener más información, consulte Profiles de Amazon Route 53 en la Guía para desarrolladores de Amazon Route 53.	 S	 S Puede compartir con cualquier Cuenta de AWS.	 S	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Reglas de Resolver `route53resolver:ResolverRule`	Cree y administre las reglas de Resolver de forma centralizada y compártalas con otras Cuentas de AWS personas o con su organización. Esto permite que varias cuentas reenvíen las consultas de DNS desde sus nubes privadas virtuales (VPCs) a las direcciones IP de destino definidas en las reglas de Resolver compartidas y administradas de forma centralizada. Para obtener más información, consulte Compartir las reglas de Resolver con otras Cuentas de AWS personas y usar reglas compartidas en la Guía para desarrolladores de Amazon Route 53.	N	S Puede compartir con cualquier Cuenta de AWS.	N	No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Configuraciones de registro de consultas de Resolver `route53resolver:ResolverQueryLogConfig`	Cree y administre registros de consultas de forma centralizada, y compártalos con otras Cuentas de AWS o con su organización. Esto Cuentas de AWS permite registrar varias consultas de DNS que se originan en ellas VPCs en un registro de consultas administrado centralmente. Para obtener más información, consulte Compartir configuraciones de registro de consultas de Resolver con otras Cuentas de AWS en la Guía del desarrollador de Amazon Route 53.	Sí	Sí Puede compartir con cualquier Cuenta de AWS.	Sí	No

Amazon Simple Storage Service

Puede compartir los siguientes Amazon Simple Storage Service recursos mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Concesiones de acceso a S3 `s3:AccessGrants`	Cree y administre la instancia S3 Access Grants de forma centralizada y compártala con otras personas Cuentas de AWS o con su organización. Esto permite que varias cuentas consulten y eliminen los recursos compartidos. Para obtener más información, consulte S3 Access Grants Cross-Account Access en la Guía del Amazon Simple Storage Service usuario.	 S	 S Puede compartir con cualquier Cuenta de AWS.	 S	 Sí

Amazon SageMaker AI

Puede compartir los siguientes recursos de Amazon SageMaker AI mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
SageMaker Catálogos de recursos de IA `sagemaker:SagemakerCatalog`	Para facilitar la detección: permite a los propietarios de las cuentas conceder permisos de detección a otras cuentas para todos los recursos de los grupos de funciones del SageMaker catálogo de IA. Una vez concedido el acceso, los usuarios de dichas cuentas pueden ver los grupos de características que se han compartido con ellos desde el catálogo. Para obtener más información, consulte Descubribilidad y acceso a grupos de funciones entre cuentas en la Guía para desarrolladores de Amazon SageMaker AI.	N	S Puede compartir con cualquier Cuenta de AWS.	S	No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	Note La visibilidad y el acceso son permisos independientes en la IA. SageMaker				

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
SageMaker Grupos de funciones de IA `sagemaker:FeatureGroup`	Con fines de acceso: permite a los propietarios de las cuentas conceder permisos de acceso a otras cuentas para determinados recursos de grupos de características. Una vez concedido el acceso, los usuarios de esas cuentas pueden usar los grupos de características que se han compartido con ellos. Para obtener más información, consulte Descubribilidad y acceso a grupos de funciones entre cuentas en la Guía para desarrolladores de Amazon SageMaker AI. **Note** La visibilidad y el acceso son permisos	S	S Puede compartir con cualquier Cuenta de AWS.	S	No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	independientes en la IA. SageMaker				
SageMaker Centros de IA `sagemaker:Hub`	Con Amazon SageMaker AI JumpStart, puede crearlos y administrarlos de `sagemaker:Hub` forma centralizada y compartirlos con otros Cuentas de AWS miembros de la misma organización. Para obtener más información, consulte Control del acceso al modelo básico mediante centros privados seleccionados en Amazon SageMaker AI JumpStart en la Guía para desarrolladores de Amazon SageMaker AI.	S	S Puede compartir con cualquier Cuenta de AWS.	S	No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
SageMaker Grupos de linaje de IA `sagemaker:LineageGroup`	Amazon SageMaker AI le permite crear grupos de linajes de los metadatos de su canalización para comprender mejor su historia y sus relaciones. Comparta el grupo de linaje con otras cuentas Cuentas de AWS o con las de su organización. Esto permite a varios Cuentas de AWS usuarios ver información sobre el grupo de linaje y consultar las entidades de seguimiento que lo integran. Para obtener más información, consulte el seguimiento del linaje entre cuentas en la Guía para desarrolladores de Amazon SageMaker AI.	S	S Puede compartir con cualquier Cuenta de AWS.	N	No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
SageMaker Tarjetas modelo AI `sagemaker:ModelCard`	Amazon SageMaker AI crea tarjetas modelo para documentar detalles críticos sobre sus modelos de aprendizaje automático (ML) en un solo lugar para agilizar la gobernanza y la elaboración de informes. Comparta sus tarjetas de modelos con otras Cuentas de AWS o con las cuentas de su organización para conseguir una estrategia multicuenta para sus operaciones de machine learning. Esto permite Cuentas de AWS compartir el acceso de las tarjetas modelo para sus actividades de aprendizaje automático con otras cuentas. Para obtener más informaci	 S	 S Puede compartir con cualquier Cuenta de AWS.	 N	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	ón, consulta las tarjetas modelo de Amazon SageMaker AI en la Guía para desarrolladores de Amazon SageMaker AI.				
SageMaker Grupos de paquetes de modelos de IA `sagemaker:model-package-group`	Con Amazon SageMaker AI Model Registry, puede crearlos y gestionar los de `sagemaker:model-package-group` forma centralizada y compartirlos con otras personas Cuentas de AWS para registrar versiones de modelos. Para obtener más información, consulte Amazon SageMaker AI Model Registry en la Guía para desarrolladores de Amazon SageMaker AI.	 S	 S	 S	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
SageMaker Aplicaciones de AI Partner `sagemaker:PartnerApp`	Con las aplicaciones de IA de SageMaker AI Partner, puede crear y gestionar las aplicaciones de IA de SageMaker AI Partner de forma centralizada y compartir el acceso a ellas con otras personas Cuentas de AWS. Para obtener más información, consulta Cómo configurar el uso compartido entre cuentas para las aplicaciones de SageMaker IA asociadas a Amazon AI en la Guía para desarrolladores de Amazon SageMaker AI.	 S	 S Puede compartir con cualquier Cuenta de AWS.	 N	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
SageMaker Canalizaciones de IA `sagemaker:Pipeline`	Con Amazon SageMaker AI Model Building Pipelines, puede crear, automatizar y gestionar flujos de trabajo end-to-end de aprendizaje automático a escala. Comparta sus canalizaciones con otras cuentas Cuentas de AWS o con las de su organización para lograr una estrategia de cuentas múltiples para sus operaciones de aprendizaje automático. Esto permite a varios Cuentas de AWS usuarios ver información sobre una canalización y sus ejecuciones, con acceso opcional para iniciar, detener y volver a intentar canalizaciones desde otras cuentas. Para obtener más informaci	 S	 S Puede compartir con cualquier Cuenta de AWS.	 S	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	ón, consulte Cross-Account Support for SageMaker AI Pipelines en la Guía para desarrolladores de Amazon SageMaker AI.				

AWS Service Catalog AppRegistry

Puede compartir los siguientes AWS Service Catalog AppRegistry recursos utilizando. AWS RAM

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
AppRegistry Aplicaciones `servicecatalog:Applications`	Cree una aplicación y utilícela para realizar un seguimiento de los recursos que pertenecen a esa aplicación en todo su AWS entorno. Comparta la aplicació	N	N Puede compartir solo con	S	No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	n con otras personas Cuentas de AWS o con su organización. Esto permite a varios Cuentas de AWS usuarios ver la información sobre la aplicación y los recursos asociados a ella de forma local. Para obtener más información, consulte Crear aplicaciones en la Guía del usuario de Service Catalog.		Cuentas de AWS de su propia organización.		

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
AppRegistry Grupos de atributos `servicecatalog:AttributeGroups`	Cree un grupo de atributos y utilícelo para almacenar metadatos relacionados con sus aplicaciones. Comparta los grupos de atributos con otras Cuentas de AWS o con su organización. Esto permite que varias Cuentas de AWS y usuarios puedan ver información sobre los grupos de atributos . Para obtener más información, consulte Crear grupos de atributos en la Guía del usuario de Service Catalog.	N	N Puede compartir solo con Cuentas de AWS de su propia organización.	S	No

Administrador de incidentes de AWS Systems Manager

Puede compartir los siguientes Administrador de incidentes de AWS Systems Manager recursos mediante AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Contactos de Incident Manager `ssm-contacts:Contact`	Cree y gestione los contactos y los planes de escalamiento de forma centralizada y comparta los detalles de contacto con otras Cuentas de AWS personas o con su organización. Esto permite a muchos Cuentas de AWS ver las interacciones que se producen durante un incidente. **Note** Actualmente, no se puede añadir un contacto compartido desde otra cuenta a un plan de respuesta a incidentes.	 S	 S Puede compartir con cualquier Cuenta de AWS.	 S	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	Para obtener más información, consulte Trabajar con contactos compartidos y planes de respuesta en la Guía del usuario del Administrador de incidentes de AWS Systems Manager.				

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Planes de respuesta del Administrador de incidentes `ssm-incidents:ResponsePlan`	Cree y gestione planes de respuesta de forma centralizada y compártalos con otras personas Cuentas de AWS o con su organización. Esto les permite Cuentas de AWS conectar las CloudWatch alarmas de Amazon y las reglas de EventBridge eventos de Amazon con los planes de respuesta, creando automáticamente un incidente cuando se detecta. El incidente también tiene acceso a las métricas de estas otras Cuentas de AWS. Para obtener más información, consulte Trabajar con contactos compartidos y planes de respuesta en la Guía del usuario del Administrador de	 S	 S Puede compartir con cualquier Cuenta de AWS.	 S	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	incidentes de AWS Systems Manager.				

AWS Systems Manager

Puede compartir los siguientes AWS Systems Manager recursos utilizando AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Políticas de rechazo automático del acceso a los nodos justo a tiempo de SSM `ssm:Document`	Cree una política de aprobación para el acceso a los just-in-time nodos con Systems Manager. Una política de denegación de acceso impide explícitamente la aprobación automática de las solicitudes de acceso a los nodos specific	 S	 S Puede compartir con cualquier Cuenta de AWS.	 S	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	ados. Comparta la política de denegación de acceso con otras personas Cuentas de AWS o con su organización. Esto garantiza que su política de denegación de acceso para el acceso a los just-in-time nodos se aplique a todas las cuentas de su organización. Para obtener más información, consulte el acceso a los Just-in-time nodos mediante Systems Manager en la Guía del AWS Systems Manager usuario.				

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Parámetros avanzados de Almacén de parámetros `ssm:Parameter`	Cree un parámetro y utilícelo para almacenar datos de configuración a los que puede hacer referencia en los scripts, comandos, documentos de SSM y flujos de trabajo de configuración y automatización. Comparta el parámetro con otras personas Cuentas de AWS o con su organización. Esto permite a varias Cuentas de AWS y usuarios ver información sobre la cadena y mejora la seguridad al separar los datos del código. Para obtener más información, consulte Trabajo con parámetros compartidos en la Guía del usuario de AWS Systems Manager .	 S	 S Puede compartir con cualquier Cuenta de AWS.	 S	 No

Amazon VPC

Puede compartir los siguientes recursos de Amazon Virtual Private Cloud (Amazon VPC) utilizando AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Propiedad del cliente IPv4pool `ec2:CoipPool`	Durante el proceso de AWS Outposts instalación, AWS crea un conjunto de direcciones, conocido como grupo de direcciones IP propiedad del cliente, en función de la información que usted proporciona sobre la red local. Las direcciones IP propiedad del cliente proporcionan conectividad local, o conectividad externa a recursos de sus subredes de Outposts a través de su red en las instalaciones. Puede asignar estas direcciones a recursos de su Outpost,	 N	 N Puede compartir solo con Cuentas de AWS de su propia organización.	 N	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	como instancias de EC2, utilizando direcciones IP elásticas, o bien utilizando la configuración de subred que asigna automáticamente las direcciones IP propiedad del cliente. Para obtener más información, consulte Direcciones IP propiedad del cliente en la Guía del usuario de AWS Outposts .				

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Grupos de IPAM `ec2:IpamPool`	Comparta los grupos de IPAM de Amazon VPC de forma centralizada con otros Cuentas de AWS roles o usuarios de IAM o con toda una organización o unidad organizativa (OU). AWS Organizations Esto permite a esos directores asignar recursos CIDRs del grupo a AWS recursos, por ejemplo VPCs, en sus cuentas respectivas. Para obtener más información, consulte Compartir un grupo de IPAM utilizando AWS RAM en la Guía del usuario del Administrador de direcciones IP de Amazon VPC.	 S	 S Puede compartir con cualquier Cuenta de AWS.	 S	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Detecciones de recursos de IPAM `ec2:IpamResourceDiscovery`	Comparta los descubrimientos de recursos con otros Cuentas de AWS. Una detección de recursos es un componente de IPAM de Amazon VPC que permite a IPAM administrar y monitorizar recursos que pertenecen a la cuenta propietaria. Para obtener más información, consulte Cómo trabajar con las detecciones de recursos en la Guía del usuario de IPAM de Amazon VPC.	 N	 S Puede compartir con cualquier Cuenta de AWS.	 N	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Listas de prefijos `ec2:PrefixList`	Cree y gestione listas de prefijos de forma centralizada y compártalas con otras personas Cuentas de AWS o con su organización. Esto permite que varias Cuentas de AWS hagan referencia a listas de prefijos de sus recursos, como grupos de seguridad de VPC y tablas de enrutamiento de subred. Para obtener más información, consulte Trabajar con listas de prefijos compartidas en la Guía del usuario de Amazon VPC.	 N	 S Puede compartir con cualquier Cuenta de AWS.	 N	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Subredes `ec2:Subnet`	Cree y administre subredes de forma centralizada, y compártalas con Cuentas de AWS de su organización. Esto permite que varias Cuentas de AWS lancen recursos de sus aplicaciones en VPC administradas de forma centralizada. Estos recursos incluyen instancias de Amazon EC2, bases de datos de Amazon Relational Database Service (RDS), clústeres y funciones de Amazon Redshift. AWS Lambda Para obtener más información, consulte Uso compartido de VPC en la Guía del usuario de Amazon VPC.	 N	 N Puede compartir solo con Cuentas de AWS de su propia organización.	 N	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	Note Para incluir una subred al crear un recurso compartido, debe disponer de los permisos `ec2:DescribeSubnets` y `ec2:DescribeVpcs` , además de `ram:CreateResourceShare` . Las subredes predeterminadas no se pueden compartir. Solo puede compartir las subredes que cree usted mismo.				

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Grupos de seguridad `ec2:SecurityGroup`	Cree y gestione grupos de seguridad de forma centralizada y compártalos con otras Cuentas de AWS personas o con su organización. Esto permite a varias Cuentas de AWS asociar el grupo de seguridad a sus interfaces de red elásticas. Para obtener más información, consulte Cómo compartir un grupo de seguridad en la Guía del usuario de Amazon VPC.	 S	 N Puede compartir solo con Cuentas de AWS de su propia organización.	 S	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Destinos de reflejo de tráfico `ec2:TrafficMirrorTarget`	Cree y gestione los objetivos duplicados de tráfico de forma centralizada y compártalos con otras Cuentas de AWS personas o con su organización. Esto permite que varias Cuentas de AWS envíen tráfico de red reflejado desde fuentes de tráfico replicadas de sus cuentas a un destino de reflejo de tráfico compartido y administrado de forma centralizada. Para obtener más información, consulte Destinos de reflejo de tráfico entre cuentas en la Guía de reflejo de tráfico.	 N	 S Puede compartir con cualquier Cuenta de AWS.	 N	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Puertas de enlace de tránsito `ec2:TransitGateway`	Cree y gestione las pasarelas de transporte de forma centralizada y compártalas con otras personas Cuentas de AWS o con su organización. Esto permite que varios Cuentas de AWS enruten el tráfico entre sus redes VPCs y las locales a través de una pasarela de tránsito compartida y gestionada de forma centralizada. Para obtener más información, consulte Compartir una puerta de enlace de tránsito en Puertas de enlace de tránsito de Amazon VPC. **Note** Para incluir una puerta de enlace de	 No	 Sí Puede compartir con cualquier Cuenta de AWS.	 No	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	tránsito al crear un recurso compartido, debe tener el permiso `ec2:DescribeTransitGateway` , además de `ram:CreateResourceShare` .				

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Dominios de multidifusión de puerta de enlace de tránsito `ec2:TransitGatewayMulticastDomain`	Cree y gestione los dominios de multidifusión de Transit Gateway de forma centralizada y compártalos con otras personas Cuentas de AWS o con su organización. Esto permite Cuentas de AWS registrar y anular el registro de varios miembros del grupo o fuentes de grupo en el dominio de multidifusión. Para obtener más información, consulte Cómo trabajar con dominios de multidifusión compartidos en la Guía de puertas de enlace de tránsito.	 N	 S Puede compartir con cualquier Cuenta de AWS.	 N	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Acceso verificado de AWS grupos `ec2:VerifiedAccessGroup`	Cree y administre Acceso verificado de AWS grupos de forma centralizada y, a continuación, compártalos con otras Cuentas de AWS personas o con su organización. Esto permite que las aplicaciones de varias cuentas utilicen un único conjunto compartido de Acceso verificado de AWS puntos finales. Para obtener más información, consulta Cómo compartir tu Acceso verificado de AWS grupo AWS Resource Access Manager en la Guía del Acceso verificado de AWS usuario.	 S	 S Puede compartir con cualquier Cuenta de AWS.	 N	 No

Amazon VPC Lattice

Puede compartir los siguientes recursos de Amazon VPC Lattice utilizando AWS RAM.

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Configuración de recursos de Amazon VPC Lattice `vpc-lattice:ResourceConfiguration`	Cree una configuración de recursos en Amazon VPC Lattice para compartir los recursos de VPC entre cuentas y. VPCs En la configuración del recurso, identifique quién podrá acceder a ese recurso y la puerta de enlace de recursos a través de la cual quiere compartir el recurso. Los consumidores podrán acceder al recurso de VPC a través del punto de conexión de VPC de recursos que hayan creado en AWS PrivateLink. Para obtener más información, consulte Acceso a los recursos de	N	S Puede compartir con cualquier Cuenta de AWS.	S	No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
	VPC a través de AWS PrivateLink en la Guía del ç usuario de AWS PrivateLink y Configuración de recursos para recursos de VPC en la Guía del usuario de VPC Lattice.				

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Servicios de Amazon VPC Lattice `vpc-lattice:Service`	Cree y gestione los servicios de Amazon VPC Lattice de forma centralizada y compártalos con una persona Cuentas de AWS o con su organización. Esto permite a los propietarios de los servicios conectarse, proteger y observar la service-to-service comunicación en un entorno de varias cuentas. Para obtener más información, consulte Trabajar con recursos compartidos en la Guía del usuario de VPC Lattice.	 N	 S Puede compartir con cualquier Cuenta de AWS.	 S	 No

Tipo de recurso y código	Caso de uso	Puede compartir con usuarios y roles de IAM	Puede compartir con cuentas externas a su organización	Puede usar permisos administrados por el cliente	Puede compartir con entidades principales de servicio
Red de servicios de Amazon VPC Lattice `vpc-lattice:ServiceNetwork`	Cree y gestione las redes de servicios Amazon VPC Lattice de forma centralizada y compártalas con una persona Cuentas de AWS o con su organización. Esto permite a los propietarios de redes de servicios conectarse, proteger y observar la service-to-service comunicación en un entorno de múltiples cuentas. Para obtener más información, consulte Trabajar con recursos compartidos en la Guía del usuario de Amazon VPC Lattice.	N	S Puede compartir con cualquier Cuenta de AWS.	S	No

Administrar permisos en AWS RAM

En AWS RAM, hay dos tipos de permisos administrados, los permisosAWS administrados y los permisos administrados por el cliente.

Los permisos administrados definen la forma en que una entidad consumidora puede actuar en los recursos de un recurso compartido. Al crear un recurso compartido, debe especificar qué permiso administrado desea usar para cada tipo de recurso incluido en el recurso compartido. La plantilla de política del permiso administrado contiene todo lo necesario para una política basada en recursos, excepto la entidad principal y el recurso. El nombre del recurso de Amazon (ARN) del recurso y el ARN de los principales asociados al recurso compartido completan los elementos de una política basada en recursos.AWS RAM a continuación, crea la política basada en recursos que se adjunta a todos los recursos de ese recurso compartido.

Cada permiso administrado puede tener una o más versiones. Se designa una versión como versión predeterminada del permiso administrado. Ocasionalmente,AWS actualiza un permiso AWS administrado para un tipo de recurso creando una nueva versión y designando esa nueva versión como predeterminada. También puede actualizar sus permisos administrados por el cliente creando versiones nuevas. Los permisos administrados que ya están adjuntos a un recurso compartido no se actualizan automáticamente. La consola de AWS RAM indica cuándo hay disponible una nueva versión predeterminada; usted puede revisar qué cambios incorpora la nueva versión predeterminada respecto de la anterior.

> **Note**
>
> Le recomendamos que actualice a la nueva versión del permiso AWS administrado lo antes posible. Por lo general, estas actualizaciones agregan soporte para nuevos o actualizados Servicios de AWS que pueden compartir tipos de recursos adicionales AWS RAM. Una nueva versión predeterminada también puede abordar y corregir vulnerabilidades de seguridad.

> **Important**
>
> A un recurso compartido nuevo solo se le puede adjuntar la versión predeterminada del permiso administrado.

Puede recuperar la lista de los permisos administrados disponibles en cualquier momento. Para obtener más información, consulte Ver permisos administrados.

Temas

Ver permisos administrados

Puede ver detalles relativos a los permisos administrados que están disponibles para asignarlos a los tipos de recursos contenidos en sus recursos compartidos. Puede identificar los permisos administrados que se asignan a los recursos compartidos. Para ver estos detalles, use la Biblioteca de permisos administrados de la consola de AWS RAM.

Console

Para ver detalles relativos a los permisos administrados disponibles en AWS RAM

1. Vaya a la página de la Biblioteca de permisos administrados en la consola de AWS RAM.
2. Puesto que los recursos compartidos de AWS RAM son específicos de las diferentes Regiones de AWS, elija la Región de AWS que corresponda en la lista desplegable de la esquina superior derecha de la consola. Para ver los recursos compartidos que contienen recursos globales, debe definir la Región de AWS como Este de EE. UU. (Norte de Virginia), (`us-east-1`). Para obtener información sobre cómo compartir recursos globales, consulte Compartir recursos regionales frente a recursos globales. Si bien todas las regiones comparten los mismos permisos administrados de AWS disponibles, esto afecta al número de recursos compartidos asociados que se muestra para cada permiso administrado en el Step 5. Los permisos administrados por el cliente solo están disponibles en la región en la se crearon.
3. En la lista Permisos administrados, elija el permiso administrado cuyos detalles desea ver. Puede usar el cuadro de búsqueda para filtrar la lista de permisos administrados; para ello,

introduzca parte de un nombre o tipo de recurso o elija un tipo de permiso administrado en la lista desplegable.

4. (Opcional) Para cambiar las preferencias de visualización, seleccione el icono de engranaje en la esquina superior derecha del panel Permisos administrados. Puede cambiar las siguientes preferencias:

   - Tamaño de página: el número de recursos que se muestran en cada página.
   - Ajustar líneas: si se deben ajustar las líneas en las filas de la tabla.
   - Columnas: si se debe mostrar u ocultar información sobre el tipo de recurso y los recursos compartidos asociados.

   Cuando termine de configurar las preferencias de visualización, seleccione Confirmar.

5. La lista muestra la siguiente información de cada permiso administrado:

   - Nombre del permiso administrado: el nombre del permiso administrado.
   - Tipo de recurso: el tipo de recurso asociado al permiso administrado.
   - Tipo de permiso administrado: si el permiso administrado es un permiso administrado por AWS o un permiso administrado por el cliente.
   - Recursos compartidos asociados: el número de recursos compartidos que están asociados al permiso administrado. Si aparece un número, pulse en él para ver una tabla de recursos compartidos con la siguiente información:
     - Nombre del recurso compartido: el nombre del recurso compartido que está asociado al permiso administrado.
     - Versión del permiso administrado: la versión del permiso administrado que se ha adjuntado al recurso compartido.
     - Propietario: el número de Cuenta de AWS del propietario del recurso compartido.
     - Permitir entidades principales externas: indica si el recurso compartido permite compartir con entidades principales externas a la organización en AWS Organizations.
     - Estado: el estado actual de la asociación entre el recurso compartido y el permiso administrado.
   - Estado: describe el permiso administrado de la siguiente forma:
     - Adjuntable: el permiso administrado se puede adjuntar a sus recursos compartidos.
     - No adjuntable: el permiso administrado no se puede adjuntar a sus recursos compartidos.

- Eliminación en curso: el permiso administrado ya no está activo y se eliminará pronto.
- Eliminado: el permiso administrado se ha eliminado. Permanece visible durante dos horas antes de desaparecer de la Biblioteca de permisos administrados.

Puede elegir el nombre del permiso administrado para que se muestre más información relacionada. La página de detalles de un permiso administrado muestra la siguiente información:

- Tipo de recurso: el tipo de recurso de AWS al que se aplica el permiso administrado.
- Número de versiones: puede tener hasta cinco versiones de un permiso administrado por el cliente.
- Versión predeterminada: especifica qué versión es la predeterminada y, por lo tanto, se asigna automáticamente a todos los recursos compartidos nuevos que utilizan este permiso administrado. Todos los recursos compartidos existentes que usan versiones diferentes muestran un mensaje para que actualice el recurso compartido a la versión predeterminada.
- ARN: el nombre de recurso de Amazon (ARN) del permiso administrado. Los ARN de los permisos administrados de AWS utilizan el siguiente formato:

  `arn:aws:ram::aws:permission/AWSRAM[DefaultPermission]ShareableResourceType`

  La subcadena *`[DefaultPermission]`* (sin los corchetes en un ARN real) solo está presente en el nombre del único permiso administrado de dicho tipo de recurso que esté designado como predeterminado.
- Versiones de permisos administrados: puede elegir qué información de la versión desea que se muestre en las pestañas situadas debajo de esta lista desplegable.
  - Pestaña Detalles:
    - Hora de creación: fecha y hora en que se creó esta versión del permiso administrado.
    - Hora de la última actualización: fecha y hora en que se actualizó por última vez esta versión del permiso administrado.
  - Pestaña Plantilla de política: la lista de acciones y condiciones del servicio que, cuando procede, esta versión del permiso administrado permite realizar a las entidades principales en el tipo de recurso asociado.

- Recursos compartidos asociados: la lista de recursos compartidos que utilizan esta versión del permiso administrado.

AWS CLI

Para ver detalles relativos a los permisos administrados disponibles en AWS RAM

Puede usar el comando list-permissions para obtener una lista de los permisos administrados disponibles para su uso en los recursos compartidos en la Región de AWS actual de la cuenta que realiza la llamada.

```
$ aws ram list-permissions
{
    "permissions": [
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority",
            "version": "1",
            "defaultVersion": true,
            "name":
 "AWSRAMBlankEndEntityCertificateAPICSRPassthroughIssuanceCertificateAuthority",
            "resourceType": "acm-pca:CertificateAuthority",
            "status": "ATTACHABLE",
            "creationTime": "2022-06-30T13:03:31.732000-07:00",
            "lastUpdatedTime": "2022-06-30T13:03:31.732000-07:00",
            "isResourceTypeDefault": false,
            "permissionType": "AWS_MANAGED"
        },
        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMBlankEndEntityCertificateAPIPassthroughIssuanceCertificateAuthority",
            "version": "1",
            "defaultVersion": true,
            "name":
 "AWSRAMBlankEndEntityCertificateAPIPassthroughIssuanceCertificateAuthority",
            "resourceType": "acm-pca:CertificateAuthority",
            "status": "ATTACHABLE",
            "creationTime": "2022-11-18T07:05:46.976000-08:00",
            "lastUpdatedTime": "2022-11-18T07:05:46.976000-08:00",
            "isResourceTypeDefault": false,
            "permissionType": "AWS_MANAGED"
        },
```

```
        ... TRUNCATED FOR BREVITY ... RUN COMMAND TO SEE COMPLETE LIST OF
 PERMISSIONS ...

        {
            "arn": "arn:aws:ram::aws:permission/
AWSRAMVPCPermissionsNetworkManagerCoreNetwork",
            "version": "1",
            "defaultVersion": true,
            "name": "AWSRAMVPCPermissionsNetworkManagerCoreNetwork",
            "resourceType": "networkmanager:CoreNetwork",
            "status": "ATTACHABLE",
            "creationTime": "2022-06-30T13:03:46.557000-07:00",
            "lastUpdatedTime": "2022-06-30T13:03:46.557000-07:00",
            "isResourceTypeDefault": false,
            "permissionType": "AWS_MANAGED"
        },        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP",
            "version": "1",
            "defaultVersion": true,
            "name": "My-Test-CMP",
            "resourceType": "ec2:IpamPool",
            "status": "ATTACHABLE",
            "creationTime": "2023-03-08T06:54:10.038000-08:00",
            "lastUpdatedTime": "2023-03-08T06:54:10.038000-08:00",
            "isResourceTypeDefault": false,
            "permissionType": "CUSTOMER_MANAGED"
        }
    ]
}
```

También puede encontrar el ARN de un permiso administrado específico por su nombre en el parámetro `--query` del comando `list-permissions` de la AWS CLI. El siguiente ejemplo filtra el resultado para incluir solo los elementos de los resultados de la matriz `permissions` que coincidan con el nombre especificado. También especificamos que queremos ver solo el campo ARN en los resultados, y en formato de solo texto en lugar del JSON predeterminado.

```
$ aws ram list-permissions \
    --query "permissions[?name == 'My-Test-CMP'].arn \
    --output text
arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP
```

Una vez que encuentre el ARN del permiso administrado en cuestión, puede recuperar sus detalles, incluido el texto de la política JSON, ejecutando el comando get-permission.

```
$ aws ram get-permission \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP
{
    "permission": {
        "arn": "arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP",
        "version": "1",
        "defaultVersion": true,
        "name": "My-Test-CMP",
        "resourceType": "ec2:IpamPool",
        "permission": "{\n\t\"Effect\": \"Allow\",\n\t\"Action\": [\n
\t\t\"ec2:GetIpamPoolAllocations\",\n\t\t\"ec2:GetIpamPoolCidrs\",\n\t
\t\"ec2:AllocateIpamPoolCidr\",\n\t\t\"ec2:AssociateVpcCidrBlock\",\n
\t\t\"ec2:CreateVpc\",\n\t\t\"ec2:ProvisionPublicIpv4PoolCidr\",\n\t\t
\"ec2:ReleaseIpamPoolAllocation\"\n\t]\n}",
        "creationTime": "2023-03-08T06:54:10.038000-08:00",
        "lastUpdatedTime": "2023-03-08T06:54:10.038000-08:00",
        "isResourceTypeDefault": false,
        "permissionType": "CUSTOMER_MANAGED",
        "featureSet": "STANDARD",
        "status": "ATTACHABLE"
    }
}
```

Creación y uso de permisos gestionados por el cliente en AWS RAM

AWS Resource Access Manager (AWS RAM) proporciona al menos un permiso AWS administrado para cada tipo de recurso que puedas compartir. No obstante, es posible que dichos permisos administrados no proporcionen acceso con privilegio mínimo para su caso de uso compartido. Si uno de los permisos AWS gestionados proporcionados no funciona, puedes crear tu propio permiso gestionado por el cliente.

Los permisos administrados por el cliente son permisos administrados que usted crea y mantiene especificando con precisión qué acciones se pueden realizar en los recursos que se comparten con AWS RAM y en qué condiciones. Por ejemplo, digamos que desea limitar el acceso de lectura a sus grupos del Administrador de direcciones IP (IPAM) de Amazon VPC, que le ayudan a administrar

sus direcciones IP a gran escala. Puede crear permisos administrados por el cliente para que sus desarrolladores asignen direcciones IP, pero no ver el rango de direcciones IP que asignan otras cuentas de desarrollador. Puede seguir las prácticas recomendadas de privilegio mínimo para conceder únicamente los permisos necesarios para realizar tareas en los recursos compartidos.

Además, puede actualizar o eliminar los permisos administrados por el cliente según sea necesario.

Temas

Crear un permiso administrado por el cliente

Los permisos gestionados por el cliente son específicos de un Región de AWS. Asegúrese de crear este permiso administrado por el cliente en la región que corresponda.

Console

Para crear un permiso administrado por el cliente

1. Lleve a cabo una de las siguientes acciones:
   - Vaya a la Biblioteca de permisos administrados y seleccione Crear un permiso administrado por el cliente.
   - Vaya directamente a la página Crear un permiso administrado por el cliente de la consola.
2. Para ver los detalles del permiso administrado por el cliente, introduzca el nombre de un permiso administrado por el cliente.
3. Seleccione el tipo de recurso al que se aplica el permiso administrado.
4. En Plantilla de política, defina qué operaciones se pueden realizar en este tipo de recurso.
   - Puede seleccionar Importar un permiso administrado para usar las acciones de un permiso administrado existente.

- Marque o desmarque la información de nivel de acceso en función de sus requisitos en el editor visual.
- Añada o modifique condiciones con el editor JSON.

5. (Opcional) Para adjuntar etiquetas al permiso administrado, en Etiquetas, introduzca una clave y un valor de etiqueta. Para añadir más etiquetas, seleccione Añadir nueva etiqueta. Repita este paso tantas veces como sea necesario.
6. Una vez que haya terminado, seleccione Crear permiso administrado por el cliente.

AWS CLI

Para crear un permiso administrado por el cliente

- Ejecute el comando create-permission y especifique un nombre, el tipo de recurso al que se aplica el permiso administrado por el cliente y el texto principal de la plantilla de política.

  El siguiente comando de ejemplo crea un permiso administrado para el tipo de recurso `imagebuilder:Component`.

```
$ aws ram create-permission \
    --name TestCMP \
    --resource-type imagebuilder:Component \
    --policy-template "{\"Effect\":\"Allow\",\"Action\":
[\"imagebuilder:ListComponents\"]}"
{
    "permission": {
        "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
        "version": "1",
        "defaultVersion": true,
        "isResourceTypeDefault": false,
        "name": "TestCMP",
        "resourceType": "imagebuilder:Component",
        "status": "ATTACHABLE",
        "creationTime": 1680033769.401,
        "lastUpdatedTime": 1680033769.401
    }
}
```

Crear una nueva versión de un permiso administrado por el cliente

Si cambia el caso de uso del permiso administrado por el cliente, puede crear una nueva versión del permiso administrado. Esta no afectará a los recursos compartidos existentes, solo a los recursos compartidos que cree en el futuro y que usen este permiso administrado por el cliente.

Cada permiso administrado puede tener hasta cinco versiones, pero solo es posible asociar la versión predeterminada.

Console

Para crear una nueva versión de un permiso administrado por el cliente

1. Vaya a la Biblioteca de permisos administrados.
2. Filtre la lista de permisos administrados por Administrados por el cliente, o bien busque el nombre del permiso administrado por el cliente que desea cambiar.
3. En la página de detalles de los permisos administrados, en la sección Versiones de permisos administrados, seleccione Crear versión.
4. En Plantilla de política, puede añadir o eliminar acciones y condiciones con el editor visual o el editor JSON.

   También puede elegir Importar permiso administrado para usar una plantilla de política existente.
5. Cuando haya terminado, elija Crear versión en la parte inferior de la página.

AWS CLI

Para crear una nueva versión de un permiso administrado por el cliente

1. Busque el nombre de recurso de Amazon (ARN) del permiso administrado del que desea crear una nueva versión. Para ello, llame al comando list-permissions con el parámetro `--permission-type CUSTOMER_MANAGED` para incluir únicamente los permisos administrados por el cliente.

```
$ aws ram-cmp list-permissions --permission-type CUSTOMER_MANAGED
{
    "permissions": [
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
```

```
            "version": "2",
            "defaultVersion": true,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "resourceType": "imagebuilder:Component",
            "status": "ATTACHABLE",
            "creationTime": 1680035597.346,
            "lastUpdatedTime": 1680035597.346
        }
    ]
}
```

2. Una vez que tenga el ARN, puede llamar a la create-permission-versionoperación y proporcionar la plantilla de política actualizada.

```
$ aws ram create-permission-version \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP \
    --policy-template {"Effect":"Allow","Action":
["imagebuilder:ListComponents"]}
{
    "permission": {
        "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
        "version": "2",
        "defaultVersion": true,
        "isResourceTypeDefault": false,
        "name": "TestCMP",
        "status": "ATTACHABLE",
        "resourceType": "imagebuilder:Component",
        "permission": "{\"Effect\":\"Allow\",\"Action\":
[\"imagebuilder:ListComponents\"]}",
        "creationTime": 1680038973.79,
        "lastUpdatedTime": 1680038973.79
    }
}
```

El resultado incluye el número de versión de la nueva versión.

Elegir una versión distinta para establecerla como versión predeterminada de un permiso administrado por el cliente

Puede establecer otra versión de un permiso administrado por el cliente como nueva versión predeterminada.

Console

Para establecer una nueva versión predeterminada para un permiso administrado por el cliente

1. Vaya a la Biblioteca de permisos administrados.
2. Filtre la lista de permisos administrados por Administrados por el cliente, o bien busque el nombre del permiso administrado por el cliente que desea cambiar.
3. En la página de detalles del permiso administrado por el cliente, en la sección Versiones del permiso administrado, use la lista desplegable para elegir la versión que desea establecer como nueva versión predeterminada.
4. Elija Establecer como versión predeterminada.
5. Cuando aparezca el cuadro de diálogo, confirme que desea que esta versión sea la predeterminada para todos los nuevos recursos compartidos que utilicen este permiso administrado por el cliente. Si está de acuerdo, elija Establecer como versión predeterminada.

AWS CLI

Para establecer una nueva versión predeterminada para un permiso administrado por el cliente

1. Llame para buscar el número de versión que desea establecer como versión predeterminada. list-permission-versions

   El ejemplo siguiente recupera las versiones actuales del permiso administrado especificado.

```
$ aws ram list-permission-versions \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP
{
    "permissions": [
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "1",
```

```
            "defaultVersion": false,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "featureSet": "STANDARD",
            "resourceType": "imagebuilder:Component",
            "status": "UNATTACHABLE",
            "creationTime": 1680033769.401,
            "lastUpdatedTime": 1680035597.345
        },
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "2",
            "defaultVersion": true,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "featureSet": "STANDARD",
            "resourceType": "imagebuilder:Component",
            "status": "ATTACHABLE",
            "creationTime": 1680035597.346,
            "lastUpdatedTime": 1680035597.346
        }
    ]
}
```


2. Una vez que tenga el número de versión que desee establecer como predeterminado, podrá llamar a la set-default-permission-versionoperación.

```
$ aws ram-cmp set-default-permission-version \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP \
    --version 2
```

Si se ejecuta correctamente, este comando no devuelve ningún resultado. Puede list-permission-versionsvolver a ejecutar y comprobar que el `defaultVersion` campo de la versión elegida está ahora establecido en`true`.

Eliminar una versión de un permiso administrado por el cliente

Puede tener hasta cinco versiones de cada permiso administrado por el cliente. Cuando ya no necesite una versión, y esta no se esté utilizando, puede eliminarla. No puede eliminar la versión

predeterminada de un permiso administrado por el cliente. Las versiones eliminadas permanecen visibles en la consola durante un máximo de dos horas con el estado eliminado hasta que se eliminan por completo.

Console

Para eliminar una versión de un permiso administrado por el cliente

1. Vaya a la Biblioteca de permisos administrados.
2. Filtre la lista de permisos administrados por Administrados por el cliente, o bien busque el nombre del permiso administrado por el cliente correspondiente a la versión que desea eliminar.
3. Asegúrese de que la versión que desea eliminar no es la versión predeterminada en ese momento.
4. En la sección Versiones de la página, elija la pestaña Recursos compartidos asociados para averiguar si algún recurso compartido usa esta versión.

   Si hay recursos compartidos asociados, debe cambiar la versión del permiso administrado por el cliente antes de poder eliminar esta versión.
5. Elija Eliminar versión en la parte derecha de la sección Versión.
6. En el cuadro de diálogo de confirmación, seleccione Eliminar para confirmar que desea eliminar esta versión del permiso administrado por el cliente.

   Si no desea eliminar esta versión del permiso administrado por el cliente, elija Cancelar.

AWS CLI

Para eliminar una versión de un permiso administrado por el cliente

1. Llame a la list-permission-versionsoperación para recuperar los números de versión disponibles.
2. Una vez que tenga el número de versión, indíquelo como parámetro para delete-permission-version.

```
$ aws ram-cmp delete-permission-version \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP \
    --version 1
```

Si se ejecuta correctamente, este comando no devuelve ningún resultado. Puede list-permission-versionsvolver a ejecutar y comprobar que la versión ya no esté incluida en la salida.

Eliminar un permiso administrado por el cliente

Si un permiso administrado por el cliente ya no es necesario y no está en uso, puede eliminarlo. No es posible eliminar un permiso administrado por el cliente que esté asociado a un recurso compartido. El permiso administrado por el cliente que se ha eliminado desaparece pasadas dos horas. Hasta entonces, permanece visible en la Biblioteca de permisos administrados con estado eliminado.

Console

Para eliminar un permiso administrado por el cliente

1. Vaya a la Biblioteca de permisos administrados.
2. Filtre la lista de permisos administrados por el cliente por Administrados por el cliente, o bien busque el nombre del permiso administrado por el cliente que desea eliminar.
3. Confirme que hay 0 recursos compartidos asociados en la lista de permisos administrados antes de seleccionar el permiso administrado por el cliente.

   Si aún hay recursos compartidos asociados al permiso administrado, debe asignar otro permiso administrado a todos los recursos compartidos para poder continuar.
4. En la esquina superior derecha de la página de detalles del permiso administrado por el cliente, elija Eliminar permiso administrado.
5. Cuando aparezca el cuadro de diálogo de confirmación, elija Eliminar para eliminar el permiso administrado.

AWS CLI

Para eliminar un permiso administrado por el cliente

1. Busque el ARN del permiso administrado que desea eliminar. Para hacerlo, llame a list-permissions con el parámetro `--permission-type CUSTOMER_MANAGED` para que se incluyan solo los permisos administrados por el cliente.

```
$ aws ram-cmp list-permissions --permission-type CUSTOMER_MANAGED
{
    "permissions": [
        {
            "arn": "arn:aws:ram:us-east-1:123456789012:permission/TestCMP",
            "version": "2",
            "defaultVersion": true,
            "isResourceTypeDefault": false,
            "name": "TestCMP",
            "permissionType": "CUSTOMER_MANAGED",
            "resourceType": "imagebuilder:Component",
            "status": "ATTACHABLE",
            "creationTime": 1680035597.346,
            "lastUpdatedTime": 1680035597.346
        }
    ]
}
```

2. Una vez que disponga del ARN del permiso administrado que desea eliminar, indíquelo como parámetro en delete-permission.

```
$ aws ram delete-permission \
    --permission-arn arn:aws:ram:us-east-1:123456789012:permission/TestCMP
{
    "returnValue": true,
    "permissionStatus": "DELETING"
}
```

Actualización de los permisos AWS gestionados a una versión más reciente

Ocasionalmente, AWS actualiza los permisos AWS administrados disponibles para adjuntarlos a un recurso compartido para un tipo de recurso específico. Cuando lo AWS hace, crea una nueva versión del permiso AWS administrado. Los recursos compartidos que incluyen el tipo de recurso especificado no se actualizan automáticamente para usar la versión más reciente del permiso administrado. Debe actualizar de forma explícita el permiso administrado para cada recurso compartido. Este paso adicional es necesario para que pueda evaluar los cambios antes de aplicarlos a sus recursos compartidos.

Console

Cuando la consola muestre una página donde se enumeren los permisos asociados a un recurso compartido y uno o varios de esos permisos utilicen una versión distinta de la predeterminada para el permiso, se mostrará un banner en la parte superior de la página de la consola. El banner indica que el recurso compartido usa una versión distinta de la predeterminada.

Además, cada permiso puede mostrar el botón Actualizar a la versión predeterminada junto al número de versión actual cuando dicha versión no es la predeterminada.

Al pulsar ese botón, se inicia el asistente Actualizar recurso compartido. En el paso 2 del asistente, puede actualizar la versión de cualquier permiso que use una versión distinta de la predeterminada para que use la versión predeterminada.

Los cambios no se guardarán hasta que complete el asistente. Para ello, seleccione Enviar en la última página del asistente.

> **Note**
>
> Solo se puede asociar la versión predeterminada, y es posible restablecer ninguna otra versión.
> En el caso de los permisos administrados por el cliente, después de actualizar los permisos a la versión predeterminada, no podrá aplicar otra versión a un recurso compartido, salvo que defina primero esa otra versión como predeterminada. Por ejemplo, si actualiza un permiso a la versión predeterminada y, a continuación, encuentra un error que deseaba revertir, puede designar la versión anterior como predeterminada. Como alternativa, puede crear una versión nueva distinta y, a continuación, designarla como predeterminada. Tras realizar una de estas acciones, tendría que actualizar los recursos compartidos para que usen la que ahora es la versión predeterminada.

AWS CLI

Para actualizar la versión de un permiso AWS administrado

1. Ejecute el comando get-resource-shares con el parámetro `--permission-arn` para especificar el nombre de recurso de Amazon (ARN) del permiso administrado que desea actualizar. Esto hará que el comando devuelva solo los recursos compartidos que usan ese permiso administrado.

Por ejemplo, el siguiente comando de ejemplo devuelve detalles de cada recurso compartido que utilice el permiso AWS gestionado predeterminado para las reservas de capacidad de Amazon EC2.

```
$ aws ram get-resource-shares \
    --resource-owner SELF \
    --permission-arn arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionCapacityReservation
```

El resultado incluye el ARN de cada recurso compartido que contiene al menos un recurso cuyo acceso esté controlado por dicho permiso administrado.

2. Ejecute el comando associate-resource-share-permission para cada recurso compartido especificado en el comando anterior. Incluya el `--resource-share-arn` para especificar el recurso compartido que se debe actualizar, el `--permission-arn` para especificar el permiso administrado de AWS que va a actualizar, y el parámetro `--replace` para especificar que desea actualizar el recurso compartido para que use la versión más reciente de dicho permiso administrado. No es necesario que especifique el número de versión; se usará automáticamente la versión predeterminada.

```
$ aws ram associate-resource-share-permission \
    --resource-share-arn < ARN of one of the shares from the output of the
 previous command > \
    --permission-arn arn:aws:ram::aws:permission/
AWSRAMDefaultPermissionCapacityReservation \
    --replace
```

3. Repita el comando del paso anterior para cada uno de los `ResourceShareArn` que haya recibido en los resultados del comando del paso 1.

Consideraciones sobre el uso de permisos gestionados por el cliente en AWS RAM

Los permisos administrados por el cliente solo están disponibles en el Región de AWS lugar en el que los creó. No todos los tipos de recursos admiten permisos administrados por el cliente. Para obtener una lista de los tipos de recursos compatibles en AWS Resource Access Manager, consulteRecursos que se pueden compartir AWS.

No se admiten los permisos administrados por el cliente con varias instrucciones. Los permisos administrados por el cliente solo admiten el uso de operadores únicos que no sean de denegación.

Los permisos administrados por el cliente no admiten las siguientes condiciones:

- Claves de condición utilizadas para hacer coincidir las propiedades de la entidad principal:
  - `aws:PrincipalOrgId`
  - `aws:PrincipalOrgPaths`
  - `aws:PrincipalAccount`

- Claves de condición utilizadas para restringir el acceso a las entidades principales del servicio:
  - `aws:SourceArn`
  - `aws:SourceAccount`
  - `aws:SourceOrgPaths`
  - `aws:SourceOrgID`
- Etiquetas del sistema:
  - `aws:PrincipalTag/aws:`
  - `aws:ResourceTag/aws:`
  - `aws:RequestTag/aws:`

> **Note**
>
> El valor `aws:SourceAccount` se rellena automáticamente cuando se comparte con las entidades principales del servicio.

Cómo funcionan los permisos administrados

Para obtener una descripción general breve, vea el siguiente vídeo, que incluye una demostración de cómo los permisos administrados le permiten aplicar las prácticas recomendadas de acceso con privilegio mínimo a sus recursos de AWS.

En este vídeo se ofrece una demostración de cómo crear y asociar permisos administrados por el cliente siguiendo las prácticas recomendadas de privilegio mínimo. Para obtener más información, consulte, ???.

Al crear un recurso compartido, se asocia un permiso AWS administrado a cada tipo de recurso que se quiera compartir. Si el permiso administrado tiene más de una versión, el nuevo recurso compartido siempre usa la versión designada como predeterminada.

Tras crear el recurso compartido,AWS RAM utiliza el permiso administrado para generar una política basada en recursos que se adjunta a cada recurso compartido.

La plantilla de política de un permiso administrado especifica lo siguiente:

Efecto

Indica si se debe `Allow` o `Deny` el permiso a la entidad principal para realizar una operación en un recurso compartido. En el caso de un permiso administrado, el efecto es siempre `Allow`. Para obtener más información, consulte Efecto en la Guía del usuario de IAM.

Action

La lista de operaciones para las que se concede permiso a la entidad principal. Puede ser una acción en la API Consola de administración de AWS o una operación en AWS Command Line Interface(AWS CLI) o AWS en la API. Las acciones las define el permiso de AWS. Para obtener más información, consulte Acción en la Guía del usuario de IAM.

Condición

Cuándo y cómo una entidad principal puede interactuar con un recurso de un recurso compartido. Las condiciones añaden un nivel adicional de seguridad a los recursos compartidos. Úselas para limitar el acceso a sus recursos compartidos para realizar acciones confidenciales. Por ejemplo, puede incluir condiciones que exijan que las acciones se originen en un determinado rango de direcciones IP corporativas, o que las acciones las realicen usuarios autenticados mediante autenticación multifactorial. Para obtener más información acerca de las condiciones, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM. Para obtener más información sobre las condiciones específicas de un servicio, consulta las acciones, los recursos y las claves de condición de los AWS servicios en la Referencia de autorización de servicios.

> **Note**
>
> Hay condiciones disponibles para los permisos administrados por el cliente y los tipos de recursos compatibles para los permisos administrados de AWS.
> Para obtener información sobre las condiciones que están excluidas del uso con permisos administrados por el cliente, consulte Consideraciones sobre el uso de permisos gestionados por el cliente en AWS RAM.

Tipos de permisos administrados

Al crear un recurso compartido, elige un permiso administrado para asociarlo a cada tipo de recurso que incluya en el recurso compartido.AWS Los permisos administrados los define el AWS servicio propietario del recurso y los administra.AWS RAM Usted se encarga de crear y mantener sus propios permisos administrados por el cliente.

- AWS permiso administrado: hay un permiso administrado predeterminado disponible para cada tipo de recurso compatible.AWS RAM El permiso administrado predeterminado es el que se usa para un tipo de recurso, a menos que se seleccione explícitamente uno de los permisos administrados adicionales. El permiso administrado predeterminado está diseñado para admitir los escenarios de cliente más frecuentes a la hora de compartir recursos del tipo especificado. El permiso administrado predeterminado permite a las entidades principales realizar acciones específicas definidas por el servicio para el tipo de recurso. Por ejemplo, para el tipo de recurso `ec2:Subnet` de Amazon VPC, el permiso administrado predeterminado permite a las entidades principales realizar las siguientes acciones:
  - `ec2:RunInstances`
  - `ec2:CreateNetworkInterface`
  - `ec2:DescribeSubnets`

  Los nombres de los permisos AWS administrados predeterminados utilizan el siguiente formato:`AWSRAMDefaultPermission`*`ShareableResourceType`*. Por ejemplo, para el tipo de `ec2:Subnet` recurso, el nombre del permiso AWS administrado predeterminado es`AWSRAMDefaultPermissionSubnet`.

> **Note**
>
> El permiso administrado predeterminado es independiente de la versión predeterminada de un permiso administrado. Todos los permisos administrados, ya sea el predeterminado o uno de los permisos administrados adicionales que admiten algunos tipos de recursos, son permisos independientes y completos con diferentes efectos y acciones que admiten diferentes escenarios de uso compartido, como el acceso de lectura y escritura o de solo lectura. Cualquier permiso administrado, ya sea administrado por AWS o por el cliente, puede tener varias versiones, una de las cuales será la versión predeterminada de dicho permiso.

Por ejemplo, si comparte un tipo de recurso que admite tanto un permiso administrado de acceso total (`Read` y `Write`) como un permiso administrado de solo lectura, puede crear un recurso compartido para el administrador con el permiso administrado de acceso completo. A continuación, puede crear un recurso compartido distinto para otros desarrolladores utilizando el permiso administrado de solo lectura y, de este modo, seguir la práctica de conceder el privilegio mínimo.

> **Note**
>
> Todos los AWS servicios con los que funcionan AWS RAM admiten al menos un permiso administrado predeterminado. Puede ver los permisos disponibles para cada Servicio de AWS en la página de la Biblioteca de permisos administrados. En esta página se proporcionan detalles sobre cada permiso administrado disponible, incluidos los recursos compartidos que están actualmente asociados al permiso y, cuando corresponda, si se permite el uso compartido con entidades principales externas. Para obtener más información, consulte Ver permisos administrados.
>
> En el caso de los servicios que no admiten permisos administrados adicionales, al crear un recurso compartido, se aplica AWS RAM automáticamente el permiso predeterminado definido para el tipo de recurso que elija. Cuando esté permitido, también tendrá la opción de elegir Crear un permiso administrado por el cliente en la página Asociar permisos administrados.

- Permiso administrado por el cliente: los permisos administrados por el cliente son permisos administrados que usted crea y mantiene especificando con precisión qué acciones se pueden realizar, y en qué condiciones, en los recursos que se comparten utilizando AWS RAM. Por

ejemplo, digamos que desea limitar el acceso de lectura a sus grupos del Administrador de direcciones IP (IPAM) de Amazon VPC, que le ayudan a administrar sus direcciones IP a gran escala. Puede crear permisos administrados por el cliente para que sus desarrolladores asignen direcciones IP, pero no ver el rango de direcciones IP que asignan otras cuentas de desarrollador. Puede seguir las prácticas recomendadas de privilegio mínimo para conceder únicamente los permisos necesarios para realizar tareas en los recursos compartidos.

Seguridad en AWS Resource Access Manager

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. 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 acerca de los programas de conformidad que se aplican a AWS Resource Access Manager (AWS RAM), consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS RAM. Los siguientes temas muestran cómo configurarlo AWS RAM para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus AWS RAM recursos.

Temas

Protección de datos en AWS Resource Access Manager

El modelo de responsabilidad AWS compartida modelo se aplica a la protección de datos en AWS Resource Access Manager. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger la información confidencial almacenada en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con AWS RAM o Servicios de AWS utiliza la

consola, la API o AWS CLI AWS SDKs Cualquier dato que introduzca en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Administración de identidad y acceso para AWS Resource Access Manager

AWS Identity and Access Management (IAM) es un AWS servicio que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. AWS Al usar IAM, usted crea principios, como roles, usuarios y grupos en su. Cuenta de AWS Usted controla los permisos que tienen esos directores para realizar tareas utilizando los recursos. AWS El uso de IAM no está sujeto a ningún cargo adicional. Para obtener más información sobre cómo administrar y crear políticas de IAM personalizadas, consulte Administrar políticas de IAM en la Guía del usuario de .

Temas

- Cómo AWS RAM funciona con IAM
- AWS políticas gestionadas para AWS Resource Access Manager
- Uso de roles vinculados a servicios para AWS RAM
- Ejemplos de políticas de IAM para AWS RAM
- Ejemplos de políticas de control de servicios para AWS Organizations y AWS RAM
- Deshabilitar el uso compartido de recursos con AWS Organizations

Cómo AWS RAM funciona con IAM

De forma predeterminada, los directores de IAM no tienen permiso para crear o modificar recursos. AWS RAM Para permitir que las entidades principales de IAM creen o modifiquen recursos y realicen tareas, debe realizar uno de los pasos siguientes. Estas acciones conceden permiso a los usuarios para utilizar recursos y acciones de API específicos.

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en: AWS IAM Identity Center

Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center .

- Usuarios gestionados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.

- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o agregue un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

AWS RAM proporciona varias políticas AWS administradas que puede utilizar para satisfacer las necesidades de muchos usuarios. Para obtener más información al respecto, consulte AWS políticas gestionadas para AWS Resource Access Manager.

Si necesita un control más preciso de los permisos que concede a sus usuarios, puede crear sus propias políticas en la consola de IAM. Para obtener información sobre cómo crear políticas y adjuntarlas a sus roles y usuarios de IAM, consulte Políticas y permisos de IAM en la Guía del usuario de AWS Identity and Access Management .

En las siguientes secciones se proporcionan los detalles AWS RAM específicos para crear una política de permisos de IAM.

Contenido

Estructura de la política

Una política de permisos de IAM es un documento JSON que incluye las siguientes instrucciones: Effect, Action, Resource y Condition. Las políticas de IAM suelen tener el siguiente formato.

```
{
    "Statement":[{
        "Effect":"<effect>",
        "Action":"<action>",
        "Resource":"<arn>",
        "Condition":{
            "<comparison-operator>":{
                "<key>":"<value>"
            }
        }
    }]
}
```

Efecto

La instrucción Effect indica si la política permite o deniega a una entidad principal el permiso para realizar una acción. Los valores posibles incluyen: `Allow` y `Deny`.

Action

La declaración Action especifica las acciones de la AWS RAM API para las que la política permite o deniega el permiso. Para obtener una lista de las acciones permitidas, consulte Acciones definidas por AWS Resource Access Manager en la Guía del usuario de IAM.

Recurso

La declaración Resource especifica los AWS RAM recursos a los que afecta la política. Para especificar un recurso en la instrucción, debe usar su nombre de recurso de Amazon (ARN) exclusivo. Para obtener una lista completa de los recursos permitidos, consulte Recursos definidos por AWS Resource Access Manager en la Guía del usuario de IAM.

Condición

Las instrucciones Condition son opcionales. Se pueden utilizar para refinar aún más las condiciones en las que se aplica la política. AWS RAM admite las siguientes claves de condición:

- `aws:RequestTag/${TagKey}`: comprueba si la solicitud de servicio que incluye una etiqueta con la clave de etiqueta especificada existe y tiene el valor especificado.
- `aws:ResourceTag/${TagKey}`: comprueba si el recurso sobre el que ha actuado la solicitud de servicio tiene una etiqueta adjunta con una clave de etiqueta que se especifique en la política.

  La siguiente condición de ejemplo comprueba que el recurso al que se hace referencia en la solicitud de servicio tiene una etiqueta adjunta con el nombre de clave "Owner" y el valor "Dev Team".

  ```
  "Condition" : {
      "StringEquals" : {
          "aws:ResourceTag/Owner" : "Dev Team"
      }
  }
  ```

- `aws:TagKeys`: especifica las claves de etiqueta que se deben utilizar para crear o etiquetar un recurso compartido.
- `ram:AllowsExternalPrincipals`: comprueba si el recurso compartido de la solicitud de servicio permite el uso compartirlo con entidades principales externas. Un director externo es una persona Cuenta de AWS externa a la organización que está dentro AWS Organizations. Si el valor que arroja es `False`, solo podrá compartir este recurso compartido con cuentas de la misma organización.
- `ram:PermissionArn`: comprueba si el ARN del permiso especificado en la solicitud de servicio coincide con una cadena de ARN que especifique en la política.
- `ram:PermissionResourceType`: comprueba si el permiso especificado en la solicitud de servicio es válido para el tipo de recurso que especifique en la política. Especifique los tipos de recursos utilizando el formato que se muestra en la lista de tipos de recursos que se pueden compartir.
- `ram:Principal`: comprueba si el ARN de la entidad principal especificada en la solicitud de servicio coincide con una cadena de ARN que especifique en la política.
- `ram:RequestedAllowsExternalPrincipals`: comprueba si la solicitud de servicio incluye el parámetro `allowExternalPrincipals` y si su argumento coincide con el valor que especifique en la política.
- `ram:RequestedResourceType`: comprueba si el tipo de recurso sobre el que se está actuando coincide con una cadena de tipo de recurso que especifique en la política. Especifique los tipos

de recursos utilizando el formato que se muestra en la lista de tipos de recursos que se pueden compartir.

- `ram:ResourceArn`: comprueba si el ARN del recurso sobre el que actúa la solicitud de servicio coincide con un ARN que especifique en la política.
- `ram:ResourceShareName`: comprueba si el nombre del recurso compartido sobre el que actúa la solicitud de servicio coincide con una cadena que especifique en la política.
- `ram:ShareOwnerAccountId`: comprueba que el número de ID de cuenta del recurso compartido sobre el que actúa la solicitud de servicio coincide con una cadena que especifique en la política.

AWS políticas gestionadas para AWS Resource Access Manager

AWS Resource Access Manager actualmente proporciona varias políticas AWS RAM administradas, que se describen en este tema.

AWS políticas gestionadas

- AWS política gestionada: AWSResource AccessManagerReadOnlyAccess
- AWS política gestionada: AWSResource AccessManagerFullAccess
- AWS política gestionada: AWSResource AccessManagerResourceShareParticipantAccess
- AWS política gestionada: AWSResource AccessManagerServiceRolePolicy
- AWS RAM actualizaciones de las políticas gestionadas AWS

En la lista anterior, puede asociar las tres primeras políticas a sus roles, grupos y usuarios de IAM para conceder permisos. La última política de la lista está reservada para el rol vinculado al servicio de AWS RAM .

Una política AWS gestionada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades

principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

AWS política gestionada: AWSResource AccessManagerReadOnlyAccess

Puede vincular la política `AWSResourceAccessManagerReadOnlyAccess` a sus identidades de IAM.

Esta política proporciona permisos de solo lectura a los recursos compartidos que son propiedad de su Cuenta de AWS.

Para hacerlo, concede permiso para ejecutar cualquiera de las operaciones `Get*` o`List*`. No permite modificar ningún recurso compartido.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `ram`: permite a las entidades principales ver los detalles relativos a los recursos compartidos que son propiedad de la cuenta.

JSON

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

AWS política gestionada: AWSResource AccessManagerFullAccess

Puede asociar la política `AWSResourceAccessManagerFullAccess` a las identidades de IAM.

Esta política proporciona acceso administrativo completo para ver o modificar los recursos compartidos que son propiedad de su Cuenta de AWS.

Para ello, concede permiso para ejecutar cualquier operación de `ram`.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `ram`: permite a las entidades principales ver o modificar cualquier información relativa a los recursos compartidos que son propiedad de la Cuenta de AWS.

JSON

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

AWS política gestionada: AWSResource AccessManagerResourceShareParticipantAccess

Puede asociar la política `AWSResourceAccessManagerResourceShareParticipantAccess` a las identidades de IAM.

Esta política proporciona a los directores la posibilidad de aceptar o rechazar los recursos compartidos con ella y de ver los detalles sobre estos recursos compartidos. Cuenta de AWS No permite modificar esos recursos compartidos.

Para ello, concede permiso para ejecutar algunas operaciones de `ram`.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `ram`: permite a las entidades principales aceptar o rechazar invitaciones a recursos compartidos y ver los detalles relativos a los recursos compartidos que se comparten con la cuenta.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "ram:AcceptResourceShareInvitation",
                "ram:GetResourcePolicies",
                "ram:GetResourceShareInvitations",
                "ram:GetResourceShares",
                "ram:ListPendingInvitationResources",
                "ram:ListPrincipals",
                "ram:ListResources",
                "ram:RejectResourceShareInvitation"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS política gestionada: AWSResource AccessManagerServiceRolePolicy

La política AWS gestionada solo se `AWSResourceAccessManagerServiceRolePolicy` puede utilizar con la función vinculada al servicio para. AWS RAM No puede vincular, desvincular, modificar ni eliminar esta política.

Esta política proporciona acceso AWS RAM de solo lectura a la estructura de su organización. Al habilitar la integración entre AWS RAM y AWS Organizations, crea AWS RAM automáticamente un rol vinculado al servicio con el nombre AWSServiceRoleForResourceAccessManagerque el servicio

asume cuando necesita buscar información sobre su organización y sus cuentas, por ejemplo, cuando ve la estructura de la organización en la consola. AWS RAM

Para ello, concede permisos de solo lectura para ejecutar las operaciones `organizations:Describe` y `organizations:List` que proporcionan los detalles de la estructura y las cuentas de la organización.

Detalles de los permisos

Esta política incluye los siguientes permisos.

- `organizations`: permite a las entidades principales ver información sobre la estructura de la organización, incluidas las unidades organizativas, y las Cuentas de AWS que contienen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:ListAccounts",
                "organizations:ListAccountsForParent",
                "organizations:ListChildren",
                "organizations:ListOrganizationalUnitsForParent",
                "organizations:ListParents",
                "organizations:ListRoots"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowDeletionOfServiceLinkedRoleForResourceAccessManager",
            "Effect": "Allow",
            "Action": [
                "iam:DeleteRole"
            ],
            "Resource": [
```

```
                "arn:aws:iam::*:role/aws-service-role/ram.amazonaws.com/*"
            ]
        }
    ]
}
```

AWS RAM actualizaciones de las políticas gestionadas AWS

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas AWS RAM desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del AWS RAM documento.

Cambio	Descripción	Fecha
AWS Resource Access Manager comenzó a rastrear los cambios	AWS RAM documentó sus políticas gestionadas existentes y comenzó a realizar un seguimiento de los cambios.	16 de septiembre de 2021

Uso de roles vinculados a servicios para AWS RAM

AWS Resource Access Manager usa roles vinculados al AWS Identity and Access Management servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente al servicio. AWS RAM Los roles vinculados al servicio están predefinidos AWS e incluyen todos los permisos AWS RAM necesarios para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración AWS RAM , ya que no es necesario añadir manualmente los permisos necesarios. AWS RAM define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS RAM puede asumir sus funciones vinculadas al servicio. Los permisos definidos incluyen tanto una política de confianza como una política de permisos, y esta última no se puede vincular a ninguna otra entidad de IAM.

Para obtener información acerca de otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado a un servicio. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de roles vinculados al servicio para AWS RAM

AWS RAM utiliza el rol vinculado al servicio denominado `AWSServiceRoleForResourceAccessManager` cuando habilitas el uso compartido con. AWS Organizations Este rol otorga permisos al AWS RAM servicio para ver los detalles de la organización, como la lista de cuentas de los miembros y las unidades organizativas en las que se encuentra cada cuenta.

Este rol vinculado a servicio confía en el siguiente servicio para asumir el rol:

- `ram.amazonaws.com`

La política de permisos de rol denominada AWSResource AccessManagerServiceRolePolicy está asociada a este rol vinculado al servicio y permite AWS RAM realizar las siguientes acciones en los recursos especificados:

- Acciones: acciones de solo lectura que permiten recuperar detalles sobre la estructura de la organización. Para ver la lista completa de acciones, puede ver la política en la consola de IAM:. AWSResourceAccessManagerServiceRolePolicy

Para que un director active el AWS RAM uso compartido en su organización, ese director (una entidad de IAM, como un usuario, un grupo o un rol) debe tener permiso para crear un rol vinculado al servicio. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Crear un rol vinculado a un servicio para AWS RAM

No necesita crear manualmente un rol vinculado a servicios. Cuando activas el uso AWS RAM compartido dentro de tu organización Consola de administración de AWS, o cuando ejecutas el rol EnableSharingWithAwsOrganizationen tu cuenta mediante una API AWS CLI o una AWS API, se AWS RAM crea automáticamente el rol vinculado al servicio.

Llame a `enable-sharing-with-aws-organizations` para crear el rol vinculado al servicio en su cuenta.

Si eliminas este rol vinculado al servicio, ya AWS RAM no tendrá permisos para ver los detalles de la estructura de tu organización.

Edición de un rol vinculado a un servicio para AWS RAM

AWS RAM no permite editar el rol vinculado al AWSResource AccessManagerServiceRolePolicy servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Edición de un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminar un rol vinculado a un servicio para AWS RAM

Puede utilizar la consola de IAM AWS CLI o la AWS API para eliminar manualmente el rol vinculado al servicio.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al servicio. `AWSResourceAccessManagerServiceRolePolicy` Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones compatibles con los roles vinculados al servicio AWS RAM

AWS RAM admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte Regiones y puntos de conexión de AWS en la Referencia general de Amazon Web Services.

Ejemplos de políticas de IAM para AWS RAM

En este tema se incluyen ejemplos de políticas de IAM AWS RAM que muestran cómo compartir recursos y tipos de recursos específicos y cómo restringir el uso compartido.

Ejemplos de políticas de IAM

- Ejemplo 1: Permitir el uso compartido de recursos específicos
- Ejemplo 2: Permitir el uso compartido de tipos de recursos específicos
- Ejemplo 3: Restringir el uso compartido con fuentes externas Cuentas de AWS

Ejemplo 1: Permitir el uso compartido de recursos específicos

Puede usar una política de permisos de IAM para restringir las entidades principales y asociar solo determinados recursos a recursos compartidos.

Por ejemplo, la siguiente política permite restringir las entidades principales para que compartan la regla de solucionador con el nombre de recurso de Amazon (ARN) especificado. El operador `StringEqualsIfExists` permite una solicitud si la solicitud no incluye un parámetro `ResourceArn` o, si incluye dicho parámetro, si su valor coincide exactamente con el ARN especificado.

Para obtener más información sobre cuándo y por qué usar `...IfExists` operadores, consulte... IfExists condicione los operadores en la Guía del usuario de IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "StringEqualsIfExists": {
                "ram:ResourceArn": "arn:aws:route53resolver:us-
west-2:123456789012:resolver-rule/rslvr-rr-5328a0899aexample"
            }
        }
    }]
}
```

Ejemplo 2: Permitir el uso compartido de tipos de recursos específicos

Puede usar una política de IAM para restringir las entidades principales y asociar solo determinados tipos de recursos a los recursos compartidos.

Las acciones, `AssociateResourceShare` y `CreateResourceShare`, pueden aceptar entidades principales y `resourceArns` como parámetros de entrada independientes. Por lo tanto, AWS RAM autoriza cada principal y cada recurso de forma independiente, por lo que puede haber varios contextos de solicitud. Esto significa que cuando una entidad principal se asocia a un recurso compartido de AWS RAM , la clave de condición de `ram:RequestedResourceType` no está presente en el contexto de la solicitud. Del mismo modo, cuando se asocia un recurso a un recurso compartido de AWS RAM , la clave de condición de `ram:Principal` no está presente en el contexto de la solicitud. Por lo tanto, para permitir `AssociateResourceShare` y

`CreateResourceShare` asociar los principales al AWS RAM recurso compartido, puede utilizar el `Null` operador de condición.

Por ejemplo, la siguiente política solo permite a las entidades principales compartir reglas de Amazon Route 53 Resolver y les permite asociar cualquier entidad principal a ese recurso compartido.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Sid": "AllowOnlySpecificResourceType",
        "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "ram:RequestedResourceType": "route53resolver:ResolverRule"
            }
        }
    },
    {
    "Sid": "AllowAssociatingPrincipals",
     "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "Null": {
                "ram:Principal": "false"
             }
        }
    }
  ]
}
```

Ejemplo 3: Restringir el uso compartido con fuentes externas Cuentas de AWS

Puede utilizar una política de IAM para evitar que los directores compartan recursos con personas Cuentas de AWS ajenas a su AWS organización.

Por ejemplo, la siguiente política de IAM impide que los directores agreguen recursos externos Cuentas de AWS a los recursos compartidos.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": "ram:CreateResourceShare",
        "Resource": "*",
        "Condition": {
            "Bool": {
                "ram:RequestedAllowsExternalPrincipals": "false"
            }
        }
    }]
}
```

Ejemplos de políticas de control de servicios para AWS Organizations y AWS RAM

AWS RAM admite políticas de control de servicios (SCPs). SCPs son políticas que se adjuntan a los elementos de una organización para gestionar los permisos dentro de esa organización. Un SCP se aplica a todos los elementos Cuentas de AWS incluidos en el elemento al que se adjunta el SCP. SCPs ofrezca un control central sobre el máximo de permisos disponibles para todas las cuentas de su organización. Pueden ayudarlo a garantizar que se Cuentas de AWS mantenga dentro de las pautas de control de acceso de su organización. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations .

Requisitos previos

Para usarlo SCPs, primero debe hacer lo siguiente:

- Habilitar todas las características en la organización. Para obtener más información, consulte Habilitar todas las características en la organización en la Guía del usuario de AWS Organizations .

- Habilite SCPs su uso en su organización. Para obtener más información, consulte Habilitar y deshabilitar tipos de políticas en la Guía del usuario de AWS Organizations .
- Cree lo SCPs que necesita. Para obtener más información sobre la creación SCPs, consulte Creación y actualización SCPs en la Guía del AWS Organizations usuario.

Ejemplo de políticas de control de servicios

Contenido

Los siguientes ejemplos le muestran cómo puede controlar varios aspectos del uso compartido de recursos en una organización.

Ejemplo 1: Impedir la posibilidad de compartir externamente

La siguiente SCP evita que los usuarios puedan crear recursos compartidos que permitan compartir con entidades principales externas a la organización del usuario que comparte.

AWS RAM autoriza APIs por separado para cada principal y recurso enumerados en la convocatoria.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:UpdateResourceShare"
```

```
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "ram:RequestedAllowsExternalPrincipals": "true"
                }
            }
        }
    ]
}
```

Ejemplo 2: Impedir que los usuarios acepten invitaciones a recursos compartidos desde cuentas externas a la organización

La siguiente SCP impide que cualquier entidad principal de una cuenta afectada acepte una invitación para usar un recurso compartido. Los recursos compartidos que se comparten con otras cuentas de la misma organización que la cuenta que los comparte no generan invitaciones y, por lo tanto, no se ven afectados por esta SCP.

JSON

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

Ejemplo 3: Permitir que determinadas cuentas compartan tipos de recursos específicos

La siguiente SCP permite que solo las cuentas 111111111111 y 222222222222 creen nuevos recursos compartidos que compartan listas de prefijos de Amazon EC2 o listas de prefijos asociadas con recursos compartidos existentes.

AWS RAM autoriza APIs por separado para cada principal y recurso enumerados en la llamada.

El operador `StringEqualsIfExists` permite una solicitud si la solicitud no incluye un parámetro de tipo de recurso o, si incluye ese parámetro, si su valor coincide exactamente con el tipo de recurso especificado. Si incluye una entidad principal, debe tener `...IfExists`.

Para obtener más información sobre cuándo y por qué usar `...IfExists` operadores, consulte... IfExists condicione los operadores en la Guía del usuario de IAM.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalAccount": [
                        "111111111111",
                        "222222222222"
                    ]
                },
                "StringEqualsIfExists": {
                    "ram:RequestedResourceType": "ec2:PrefixList"
                }
            }
        }
    ]
}
```

Ejemplo 4: Impedir que se comparta con toda la organización o con unidades organizativas

La siguiente SCP impide que los usuarios creen recursos compartidos que compartan recursos con toda una organización o con cualquier unidad organizativa. Los usuarios pueden compartir con personas Cuentas de AWS de la organización o con roles o usuarios de IAM.

AWS RAM autoriza APIs por separado para cada principal y recurso enumerados en la llamada.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ram:Principal": [
                        "arn:aws:organizations::*:organization/*",
                        "arn:aws:organizations::*:ou/*"
                    ]
                }
            }
        }
    ]
}
```

Ejemplo 5: Permitir compartir solo con determinadas entidades principales

La siguiente SCP de ejemplo permite a los usuarios compartir recursos solo una organización `o-12345abcdef,`, una unidad organizativa `ou-98765fedcba`, y una Cuenta de AWS `111111111111`.

Si utiliza un elemento `"Effect": "Deny"` con un operador de condición negada, como `StringNotEqualsIfExists`, la solicitud se seguirá denegando aunque la clave de condición no se encuentre presente. Utilice un operador de condición `Null` para comprobar si una clave de condición está ausente en el momento de la autorización.

AWS RAM autoriza APIs por separado para cada principal y recurso enumerados en la llamada.

JSON

```
{
```

```
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ram:AssociateResourceShare",
        "ram:CreateResourceShare"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "ram:Principal": [
            "arn:aws:organizations::123456789012:organization/o-12345abcdef",
            "arn:aws:organizations::123456789012:ou/o-12345abcdef/
ou-98765fedcba",
            "111111111111"
          ]
        },
        "Null": {
          "ram:Principal": "false"
        }
      }
    }
  ]
}
```

Ejemplo 6: Impedir que se compartan recursos si está activado RetainSharingOnAccountLeaveOrganization

El siguiente SCP impide que los usuarios creen o modifiquen recursos compartidos cuando la clave de `ram:RetainSharingOnAccountLeaveOrganization` condición está establecida en. `true`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare",
                "ram:DisassociateResourceShare"
            ],
```

```
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "ram:RetainSharingOnAccountLeaveOrganization": "true"
                }
            }
        }
    ]
}
```

Deshabilitar el uso compartido de recursos con AWS Organizations

Si anteriormente habilitaste el uso compartido con toda tu organización o unidades organizativas () AWS Organizations y ya no necesitas compartir recursos con toda tu organización o unidades organizativas (OUs), puedes inhabilitar el uso compartido. Si inhabilitas el uso compartido con AWS Organizations todas las organizaciones o se OUs eliminan de los recursos compartidos que has creado, estas pierden el acceso a los recursos compartidos. Las cuentas externas (las cuentas agregadas al recurso compartido mediante invitación) no se verán afectadas y seguirán asociadas al recurso compartido.

Para deshabilitar el uso compartido con AWS Organizations

1. Deshabilite el acceso de confianza para AWS Organizations utilizar el AWS Organizations disable-aws-service-access AWS CLI comando.

   ```
   $  aws organizations disable-aws-service-access --service-principal
    ram.amazonaws.com
   ```

   > **Important**
   >
   > Al deshabilitar el acceso de confianza a AWS Organizations, los directores de sus organizaciones se eliminan de todos los recursos compartidos y pierden el acceso a esos recursos compartidos.

2. Utilice la consola de IAM o las operaciones de la AWS CLI API de IAM para eliminar la función vinculada al AWSServiceRoleForResourceAccessManagerservicio. Para obtener más información, consulte Eliminación de un rol vinculado a un servicio en la Guía del usuario de IAM.

Registro y monitorización en AWS RAM

La supervisión es un aspecto importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de AWS RAM y sus soluciones de AWS. Debe recopilar datos de monitorización de todas las partes de su solución de AWS para poder depurar más fácilmente un error multipunto si se produce. AWS proporciona varias herramientas para monitorizar sus recursos de AWS RAM y responder a posibles incidentes:

Amazon EventBridge

Proporciona un flujo de eventos del sistema prácticamente en tiempo real que describen los cambios en los recursos de AWS. EventBridge habilita la computación basada en eventos automatizada, para que pueda escribir reglas que vigilan determinados eventos y desencadenan acciones automatizadas en otros servicios de AWS cuando estos eventos se producen. Para obtener más información, consulte Monitorización AWS RAM mediante EventBridge.

AWS CloudTrail

Captura las llamadas a la API y otros eventos relacionados que realiza la Cuenta de AWS o que se realizan en nombre de esta. Además, entrega los archivos de registro a un bucket de Amazon S3 especificado. También pueden identificar qué usuarios y cuentas han llamado a AWS, la dirección IP de origen de las llamadas y el momento en que se hicieron dichas llamadas. Para obtener más información, consulte Registrar llamadas a la AWS RAM API con AWS CloudTrail.

Monitorización AWS RAM mediante EventBridge

Con Amazon EventBridge, puedes configurar notificaciones automáticas para eventos específicos en AWS RAM. Los eventos de AWS RAM se envían casi EventBridge en tiempo real. Puede configurarlo EventBridge para supervisar los eventos e invocar los objetivos en respuesta a los eventos que indiquen cambios en sus recursos compartidos. Los cambios en un recurso compartido activan eventos tanto para el propietario del recurso compartido como para las entidades principales a las que se ha concedido acceso al recurso compartido.

Cuando se crea un patrón de eventos, el origen es `aws.ram`.

> **Note**
>
> Tenga cuidado al escribir código que depende de tales eventos. Los eventos no están garantizados, sino que se emiten en la medida de lo posible. Si se produce un error al AWS

RAM intentar emitir un evento, el servicio lo intentará varias veces más. Sin embargo, puede agotarse el tiempo de espera y provocar la pérdida de ese evento en concreto.

Para obtener más información, consulta la Guía del EventBridge usuario de Amazon.

Ejemplo: Alertar de errores en un recurso compartido

Imagine una situación en la que desea compartir reservas de capacidad de Amazon EC2 con otras cuentas de su organización. Esta sería una buena forma de reducir costos.

Sin embargo, si no cumple todos los requisitos previos para compartir una reserva de capacidad, es posible que se produzca un fallo silencioso a la hora de realizar las tareas asíncronas que implica compartir los recursos. Si la operación de compartir falla y los usuarios de otras cuentas intentan lanzar instancias con una de esas reservas de capacidad, Amazon EC2 actúa como si la reserva de capacidad estuviera llena y, en su lugar, lanza la instancia como una instancia bajo demanda. Esto se puede traducir en costos mayores de lo esperado.

Para supervisar los errores en el uso compartido de recursos, configura una EventBridge regla de Amazon que te avise cada vez que se produzca un error en un AWS RAM recurso compartido. El siguiente procedimiento de tutorial utiliza un tema del Amazon Simple Notification Service (SNS) para notificar a todos los suscriptores del tema cada vez que se EventBridge descubre un error al compartir recursos. Para obtener más información sobre Amazon SNS, consulte la Guía para desarrolladores de Amazon Simple Notification Service.

Para crear una regla que le notifique cuando se produzca un error al compartir recursos

1. Abre la EventBridge consola de Amazon.
2. En el panel de navegación, elija Reglas y, a continuación, en la lista Reglas, elija Crear regla.
3. Ingrese un nombre y una descripción opcional para la regla y, a continuación, elija Siguiente.
4. Desplácese hacia abajo, hasta el cuadro Patrón de eventos, y elija Patrones personalizados (editor JSON).
5. Copie y pegue el siguiente patrón de eventos:

```
{
  "source": ["aws.ram"],
  "detail-type": ["Resource Sharing State Change"],
  "detail": {
```

```
    "event": ["Resource Share Association"],
    "status": ["failed"]
  }
}
```

6. Elija Siguiente.
7. Para Destino 1, en Tipo de destino, elija Servicio de AWS.
8. En Seleccione un destino, elija Tema de SNS.
9. En Tema, elija el tema de SNS en el que desea publicar la notificación. Debe tratarse de un tema ya existente.
10. Elija Siguiente y, a continuación, otra vez Siguiente para revisar la configuración.
11. Cuando esté satisfecho con las opciones, elija Crear regla.
12. Al volver a la página Reglas, asegúrese de que la nueva regla esté marcada como Habilitada. Si es necesario, seleccione el botón de opción situado junto al nombre de la regla y, a continuación, elija Habilitar.

Mientras esa regla esté habilitada, cualquier AWS RAM recurso compartido que falle generará una alerta de SNS para los destinatarios del tema en el que publicaste.

También puede confirmar que las cuentas con las que ha compartido pueden acceder a las reservas de capacidad compartida. Para hacerlo, intente verlas en la consola de Amazon EC2 desde dichas cuentas.

Registrar llamadas a la AWS RAM API con AWS CloudTrail

AWS RAM está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en AWS RAM. CloudTrail captura todas las llamadas a la API AWS RAM como eventos. Las llamadas capturadas incluyen llamadas desde la AWS RAM consola y llamadas en código a las operaciones de la AWS RAM API. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3 que especifique, incluidos los eventos para ellos AWS RAM. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Usa la información recopilada por CloudTrail para determinar la solicitud que se realizó AWS RAM, la dirección IP solicitante, el solicitante, cuándo se realizó y detalles adicionales.

Para obtener más información al respecto CloudTrail, consulte la Guía del AWS CloudTrail usuario.

AWS RAM información en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en AWS RAM, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para mantener un registro continuo de eventos en la Cuenta de AWS, incluidos los eventos de AWS RAM, cree un registro de seguimiento. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando crea una ruta en la consola, la ruta se aplica a todas AWS las regiones. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para obtener más información, consulte los siguientes temas:

- Creando una ruta para tu Cuenta de AWS
- Servicio de AWS integraciones con registros CloudTrail
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas AWS RAM las acciones se registran CloudTrail y se documentan en la Referencia de la AWS RAM API. Por ejemplo, las llamadas a las acciones `CreateResourceShare`, `AssociateResourceShare`, `yEnableSharingWithAwsOrganization` generan entradas en los archivos de registro de CloudTrail.

Cada entrada de registro o evento contiene información que ayuda a determinar quién generó la solicitud.

- Cuenta de AWS credenciales raíz
- Credenciales de seguridad temporales de un rol AWS Identity and Access Management (IAM) o un usuario federado.
- Credenciales de seguridad a largo plazo de un usuario de IAM.
- Otro servicio AWS .

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Descripción de las entradas de los archivos de AWS RAM registro

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro para la `CreateResourceShare` acción.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "NOPIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/admin",
        "accountId": "111122223333",
        "accessKeyId": "BCDIOSFODNN7EXAMPLE",
        "userName": "admin"
    },
    "eventTime": "2018-11-03T04:23:19Z",
    "eventSource": "ram.amazonaws.com",
    "eventName": "CreateResourceShare",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.1.0",
    "userAgent": "aws-cli/1.16.2 Python/2.7.10 Darwin/16.7.0 botocore/1.11.2",
    "requestParameters": {
        "name": "foo"
    },
    "responseElements": {
        "resourceShare": {
            "allowExternalPrincipals": true,
            "name": "foo",
            "owningAccountId": "111122223333",
            "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/
EXAMPLE0-1234-abcd-1212-987656789098",
            "status": "ACTIVE"
        }
    },
```

```
    "requestID": "EXAMPLE0-abcd-1234-mnop-987654567876",
    "eventID": "EXAMPLE0-1234-abcd-hijk-543234565434",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Validación de conformidad para AWS Resource Access Manager

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. Para obtener más información sobre su responsabilidad de conformidad al utilizarlos Servicios de AWS, consulte AWS la documentación de seguridad.

Resiliencia en AWS Resource Access Manager

La infraestructura AWS global se basa en zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. 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 zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Seguridad de la infraestructura en AWS Resource Access Manager

Como servicio gestionado, AWS Resource Access Manager está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo

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

Utiliza las llamadas a la API AWS publicadas para acceder a AWS RAM través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Acceso AWS Resource Access Manager mediante un punto final de interfaz (AWS PrivateLink)

Puede usarlo AWS PrivateLink para crear una conexión privada entre su VPC y. AWS Resource Access Manager Puede acceder AWS RAM como si estuviera en su VPC, sin el uso de una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o Direct Connect una conexión. Las instancias de la VPC no necesitan direcciones IP públicas para acceder a AWS RAM.

Esta conexión privada se establece mediante la creación de un punto de conexión de interfaz alimentado por AWS PrivateLink. Creamos una interfaz de red de punto de conexión en cada subred habilitada para el punto de conexión de interfaz. Se trata de interfaces de red administradas por el solicitante que sirven como punto de entrada para el tráfico destinado a AWS RAM.

Para obtener más información, consulte Acceso a los Servicios de AWS a través de AWS PrivateLink en la Guía de AWS PrivateLink .

Consideraciones sobre AWS RAM

Antes de configurar un punto final de interfaz para AWS RAM, consulte las consideraciones de la AWS PrivateLink guía.

AWS RAM permite realizar llamadas a todas sus acciones de API a través del punto final de la interfaz.

Se admiten las políticas de puntos finales de VPC. AWS RAM De forma predeterminada, se concede acceso completo a AWS RAM a través del punto de conexión de interfaz.

Cree un punto final de interfaz para AWS RAM

Puede crear un punto final de interfaz para AWS RAM usar la consola de Amazon VPC o AWS Command Line Interface ()AWS CLI. Para obtener más información, consulte Creación de un punto de conexión de interfaz en la Guía de AWS PrivateLink .

Cree un punto final de interfaz para AWS RAM usar el siguiente nombre de servicio:

```
com.amazonaws.region.ram
```

Si habilita DNS privado para el punto de conexión de interfaz, puede realizar solicitudes a la API para AWS RAM usando su nombre de DNS predeterminado para la región. Por ejemplo, `ram.us-east-1.amazonaws.com`.

Creación de una política de puntos de conexión para el punto de conexión de interfaz

Una política de punto de conexión es un recurso de IAM que puede adjuntar al punto de conexión de su interfaz. La política de punto final predeterminada permite el acceso total a AWS RAM través del punto final de la interfaz. Para controlar el acceso permitido AWS RAM desde su VPC, adjunte una política de punto final personalizada al punto final de la interfaz.

Una política de punto de conexión especifica la siguiente información:

- Las entidades principales que pueden llevar a cabo acciones (Cuentas de AWS, usuarios de IAM y roles de IAM).
- Las acciones que se pueden realizar.
- El recurso en el que se pueden realizar las acciones.

Para obtener más información, consulte Control del acceso a los servicios con políticas de punto de conexión en la Guía del usuario de AWS PrivateLink .

Ejemplo: política de puntos finales de VPC para acciones AWS RAM

El siguiente es un ejemplo de una política de un punto de conexión personalizado. Al adjuntar esta política al punto final de la interfaz, se concede acceso a las AWS RAM acciones enumeradas a todos los principales de todos los recursos.

JSON

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

Solución de problemas con AWS RAM

Usa la información de esta sección de la guía como ayuda para diagnosticar y solucionar problemas comunes cuando trabajas con AWS Resource Access Manager (AWS RAM).

Temas

Error: «El ID de tu cuenta no existe en una AWS organización»

Escenario

Cuando intentas compartir un recurso con cuentas o unidades organizativas (OUs) de tu AWS organización, aparece el error «Tu ID de cuenta no existe en una organización».

Causa

Este error puede producirse si el rol vinculado al servicio AWSServiceRoleForResourceAccessManagerno se crea correctamente al activar la integración entre y AWS Resource Access Manager . AWS Organizations

Solución

Para volver a crear el rol vinculado al servicio requerido, lleve a cabo los siguientes pasos para desactivar la integración y luego volver a activarla.

> **Important**
>
> Al deshabilitar el acceso de confianza a AWS Organizations, los directores de la organización se eliminan de todos los recursos compartidos y pierden el acceso a esos recursos compartidos.

1. Inicie sesión en la cuenta de administración de su organización con un rol o usuario de IAM que disponga de permisos administrativos.
2. Diríjase a la página de servicios de la AWS Organizations consola.
3. Seleccione RAM.
4. Seleccione Deshabilitar el acceso de confianza.
5. Navegue hasta la página de configuración de la AWS RAM consola.
6. Selecciona la casilla Habilitar el uso compartido con y AWS Organizations, a continuación, selecciona Guardar configuración.

Ahora deberías poder utilizarlos AWS RAM para compartir tus recursos con las cuentas y OUs la organización.

Error: "AccessDeniedException»

Escenario

Obtiene una excepción de acceso denegado al intentar compartir un recurso o ver un recurso compartido.

Causa

Puede obtener este error si intenta crear un recurso compartido cuando sin disponer de los permisos necesarios. Esto puede deberse a la insuficiencia de permisos en las políticas asociadas a su entidad principal AWS Identity and Access Management (IAM). También puede ocurrir debido a las restricciones impuestas por una política de control de AWS Organizations servicios (SCP) que le afecten. Cuenta de AWS

Solución

Para proporcionar acceso, añada permisos a sus usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center .
- Usuarios gestionados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones descritas en Creación de un rol para un proveedor de identidad de terceros (federación) en la Guía del usuario de IAM.
- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o agregue un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Para resolver el error, debe asegurarse de que los permisos se concedan mediante instrucciones `Allow` en la política de permisos utilizada por la entidad principal que realiza la solicitud. Además, la organización no debe bloquear los permisos SCPs.

Para crear un recurso compartido, necesita los dos permisos siguientes:

- `ram:CreateResourceShare`
- `ram:AssociateResourceShare`

Para ver un recurso compartido, necesita el siguiente permiso:

- `ram:GetResourceShares`

Para adjuntar permisos a un recurso compartido, necesita el siguiente permiso:

- *`resourceOwningService`*`:`*`PutPolicyAction`*

  Esto es un marcador de posición. Debe sustituirlo por el permiso PutPolicy «» (o equivalente) del servicio propietario del recurso que desea compartir. Por ejemplo, si desea compartir una regla de solucionador de Route 53, el permiso necesario sería: `route53resolver:PutResolverRulePolicy`. Si desea permitir la creación de un recurso

compartido que contenga varios tipos de recursos, debe incluir el permiso correspondiente para cada tipo de recurso que desea permitir.

En el siguiente ejemplo se muestra el aspecto que tendría una política de permisos de IAM de este tipo.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ram:CreateResourceShare",
                "ram:AssociateResourceShare",
                "ram:GetResourceShares",
                "resourceOwningService:PutPolicyAction"
            ],
            "Resource": "*"
        }
    ]
}
```

Error: «UnknownResourceException»

Escenario

Obtiene uno de los siguientes errores:

- «CannotCreateResourceShare: UnknownResourceException: OrganizationalUnit ou- no se *xxxx* pudo encontrar»
- «CannotUpdateResourceShare: UnknownResourceException: no se *xxxx* pudo encontrar OrganizationalUnit ou».

Causa

Estos errores pueden producirse si habilita la integración entre AWS RAM y AWS Organizations mediante la consola Organizations o la API Organizations Enable AWSService Access en lugar de utilizar la AWS RAM consola. Cuando habilita la integración utilizando la consola o la API de Organizations, el servicio no crea el rol `AWSServiceRoleForResourceAccessManager` en su cuenta. Ese rol es necesario para acceder a la información relativa a su organización. Como el rol no se creó, no AWS RAM puedes acceder a los detalles de las cuentas o unidades organizativas (OUs) de tu organización.

Solución

Para resolver el problema, desactiva la integración entre AWS RAM y AWS Organizations. A continuación, vuelva a activarla llamando a la operación de AWS RAM EnableSharingWithAwsOrganizationAPI o utilizando la Consola de administración de AWS para realizar los siguientes pasos.

> **Important**
>
> Al deshabilitar el acceso de confianza a AWS Organizations, los directores de la organización se eliminan de todos los recursos compartidos y pierden el acceso a esos recursos compartidos.

1. Inicie sesión en la cuenta de administración de su organización con un rol o usuario de IAM que disponga de permisos administrativos.
2. Diríjase a la página de servicios de la AWS Organizations consola.
3. Seleccione RAM.
4. Seleccione Deshabilitar el acceso de confianza.
5. Navegue hasta la página de configuración de la AWS RAM consola.
6. Selecciona la casilla Habilitar el uso compartido con y AWS Organizations, a continuación, selecciona Guardar configuración.

Ahora deberías poder utilizarlos AWS RAM para compartir tus recursos con las cuentas y OUs la organización.

Errores al intentar compartir con cuentas externas a mi organización

Escenario

Obtiene uno de los siguientes errores al intentar compartir recursos con cuentas externas a su organización:

- "No puede compartir el recurso fuera de su organización".
- «El recurso que intentas compartir solo se puede compartir dentro de tu AWS organización. »
- «InvalidParameterException: El ID de la cuenta principal no está en su AWS organización. No tiene permiso para añadir Cuentas de AWS a un recurso compartido".
- «OperationNotPermittedException: El recurso que intenta compartir solo se puede compartir dentro de su AWS organización. »

Posibles causas y soluciones

Algunos tipos de recursos solo se pueden compartir con cuentas de la misma organización

Algunos tipos de recursos no se pueden compartir con ninguna cuenta que no sea miembro de esa organización. Un ejemplo de tipo de recurso con esta restricción son las conexiones privadas virtuales (VPC) que forman parte de Amazon Elastic Compute Cloud (Amazon EC2).

Para comprobar si puede compartir un determinado tipo de recurso con cuentas y entidades principales externas a su organización, consulte Recursos de AWS que se pueden compartir.

El rol vinculado al servicio no se creó correctamente

Este problema puede producirse si el rol vinculado al servicio `AWSServiceRoleForResourceAccessManager` no se creó correctamente al activar la integración entre y AWS RAM . AWS Organizations

Si recibe uno de estos errores al intentar compartir un recurso con una cuenta que forma parte de su organización, siga estos pasos para eliminar y volver a crear el rol vinculado al servicio.

> **Important**
>
> Al deshabilitar el acceso de confianza a AWS Organizations, los directores de la organización se eliminan de todos los recursos compartidos y pierden el acceso a esos recursos compartidos.

1. Inicie sesión en la cuenta de administración de su organización con un rol o usuario de IAM que disponga de permisos administrativos.
2. Diríjase a la página de servicios de la AWS Organizations consola.
3. Seleccione RAM.
4. Seleccione Deshabilitar el acceso de confianza.
5. Navegue hasta la página de configuración de la AWS RAM consola.
6. Selecciona la casilla Habilitar el uso compartido con y AWS Organizations, a continuación, selecciona Guardar configuración.

No puede ver los recursos compartidos en la cuenta de destino

Escenario

Los usuarios no pueden ver recursos que creen que se han compartido con ellos desde otras Cuentas de AWS.

Posibles causas y soluciones

AWS Organizations La opción Compartir con se activó mediante Organizations en lugar de AWS RAM

Si AWS Organizations se activó mediante Organizations en lugar de hacerlo AWS RAM, se produce un error al compartir dentro de la organización. Para comprobar si esta es la causa del problema, vaya a la página Configuración de la consola de AWS RAM y compruebe que la casilla Habilitar el uso compartido con AWS Organizations esté seleccionada.

- Si la casilla de verificación está seleccionada, esta no es la causa.
- Si la casilla de verificación no está seleccionada, esta podría ser la causa. No seleccione la casilla de verificación aún. Lleve a cabo los siguientes pasos para corregir la situación.

> **Important**
>
> Al deshabilitar el acceso de confianza a AWS Organizations, los directores de la organización se eliminan de todos los recursos compartidos y pierden el acceso a esos recursos compartidos.

1. Inicie sesión en la cuenta de administración de su organización con un rol o usuario de IAM que disponga de permisos administrativos.
2. Diríjase a la página de servicios de la AWS Organizations consola.
3. Seleccione RAM.
4. Seleccione Deshabilitar el acceso de confianza.
5. Navegue hasta la página de configuración de la AWS RAM consola.
6. Selecciona la casilla Habilitar el uso compartido con y AWS Organizations, a continuación, selecciona Guardar configuración.

Es posible que tenga que actualizar el recurso compartido y especificar las cuentas o unidades organizativas de la organización con las que desea compartir.

El recurso compartido no especifica esta cuenta como entidad principal

En la Cuenta de AWS que se creó el recurso compartido, visualiza el recurso compartido en la AWS RAM consola. Asegúrese de que la cuenta que no puede acceder a los recursos figura como Entidad principal. Si no es así, actualice el recurso compartido para añadir la cuenta como entidad principal.

El rol o el usuario de la cuenta no tienen los permisos mínimos necesarios

Cuando comparte un recurso de la cuenta A con otra cuenta B, los roles y los usuarios de la cuenta B no obtienen acceso automáticamente a los recursos del recurso compartido. El administrador de la cuenta B primero debe conceder permiso a los roles y usuarios de IAM de la cuenta B que necesiten acceder al recurso. A modo de ejemplo, la siguiente política muestra cómo se puede conceder acceso de solo lectura a roles y usuarios de la cuenta B para un recurso desde la cuenta A. La política especifica el recurso por su nombre de recurso de Amazon (ARN).

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "ram:Get*",
                "ram:List*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:<service>:us-east-1:<Account-A-ID>:<resource-
id>"
        }
    ]
}
```

El recurso está en una configuración Región de AWS diferente a la configuración actual de la consola

AWS RAM es un servicio regional. Los recursos existen en una región específica y Región de AWS, para verlos, Consola de administración de AWS deben estar configurados para ver los recursos de esa región.

El Región de AWS elemento al que la consola está accediendo actualmente se muestra en la esquina superior derecha de la consola. Para cambiarla, seleccione el nombre de la región actual y, en el menú desplegable, elija la región cuyos recursos desea ver.

Error: Se ha superado el límite

Escenario

Al intentar compartir recursos, aparece el mensaje «Has alcanzado el límite de recursos que puedes compartir ResourceShareLimitExceededException» o «».

Causa

Estos errores se producen cuando alcanzas el número máximo de recursos que puedes compartir mediante el AWS RAM servicio o con el Servicio de AWS que se creó el recurso que estás intentando compartir. Esta cuota (antes denominada "límite") puede afectar tanto a la cuenta que comparte el recurso como a la cuenta con la que se comparte.

Solución

1. Para ver tus cuotas, en el Cuenta de AWS lugar donde aparece el error, accede a una de las siguientes páginas, en función del tipo de cuota que estés alcanzando:
   - La página AWS RAM de la consola de Service Quotas
   - La página del Servicio de AWS a cuyos recursos afecta la cuota
2. Desplácese hacia abajo y seleccione la cuota que corresponda.
3. Seleccione la opción Solicitar aumento de cuota, si está disponible para esta cuota.
4. Ingrese un nuevo valor para cuota y seleccione Solicitar.
5. La solicitud aparece en la página Historial de solicitudes de cuota, donde puede comprobar el estado de la solicitud hasta su finalización.

La otra cuenta de mi organización nunca recibe una invitación

Escenario

Cuando comparte recursos con otra cuenta de la misma organización administrada por AWS Organizations, esta no recibe invitaciones.

Causa

Este es el comportamiento esperado si su cuenta tiene activada la opción de compartir dentro de la organización de AWS.

Cuando esta opción está activada y comparte con otra cuenta de su organización, no se envían invitaciones ni es necesaria su aceptación. Todas las cuentas de la organización a las que haga referencia como entidades principales en el recurso compartido pueden empezar a acceder inmediatamente a los recursos del recurso compartido.

Si tu cuenta no ha activado el uso compartido dentro de la AWS organización, cuando compartas con otras cuentas, aunque estén en la misma AWS organización, se tratarán como cuentas independientes. Se envían invitaciones, que deben aceptarse para que los usuarios puedan acceder a los recursos de los recursos compartidos.

No puede compartir una subred de VPC

Escenario

Cuando intentas compartir una subred de VPC con otra cuenta, la operación de uso compartido se realiza correctamente. AWS RAM Sin embargo, la cuenta consumidora aparece `LIMIT EXCEEDED` para ese recurso en la consola. AWS RAM

Causa

Algunos tipos de recursos individuales tienen restricciones específicas del servicio, independientes de las restricciones impuestas por ellos. AWS RAM Algunas de esas restricciones pueden impedir de manera efectiva el uso compartido, incluso si no se ha alcanzado ninguna de las restricciones en AWS RAM. Un ejemplo de estas restricciones son los límites. Amazon Virtual Private Cloud (Amazon VPC) limita el número de subredes que puede compartir con otra cuenta individual. Si intenta compartir una subred con una cuenta consumidora que ya contiene el número máximo de subredes, esa cuenta consumidora muestra `LIMIT EXCEEDED` en la consola para dicho recurso. Para obtener más información sobre este límite, consulte Cuotas de Amazon VPC: uso compartido de VPC en la Guía del usuario de Amazon Virtual Private Cloud.

Para solucionar este problema, compruebe primero si hay otros recursos compartidos que puedan estar compartiendo el recurso especificado con la cuenta afectada, y elimine los recursos compartidos que tal vez ya no necesite. También puede solicitar el aumento de un límite que se pueda ajustar. Para solicitar un aumento del límite, use la Consola de Service Quotas.

> **Note**
>
> AWS RAM no detecta automáticamente los cambios en el aumento del límite. Debe volver a asociar el recurso o la entidad principal al recurso compartido para que RAM detecte el cambio.

Cuotas de servicio de AWS RAM

Su Cuenta de AWS tiene los siguientes límites relativos a AWS Resource Access Manager (AWS RAM). Puede solicitar un incremento de algunos de estos límites. Para solicitar un incremento del límite, póngase en contacto con Soporte.

Note

Las siguientes definiciones se aplican a la descripción de las siguientes cuotas:

- Recurso: elemento individual creado por Servicio de AWS que se desea compartir, como un bucket de Amazon S3 o una instancia de Amazon EC2. Cada recurso al que se hace referencia en un recurso compartido cuenta como uno a efectos de esta cuota. Si comparte el mismo recurso en tres recursos compartidos diferentes, el recuento de esta cuota aumentará en tres.
- Recurso compartido: contenedor creado por AWS RAM que se puede usar para compartir recursos. Cada recurso compartido, independientemente del número de recursos que contenga, cuenta como uno a efectos de la cuota.
- Entidad principal compartida: identificador que ha asociado a un recurso compartido. Puede tratarse de un rol o un usuario de AWS Identity and Access Management (IAM), un identificador de Cuenta de AWS, una unidad organizativa o toda una organización. Cada entidad principal compartida a la que se hace referencia en un recurso compartido cuenta como uno a efectos de la cuota de uso. Si comparte con toda una organización haciendo referencia al ID de esta, solo cuenta como uno a efectos de esta cuota.
- Permiso administrado por el cliente: permisos administrados que se crean para abordar casos de uso específicos utilizando un acceso basada en el privilegio mínimo para administrar el uso de los recursos compartidos.

Recurso	Límite predeterminado
Número máximo de recursos compartidos por Región de AWS	25 000
Número máximo de asociaciones de recursos por recurso compartido	5 000

Recurso	Límite predeterminado
Número máximo de asociaciones de entidades principales por recurso compartido	5 000
Número máximo de permisos administrados por el cliente	1500
Número máximo de permisos administrados por el cliente por tipo de recurso	10
Número máximo de versiones por permiso administrado por el cliente	5
Número máximo de asociaciones de recursos en todos los recursos compartidos de una Región de AWS **Note** Cada recurso incluido en un recurso compartido cuenta a efectos de este límite. Si un recurso está incluido en 10 recursos compartidos diferentes, cuenta como 10 a efectos de dicho límite.	25 000

Recurso	Límite predeterminado
Número máximo de asociaciones de entidades principales en todos los recursos compartidos de una Región de AWS **Note** Cada entidad principal incluida en un recurso compartido cuenta a efectos de este límite. Si una entidad principal está incluida en 10 recursos compartidos diferentes, cuenta como 10 a efectos de dicho límite.	25 000
Número máximo de invitaciones pendientes por cuenta de uso compartido • Esta cuota se aplica únicamente a las cuentas de envío que comparten con cuentas que no forman parte de la misma AWS Organizations. • No existe una cuota que limite el número de invitaciones pendientes que puede tener una cuenta de recepción. • Las invitaciones no se utilizan cuando se comparte entre cuentas que forman parte de la misma AWS Organizations y se ha activado el uso compartido de recursos dentro de dicha AWS Organizations.	250

Uso de AWS RAM con un AWS SKD

Los kits de desarrollo de software (SDK) de AWS están disponibles en muchos lenguajes de programación de uso común. Cada SDK proporciona una API, ejemplos de código y documentación que facilitan a los desarrolladores la creación de aplicaciones en el lenguaje de su preferencia.

Documentación de SDK	Ejemplos de código
AWS SDK para C++	AWS SDK para C++ Ejemplos de código de la
AWS SDK para Go	AWS SDK para Go Ejemplos de código de la
AWS SDK para Java	AWS SDK para Java Ejemplos de código de la
AWS SDK para JavaScript	AWS SDK para JavaScript Ejemplos de código de la
AWS SDK para .NET	AWS SDK para .NET Ejemplos de código de la
AWS SDK para PHP	AWS SDK para PHP Ejemplos de código de la
AWS SDK para Python (Boto3)	AWS SDK para Python (Boto3) Ejemplos de código de la
AWS SDK para Ruby	AWS SDK para Ruby Ejemplos de código de la

Ejemplo de disponibilidad

¿No puede encontrar lo que necesita? Solicite un ejemplo de código con el enlace de comentarios.

Historial de documentos de la Guía AWS RAM del usuario

En la siguiente tabla se describen las adiciones importantes a la AWS Resource Access Manager documentación. También actualizamos la documentación para abordar los comentarios que se nos hacen llegar.

Para recibir notificaciones sobre estas actualizaciones, puede suscribirse a la AWS RAM fuente RSS.

Cambio	Descripción	Fecha
Se agregó soporte para compartir CloudFront los recursos de Amazon	Ahora puede compartir Amazon CloudFront VPC Origins con otras personas de su Cuentas de AWS organización.	6 de octubre de 2025
Compatibilidad ampliada para compartir recursos de Administración de facturación y costos	Ahora puede compartir los paneles de Billing and Cost Management con otras personas Cuentas de AWS o con AWS RAM su organización.	19 de agosto de 2025
Se agregó soporte para compartir recursos AWS Cloud Map	Ahora puede compartir AWS Cloud Map espacios de nombres con otros miembros de su Cuentas de AWS organización.	14 de agosto de 2025
Compatibilidad ampliada para compartir recursos del Controlador de recuperación de aplicaciones de Amazon (ARC)	Ahora puede compartir los planes de Amazon Application Recovery Controller (ARC) con otras personas Cuentas de AWS o con las de su organización AWS RAM.	31 de julio de 2025

Se agregó soporte para compartir Oracle Database@ AWS recursos	Ahora puede compartir la infraestructura de Oracle Database@AWS Exadata y las redes ODB con otros miembros de su organización Cuentas de AWS .	30 de junio de 2025
Compatibilidad ampliada para compartir recursos de aprobación de varias partes	Ahora puede compartir los equipos de aprobación y aprobación multipartitos con otros miembros de su organización Cuentas de AWS o dentro de ella.	17 de junio de 2025
Se agregó soporte para compartir los recursos de Amazon SageMaker AI	Ahora puede utilizarlas AWS RAM para compartir las aplicaciones de Amazon SageMaker AI Partner con otras Cuentas de AWS perso nas y con su organización.	6 de junio de 2025
Se agregó soporte para compartir AWS Network Firewall recursos	Ahora puede utilizarlos AWS RAM para compartir AWS Network Firewall firewalls con otras personas Cuentas de AWS y con su organización.	28 de mayo de 2025
Se agregó soporte para compartir recursos AWS Systems Manager	Puede compartir una política de AWS Systems Manager denegación de acceso con otras organizaciones Cuentas de AWS o con las suyas. AWS RAM	30 de abril de 2025

Se agregó soporte para compartir recursos AWS CodeConnections	Ahora puede compartir conexiones AWS CodeConnections de código con otras personas Cuentas de AWS o dentro de su organización.	5 de marzo de 2025
Se agregó soporte para compartir AWS Billing recursos	Ahora puede compartir AWS Billing vistas con otros miembros Cuentas de AWS de su organización.	20 de diciembre de 2024
Compatibilidad ampliada para compartir configuraciones de recursos de Amazon VPC Lattice	Ahora puede compartir las configuraciones de recursos de Amazon VPC Lattice con otras Cuentas de AWS.	1 de diciembre de 2024
Compatibilidad ampliada para compartir recursos de Amazon API Gateway	Ahora puede compartir los nombres de dominio de API Gateway con otras personas Cuentas de AWS o dentro de su organización.	21 de noviembre de 2024
Compatibilidad ampliada para compartir recursos de Amazon VPC	Ahora puede compartir grupos de seguridad de Amazon VPC con otros miembros de su organización Cuentas de AWS o dentro de ella.	30 de octubre de 2024
Se agregó soporte para compartir recursos AWS End User Messaging SMS	Puede compartir AWS End User Messaging SMS recursos con otras organizaciones Cuentas de AWS o con las suyas AWS RAM.	24 de septiembre de 2024

AWS PrivateLink	Con AWS PrivateLink for AWS RAM, puede conectarse directamente a la RAM mediante un punto final de interfaz en su nube privada virtual (VPC).	9 de septiembre de 2024
Se agregó soporte para compartir AWS Backup	Puede compartir bóvedas aisladas de forma lógica en toda Cuentas de AWS la organización o dentro de ella.	7 de agosto de 2024
Compatibilidad ampliada para compartir recursos de Elastic Load Balancing	Puede compartir los almacenes de confianza de Elastic Load Balancing en toda la organización Cuentas de AWS o dentro de ella.	5 de agosto de 2024
Compatibilidad ampliada para compartir modelos personalizados de Amazon Bedrock	Ahora puede utilizarlos AWS RAM para compartir modelos personalizados de Amazon Bedrock con otras personas Cuentas de AWS y con su organización.	1 de agosto de 2024
Se agregó soporte para compartir copias de seguridad AWS CloudHSM	Puede compartir las AWS CloudHSM copias de seguridad con otras organizaciones Cuentas de AWS o con las suyas AWS RAM.	28 de junio de 2024
Se agregó soporte para compartir Model Registry los recursos de Amazon SageMaker AI.	Ahora puede compartir parámetros avanzados de forma segura y eficiente en sus Cuentas de AWS o en su organización.	27 de junio de 2024

Se agregó soporte para compartir Amazon SageMaker AI JumpStart	Ahora puede compartir Amazon SageMaker AI JumpStart Hubs con Cuentas de AWS o dentro de su organización.	27 de junio de 2024
Se agregó soporte para compartir Amazon Route 53 ResolverProfiles	Ahora puede usarlo AWS RAM para compartir Amazon Route 53 Resolver Profiles con otros miembros Cuentas de AWS de su organización.	22 de abril de 2024
Se agregó soporte para compartir los recursos de AWS Systems Manager Parameter Store	Ahora puede compartir parámetros avanzados de forma segura y eficiente en sus Cuentas de AWS o en su organización.	21 de febrero de 2024
Se agregó soporte para compartir Amazon FSx para OpenZFS Snapshots	Ahora puede compartir las instantáneas de Amazon FSx for OpenZFS con otras personas de su organización Cuentas de AWS .	19 de diciembre de 2023
Se agregó soporte para compartir recursos Amazon Simple Storage Service	Ahora puede compartir la instancia de Amazon Simple Storage Service Access Grants con otras Cuentas de AWS personas o con su organización AWS RAM.	27 de noviembre de 2023
Se agregó soporte para compartir Explorador de recursos de AWS vistas	Ahora puede compartir Explorador de recursos de AWS vistas con otras personas Cuentas de AWS de su organización.	14 de noviembre de 2023

Compatibilidad ampliada para compartir recursos del Controlador de recuperación de aplicaciones de Amazon (ARC)	Ahora puede compartir clústeres de Amazon Application Recovery Controller (ARC) con otras personas Cuentas de AWS o con las de su organización AWS RAM.	18 de octubre de 2023
Se agregó soporte para compartir DataZone los recursos de Amazon	Ahora puedes compartir DataZone los recursos de Amazon con otras personas Cuentas de AWS o con tu organización.	4 de octubre de 2023
Compatibilidad ampliada para compartir entidades principales de servicio	Ahora puede asociar entidades principales de servicio a recursos compartidos. Esto permite que los servicios especificados administren en su nombre las acciones necesarias para los recursos del cliente.	29 de agosto de 2023
Se agregó soporte para compartir los recursos de SageMaker Model Card	Ahora puede compartir los recursos de SageMaker Model Card con otras personas Cuentas de AWS o con su organización.	18 de agosto de 2023
Se agregó compatibilidad con los grupos de funciones de Amazon SageMaker AI Feature Store y SageMaker AI Catalog como recursos que se pueden compartir	Ahora puede compartir los grupos de funciones de Amazon SageMaker AI Feature Store y los recursos del catálogo de SageMaker IA con otras personas Cuentas de AWS o con su organización.	20 de julio de 2023

Incremento del límite de cuota de servicio para invitaciones pendientes	El número máximo de invitaciones pendientes por cuenta de uso compartido se ha incrementado de 20 a 250.	8 de junio de 2023
Se agregó soporte para AWS AppSync GraphQL APIs como recursos compartibles	Ahora puedes compartir AWS AppSync GraphQL APIs con otras Cuentas de AWS personas. AWS RAM	24 de mayo de 2023
Se agregó soporte para Acceso verificado de AWS grupos como recursos compartibles	Ahora puede crear y administrar Acceso verificado de AWS grupos de forma centralizada y, a continuación, compartirlos con otras personas Cuentas de AWS o con su organización.	27 de abril de 2023
Se ha añadido soporte para los permisos gestionados por el cliente en la AWS RAM consola	Ahora puede crear y mantener de forma segura controles detallados de acceso a recursos para los tipos de recursos compatibles.	19 de abril de 2023
Compatibilidad ampliada para el servicio de Amazon VPC Lattice y la red de servicios como recursos que se pueden compartir	Ahora puede compartir el servicio Amazon VPC Lattice y los recursos de red de servicios con otras personas. Cuentas de AWS	31 de marzo de 2023
Se agregó soporte para las entidades del AWS Marketplace catálogo como recursos que se pueden compartir	Ahora puedes compartir tus entidades con otras Cuentas de AWS en el Marketplace.	27 de marzo de 2023

Se agregó soporte para administrar las versiones de permisos en la AWS RAM consola	Ahora puede usar la AWS RAM consola para ver los detalles de la versión y actualizar los permisos a la versión que esté designada como predeterminada.	16 de enero de 2023
Actualizaciones de las prácticas recomendadas de IAM	Guía actualizada para implementar las prácticas recomendadas de IAM. Para obtener más información, consulte prácticas recomendadas de seguridad en IAM.	3 de enero de 2023
Compatibilidad ampliada para los grupos de ubicación de Amazon EC2 como recursos que se pueden compartir	Ahora puede compartir los grupos de ubicación de Amazon EC2 con otras personas Cuentas de AWS para lanzar sus instancias.	8 de noviembre de 2022
Se agregaron enlaces a dos vídeos introductorios sobre AWS RAM	Se agregaron videos de información general que describen AWS RAM y proporcionan una guía sobre cómo compartir un recurso con otras personas. Cuentas de AWS	29 de agosto de 2022
Se agregó soporte para las canalizaciones de Amazon SageMaker AI	Ahora puede compartir las canalizaciones de SageMaker IA con otras personas. Cuentas de AWS	2 de agosto de 2022

Se ha añadido compatibilidad con AWS Service Catalog AppRegistry aplicaciones y grupos de atributos como tipos de recursos que se pueden compartir	Ahora puede compartir AppRegistry aplicaciones y grupos de atributos con otros Cuentas de AWS usuarios.	17 de junio de 2022
AWS Resource Access Manager recibe las certificaciones SOC e ISO	AWS RAM ha sido validado por su conformidad con las normas ISO 9001, ISO 27001, ISO 27017, ISO 27018 e ISO 27701 de la Organización Internacional de Normalización (ISO) y de la Organización Internacional de Normalización (ISO).	31 de mayo de 2022
AWS Resource Access Manager recibe la certificación FedRAMP	AWS RAM se ha validado que cumple con el Programa Federal de Gestión de Riesgos y Autorizaciones (FedRAMP).	8 de abril de 2022
AWS Resource Access Manager recibe la certificación PCI DSS	AWS RAM ha sido validado por su conformidad con el estándar de seguridad de datos (DSS) de la industria de tarjetas de pago (PCI).	27 de febrero de 2022
Se ha ampliado la compatibilidad de las detecciones de recursos de IPAM de Amazon VPC como recursos que se pueden compartir. Además, ahora puede compartir grupos de IPAM con cuentas ajenas a una organización	Ahora puede compartir detecciones de recursos de IPAM con otras Cuentas de AWS.	25 de enero de 2022

Compatibilidad ampliada para compartir recursos globales	Ahora puede compartir recursos globales con otras Cuentas de AWS personas.	2 de diciembre de 2021
Se agregó soporte para las redes principales de AWS Cloud WAN como recursos globales que se pueden compartir	Ahora puedes compartir las redes principales de Cloud WAN con otras Cuentas de AWS.	2 de diciembre de 2021
Compatibilidad para compartir grupos del Administrador de direcciones IP (IPAM) de Amazon VPC	Puede usarlo AWS RAM para compartir grupos de IPAM de Amazon VPC. Para obtener más información, consulte AWS Recursos que se pueden compartir en la Guía del AWS RAM usuario.	1 de diciembre de 2021
Support para compartir los recursos de Amazon SageMaker AI	Puede utilizarlos AWS RAM para compartir grupos de linaje de SageMaker IA. Para obtener más información, consulte Recursos de AWS que se pueden compartir en la Guía del usuario de AWS RAM .	30 de noviembre de 2021
Support para compartir recursos AWS Migration Hub de Refactor Spaces	Puede usarlo AWS RAM para compartir entornos de Migration Hub. Para obtener más información, consulte Recursos de AWS que se pueden compartir en la Guía del usuario de AWS RAM .	29 de noviembre de 2021

Se agregó información sobre las políticas AWS RAMAWS de permisos de IAM gestionadas	Se ha publicado información sobre las políticas de permisos AWS gestionados disponibles a las que puede acceder en la consola de IAM y adjuntarlas a los principios de IAM de su propia consola. Cuenta de AWS	16 de septiembre de 2021
Compatibilidad ampliada para compartir recursos de S3 en Outposts	Ahora puedes usarlo AWS RAM para compartir S3 en Outposts con otros. Cuentas de AWS	5 de agosto de 2021
Compatibilidad ampliada para admitir permisos administrados adicionales y compartir recursos con entidades principales de IAM	Para los tipos de recursos compatibles, puede elegir entre permisos AWS RAM gestionados adicionales y compartir recursos con funciones y usuarios individuales de IAM.	10 de junio de 2021
Se agregó soporte para compartir AWS los recursos de Systems Manager Incident Manager	Ahora puede utilizarla AWS RAM para compartir AWS los contactos y planes de respuesta de Systems Manager Incident Manager con otras personas Cuentas de AWS.	10 de mayo de 2021
Compatibilidad ampliada para compartir recursos de Amazon Route 53	Ahora puede utilizarlos AWS RAM para compartir grupos de reglas de Firewall DNS de Amazon Route 53 Resolver con otros Cuentas de AWS.	31 de marzo de 2021

Se agregó soporte para compartir AWS Transit Gateway recursos	Ahora puede utilizarlos AWS RAM para compartir dominios de multidifusión de Transit Gateway con otros Cuentas de AWS.	10 de diciembre de 2020
Se agregó soporte para compartir recursos AWS Network Firewall	Ahora puede usarlo AWS RAM para compartir políticas de AWS Network Firewall firewall y grupos de reglas con otros Cuentas de AWS.	17 de noviembre de 2020
Compatibilidad ampliada para compartir Outposts y tablas de enrutamiento de puerta de enlace local	Ahora puedes usarlo AWS RAM para compartir las tablas de rutas de Outposts y puertas de enlace locales con otros. Cuentas de AWS	15 de octubre de 2020
Compatibilidad ampliada para compartir registros de consultas de Route 53	Ahora puede usarlo AWS RAM para compartir los registros de consultas de Route 53 con otras Cuentas de AWS personas.	7 de septiembre de 2020
Se agregó soporte para compartir AWS Private Certificate Authority recursos	Ahora puede usarlo AWS RAM para compartir autoridad es de certificación Autoridad de certificación privada de AWS privadas (CAs) con otras Cuentas de AWS.	17 de agosto de 2020
Se agregó soporte para compartir catálogos de datos, bases de datos y tablas de AWS Glue	Ahora puede utilizar AWS Glue AWS RAM para compartir catálogos de datos, bases de datos y tablas con otros Cuentas de AWS usuarios.	7 de julio de 2020

Se agregó soporte para compartir listas de prefijos de Amazon VPC	Ahora puede usarlo AWS RAM para compartir listas de prefijos.	29 de junio de 2020
Se agregó soporte para compartir direcciones propiedad de AWS Outposts los clientes IPv4	Ahora puedes usarlo AWS RAM para compartir las direcciones de los AWS Outposts clientes con otras personas. IPv4 Cuentas de AWS	22 de abril de 2020
Se ha añadido soporte para compartir mallas AWS App Mesh	Ahora puede utilizarlas AWS RAM para compartir mallas con otras personas. Cuentas de AWS	17 de enero de 2020
Se agregó soporte para compartir AWS CodeBuild proyectos y grupos de informes	Ahora puede usarlo AWS RAM para compartir AWS CodeBuild proyectos y grupos de informes con otros Cuentas de AWS.	13 de diciembre de 2019
Compatibilidad ampliada para compartir recursos adicionales	Ahora puede utilizarlos AWS RAM para compartir hosts dedicados de Amazon EC2, grupos de Grupos de recursos de AWS recursos y componentes, imágenes y recetas de imágenes de Amazon EC2 Image Builder con otros usuarios. Cuentas de AWS	2 de diciembre de 2019

Compatibilidad ampliada para compartir reservas de capacidad bajo demanda	Ahora puede utilizarlo AWS RAM para compartir las reservas de capacidad bajo demanda con otras personas. Cuentas de AWS	29 de julio de 2019
Compatibilidad ampliada para compartir clústeres de bases de datos de Aurora	Ahora puede utilizarlos AWS RAM para compartir clústeres de base de datos Aurora con otros Cuentas de AWS.	2 de julio de 2019
Compatibilidad ampliada para compartir objetivos de reflejo de tráfico	Ahora puede utilizarlos AWS RAM para compartir los objetivos de duplicación de tráfico con otros usuarios. Cuentas de AWS	25 de junio de 2019
Compatibilidad ampliada para compartir configuraciones de licencias	Ahora puede utilizarla AWS RAM para compartir las configuraciones AWS de licencia de License Manager con otros usuarios Cuentas de AWS.	5 de diciembre de 2018
Compatibilidad ampliada para compartir subredes	Ahora puede utilizarlas AWS RAM para compartir subredes de Amazon VPC con otras personas. Cuentas de AWS	27 de noviembre de 2018
Compatibilidad ampliada para compartir puertas de enlace de tránsito	Ahora puede utilizarlas AWS RAM para compartir las pasarelas de tránsito de Amazon VPC con otras personas. Cuentas de AWS	26 de noviembre de 2018

Compatibilidad ampliada para compartir reglas de Resolver	Ahora puede utilizarlas AWS RAM para compartir las reglas de Route 53 Resolver con otras personas. Cuentas de AWS	20 de noviembre de 2018

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.