Guía del usuario

# AWS Resource Access Manager

# AWS Resource Access Manager: Guía del usuario

# Table of Contents

# ¿Qué es AWS Resource Access Manager?

AWS Resource Access Manager(AWS RAM) le ayuda a compartir sus recursos de forma segura entre Cuentas de AWS, dentro de su organización o de unidades organizativas (OU), y con roles y usuarios de AWS Identity and Access Management (IAM), para los tipos de recursos compatibles. Si tiene varias Cuentas de AWS, puede crear un recurso una vez y usar AWS RAM para que dichos recursos estén disponibles para su uso por parte de otras cuentas. Si su cuenta está administrada por AWS Organizations, puede compartir recursos con todas las demás cuentas de la organización o solo con las cuentas que pertenezcan a una o más unidades organizativas (OU) específicas. También puede compartirlos con Cuentas de AWS específicas por ID de cuenta, 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

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

El siguiente vídeo le muestra cómo aplicar permisos administrados de AWS a sus recursos de AWS. 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 utilizar AWS RAM? Ofrece las siguientes ventajas:

- Reduce la sobrecarga operativa: cree un recurso una vez y luego use AWS RAM para compartir dicho recurso 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, AWS RAM simplifica la concesión de acceso a todos los roles y usuarios de esa cuenta sin necesidad de 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 recurso compartido de AWS RAM se administran mediante un único conjunto de políticas y permisos. AWS RAMofrece una experiencia coherente para compartir diferentes tipos de recursos de AWS.
- Proporciona visibilidad y capacidades de auditoría: consulte los detalles de uso de sus recursos compartidos mediante la integración de AWS RAM con Amazon CloudWatch y AWS CloudTrail. AWS RAM proporciona una visibilidad completa de los recursos compartidos y las cuentas.

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

Puede compartir algunos tipos de recursos de AWS con otras Cuentas de AWS adjuntando una política basada en recursos que identifique a las entidades principales de AWS Identity and Access Management (IAM) (funciones y usuarios de IAM) externas a su Cuenta de AWS. Sin embargo, compartir un recurso adjuntando una política no permite aprovechar las ventajas adicionales que ofrece AWS RAM. Al usar AWS RAM, se beneficiará de las siguientes características:

- Puede compartir con una organización o una unidad organizativa (OU) sin tener que enumerar cada uno de los ID de Cuenta de AWS.
- 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 usa AWS RAM para compartir una subred de Amazon VPC con otra cuenta, los usuarios de dicha 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, AWS RAM inicia 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 tiene recursos que ha compartido utilizando una política de permisos basada en recursos, puedes promocionar tales recursos a recursos totalmente administrados de AWS RAM de la siguiente manera:

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

# Cómo funciona el uso compartido de recursos

Cuando comparte un recurso de la cuenta propietaria con otra Cuenta de AWS, la cuenta consumidora, está concediendo acceso al recurso compartido a las entidades 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 de las Cuentas de AWS con las que los ha compartido.

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

## Compartir sus recursos

Con AWS RAM, puede compartir recursos de su propiedad creando un recurso compartido. Para crear un recurso compartido, especifique lo siguiente:

- La Región de AWS en la 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 la AWS CLI, utilice el parámetro `--region`.

  - 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. Las entidades principales pueden ser Cuentas de AWS individuales, las cuentas de una organización o una unidad organizativa (OU) de AWS Organizations, o bien roles o usuarios individuales de AWS Identity and Access Management (IAM).

  > **Note**
  >
  > No todos los tipos de recursos se pueden compartir con roles y 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 a través de la consola de servicio pertinente o mediante los comandos de la AWS CLI y las

operaciones de API. 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 accede a un recurso compartido utilizando el servicio de ese recurso, tiene las mismas capacidades y limitaciones que la Cuenta de AWS propietaria 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 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`.

# Acceso a AWS RAM

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

Consola de AWS RAM

AWS RAM cuenta con una interfaz de usuario basada en web, la consola de AWS RAM. Si se ha registrado con una cuenta de Cuenta de AWS, puede acceder a la consola de AWS RAM iniciando sesión en la AWS Management Console y seleccionando AWS RAM en la página de inicio de la consola.

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

La AWS CLI y AWS Tools for PowerShell proporcionan acceso directo a las operaciones de API pública de AWS RAM. AWS admite estas herramientas en Windows, macOS y Linux. Para obtener más información acerca de cómo empezar, consulte la Guía del usuario deAWS Command Line Interface o la Guía del usuario AWS Tools for Windows PowerShell. Para obtener más información acerca de los comandos de AWS RAM, consulte la Referencia de comandos de AWS CLI o la Referencia de Cmdlet de AWS Tools for Windows PowerShell.

SDK de AWS

AWS cuenta con comandos de API para una amplia gama de lenguajes de programación. Para obtener más información acerca de cómo empezar a trabajar, consulte la Guía de referencia de las herramientas y los SDK de AWS.

API de consulta

Si no usa uno de los lenguajes de programación compatibles, la API de consulta HTTPS de AWS RAM le proporciona acceso programático a AWS RAM y AWS. Con la API de AWS RAM, puede emitir solicitudes HTTPS directamente al servicio. Cuando use la API de AWS RAM, debe incluir código para firmar digitalmente las solicitudes utilizando sus credenciales. Para obtener más información, consulte la referencia de la API de AWS RAM.

# Precios de AWS RAM

No se aplican cargos adicionales por usar AWS RAM ni por crear recursos compartidos o compartir recursos entre cuentas. Los cargos por el uso de recursos varían en función del tipo de recurso. Para obtener más información acerca de cómo AWS factura los recursos que se comparten, consulte la documentación correspondiente al servicio propietario del recurso.

# Conformidad y estándares internacionales

## PCI DSS

AWS RAM admite el procesamiento, el almacenamiento y la transmisión de datos de tarjetas de crédito por parte de un comerciante o proveedor de servicios y se ha validado por estar conforme 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 Moderate en las siguientes Regiones de AWS: Este de EE. UU. (Norte de Virginia), Este de EE. UU. (Ohio), Oeste de EE. UU. (Norte de California) y Oeste de EE. UU (Oregón).

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

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 usar para cargas de trabajo sujetas a conformidad con la entidad de Control de Organizaciones de Servicio (SOC, Service Organisation Control) y con las normas ISO 9001, ISO 27001, ISO 27017, ISO 27018 e ISO 27701 de la Organización Internacional de Normalización (ISO, International Standardization Organization). 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.

# Introducción a AWS RAM

AWS Resource Access Manager le permite compartir recursos de su propiedad con otras Cuentas de AWS individuales. Si su cuenta está administrada 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 habilita el uso compartido en AWS Organizations, no podrá compartir recursos con su organización ni con las unidades organizativas (OU) de esta. No obstante, puede seguir compartiendo recursos con Cuentas de AWS individuales de la 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 de AWS RAM

Los siguientes conceptos ayudan a entender cómo se puede usar AWS Resource Access Manager (AWS RAM) para compartir recursos.

## Uso compartido de recursos

AWS RAM le permite compartir recursos creando un recurso compartido. Un recurso compartido consta de los tres elementos siguientes:

- Una lista de uno o más recursos de AWS que se van a 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.

Una vez que ha usado AWS RAM para crear un recurso compartido, se puede conceder a las entidades principales especificadas en el recurso compartido acceso a los recursos que este contiene.

- Si activa el uso compartido de AWS RAM con AWS Organizations, y las entidades principales con las que comparte pertenecen a la misma organización que la cuenta que comparte, dichas entidades principales podrán recibir acceso tan pronto como el administrador de la cuenta les conceda permisos para usar los recursos mediante una política de permisos de AWS Identity and Access Management (IAM).
- Si no activa el uso compartido de AWS RAM con organizaciones, puede seguir compartiendo recursos con Cuentas de AWS individuales de su 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 que comparte contiene el recurso que se comparte y en el que el administrador de AWS RAM crea el recurso compartido de AWS mediante AWS RAM.

Un administrador de AWS RAM es una entidad principal de IAM que dispone de permisos para crear y configurar recursos compartidos en la Cuenta de AWS. Puesto que AWS RAM funciona adjuntando una política basada en recursos a los recursos de un recurso compartido, el administrador de AWS RAM también debe tener permisos para llamar a la operación `PutResourcePolicy` del Servicio de AWS para cada tipo de recurso incluido en un recurso compartido.

## Entidades principales consumidoras

La cuenta consumidora es la 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 admite las entidades principales de servicio como entidades consumidoras 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 de entidades principales de IAM como entidades consumidoras de recursos compartidos:

- Otra Cuenta de AWS: el recurso compartido hace que los recursos incluidos en la cuenta que comparte 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`
- Entidad principal de servicio: comparta un recurso con un servicio de AWS servicio para conceder al servicio acceso a un recurso compartido. Compartir con una entidad principal de servicio hace posible que un servicio de AWS emprenda acciones en su nombre para mitigar 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 que comparte está administrada por AWS Organizations, el recurso compartido puede especificar el ID 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 solo puede compartir con su propia organización o con ID de OU 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 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.

## Política basada en 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 identidad que se adjuntan a la entidad principal, como un rol o usuario de IAM, las políticas basadas en recursos se adjunta al recurso. AWS RAM crea políticas basadas en recursos en su nombre en función de la información que proporcione para el recurso compartido. 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 AWS RAM se evalúan junto con todos los demás tipos de políticas de IAM. Esto incluye cualquier política basada en la identidad de IAM que se adjunte a las entidades principales que intenten acceder al recurso, así como las políticas de control de servicios (SCP) de AWS Organizationsque puedan aplicarse a la Cuenta de AWS. Las políticas basadas en recursos generadas por AWS RAM participan en la misma lógica de evaluación de políticas que el resto de 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 uso compartido de recursos sencilla y segura al proporcionar políticas de abstracción basadas en recursos fáciles de usar.

En el caso de los tipos de recursos que admiten políticas basadas en recursos, AWS RAM crea y administra automáticamente las políticas basadas en recursos en su nombre. 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, piense en una canalización de Amazon Sagemaker que comparte utilizando AWS RAM y que incluye 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 a una sola cuenta. AWS RAM combina automáticamente esos dos conjuntos diferentes de permisos en una única política de recursos con varias instrucciones. A continuación, adjunta la política combinada basada en recursos al recurso de la canalización. Puede ver esta política de recursos subyacente llamando a la operación GetResourcePolicy. Los Servicios

de AWS utilizan entonces esa política basada en recursos para autorizar a cualquier entidad principal 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 detección para entidades consumidoras de recursos compartidos: si comparte recursos utilizando AWS RAM, los usuarios pueden ver todos los recursos compartidos con ellos directamente en la consola de servicio y las operaciones de API del recurso propietario, como si dichos recursos estuvieran directamente en la cuenta del usuario. Por ejemplo, si comparte un proyecto de AWS CodeBuild con otra cuenta, los usuarios de la cuenta consumidora pueden ver el proyecto en la consola de CodeBuild y en los resultados de las operaciones de la API de CodeBuild 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 del recurso compartido: si comparte recursos utilizando AWS RAM, los propietarios de los recursos de la cuenta que comparte 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 comparte recursos utilizando 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.
- Sencillez: con AWS RAM, no necesita entender el lenguaje de políticas basado en JSON que utiliza IAM. AWS RAM proporciona permisos administrados de AWS listos para usar entre los que puede elegir para adjuntarlos a sus recursos compartidos.

Al usar 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, AWS RAM genera automáticamente una política basada en 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 licencias
- AWS Outposts: tablas de enrutamiento de puerta de enlace, outposts y sitios
- Amazon Route 53: reglas de reenvío
- Amazon Virtual Private Cloud: 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

## Ejemplos de políticas basadas en recursos generadas por AWS RAM

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

```
{
    "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 de una Cuenta de AWS diferente, AWS RAM genera una política similar a la del ejemplo siguiente y la adjunta a todos los recursos de imagen que estén incluidos en el recurso compartido.

```
{
  "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 a la del 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.

```
{
    "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 de `actions` y las condiciones que las entidades principales pueden llevar a cabo en el recurso compartido utilizando 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:

Permisos administrados de AWS

Los permisos administrados de AWS, de cuya creación y mantenimiento se encarga AWS, otorgan permisos para escenarios frecuentes del cliente. AWS RAM define al menos un permiso

administrado de AWS para cada tipo de recurso compatible. Algunos tipos de recursos admiten más de un permiso administrado de AWS, designándose uno de ellos como el predeterminado de AWS. El permiso administrado predeterminado de AWS se asocia a menos que se 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, y en qué condiciones, en los recursos compartidos 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.

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 recursos compartidos de AWS RAM. Los permisos administrados por el cliente son específicos de una región.

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

## 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. Cuando usted o AWS crean una nueva versión de un permiso administrado, 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.

Versiones de los permisos administrados de AWS

AWS gestiona todos los cambios en los permisos administrados de AWS. 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 Actualizar los permisos administrados de AWS a una versión más reciente.

## Compartir recursos de AWS de su propiedad

Para compartir un recurso de su propiedad utilizando AWS RAM, haga lo siguiente:

- Habilitar el uso compartido de recursos en AWS Organizations (opcional)
- Crear un recurso compartido

Notas

- Compartir un recurso con entidades principales externas a la Cuenta de AWS propietaria del recurso no cambia los permisos ni las cuotas que se aplican al recurso en el ámbito de la cuenta que lo creó.
- AWS RAM es un servicio regional. Las entidades principales con las que comparte pueden acceder únicamente a los recursos compartidos de las Regiones de AWS en las que se crearon.
- Algunos recursos tienen consideraciones y requisitos previos especiales para su uso compartido. Para obtener más información, consulte Recursos que se pueden compartir AWS.

# Habilitar el uso compartido de recursos en AWS Organizations

Cuando su cuenta esté administrada por AWS Organizations, puede aprovechar para compartir recursos más fácilmente. 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 debe usar la consola de AWS RAM o AWS Command Line Interface (AWS CLI) para habilitar el uso compartido con AWS Organizations. Cuando comparte recursos en su organización, AWS RAM no envía invitaciones a las entidades principales. Las entidades principales de su organización obtienen acceso a los recursos compartidos sin necesidad de intercambiar invitaciones.

Al habilitar el uso compartido de recursos en su organización, AWS RAM crea un rol vinculado a un servicio denominado **`AWSServiceRoleForResourceAccessManager`**. Este rol, que solo lo puede asumir el servicio AWS RAM, otorga a AWS RAM permiso para recuperar información sobre la organización de la que es miembro utilizando la política administrada de AWS `AWSResourceAccessManagerServiceRolePolicy`.

Si ya no necesita compartir recursos con toda la organización o con determinadas OU, 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 utilizando la consola de AWS RAM o el comando enable-sharing-with-aws-organization de la AWS CLI. Así se asegurará de crear el rol vinculado al servicio `AWSServiceRoleForResourceAccessManager`. Si habilita el acceso de confianza con AWS Organizations utilizando la consola de AWS Organizations o el comando enable-aws-service-access de la AWS CLI, el rol vinculado al servicio `AWSServiceRoleForResourceAccessManager` no se creará y no podrá compartir recursos dentro de la organización.

Console

Para habilitar el uso compartido de recursos dentro de la organización

1. Abra la página Configuración en la consola de AWS RAM.
2. Seleccione Habilitar el uso compartido con AWS Organizations y, a continuación, seleccione Guardar configuración.

AWS CLI

Para habilitar el uso compartido de recursos dentro de la organización

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

Este comando se puede usar en cualquier Región de AWS, y habilita el uso compartido con AWS Organizations en todas las regiones en las que se admite AWS RAM.

```
$ 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 aparece 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 recursos 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 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 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 los 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 ruta de puerta de enlace local, 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 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 desea 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 que se muestren 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 desea añadir.

> **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 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

Use 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"
    }
}
```

# Usar recursos compartidos de AWS

Para empezar a usar los recursos que se han compartido con su cuenta mediante AWS Resource Access Manager, lleve a cabo 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 forma parte de una organización de AWS Organizations que tiene habilitado el uso compartido, las entidades principales de la organización obtendrán acceso automáticamente a los recursos compartidos sin necesidad de recibir invitaciones.
- Si comparte con la Cuenta de AWS a la que pertenece el recurso, las entidades principales de dicha cuenta obtendrán acceso automáticamente a los recursos compartidos sin necesidad de recibir 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 la Región de AWS en la que se creó. Si el recurso compartido en cuestión no aparece en la consola, es posible que tenga que cambiar a otra Región de AWS utilizando 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 luego 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 en las operaciones de API/CLI de cada recurso. Si el recurso es regional, debe usar la Región de AWS correcta en el comando de la consola de servicio o de la API/CLI. Si el recurso es global, debe usar la región de origen designada, Este de EE. UU. (Norte de Virginia), `us-east-1`. Para ver el recurso en AWS RAM, debe abrir la consola de AWS RAM en la Región de AWS en la 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

Este tema analiza las diferencias en cómo AWS Resource Access Manager (AWS RAM) administra 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 que se pueden compartir con AWS RAM son regionales. Se crean en una Región de AWS específica y existen en esa región. Para ver estos recursos o interactuar con ellos, debe dirigir sus operaciones a la región correspondiente. Por ejemplo, para crear una instancia de Amazon Elastic Compute Cloud (Amazon EC2) con la AWS Management Console, debe elegir la Región de AWS en la que desea crear la instancia. Si usa la AWS Command Line Interface (AWS CLI) para crear la instancia, debe incluir el parámetro `--region`. Cada uno de los SDK de AWS 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 especifica una Región de AWS diferente en la consola o en un comando de AWS CLI, ya no podrá ver ni interactuar con los recursos que vería 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 ARN similares a los del siguiente ejemplo en el caso de una VPC que existe en la región `us-east-1`.

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

### Recursos globales

Algunos servicios de AWS admiten recursos a los que se puede acceder globalmente, lo que significa que puede usar el recurso desde cualquier lugar. No se especifica ninguna Región de AWS en la consola de un servicio global. Para acceder a un recurso global, no se especifica

un parámetro `--region` cuando se utiliza la AWS CLI y las operaciones del SDK de AWS del servicio.

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 se crea una red central WAN en la nube de AWS como recurso global, esta 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 de la misma Región de AWS que el recurso compartido, además de los recursos globales compatibles. 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 región `us-west-2`, debe configurar la consola de AWS RAM para que utilice `us-west-2` y cree allí el recurso compartido. 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 consola de AWS RAM, debe configurar la consola de AWS RAM para que utilice la región de origen designada, Este de EE. UU. (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 está visible en un recurso compartido de AWS RAM solo en la región de origen designada, sigue siendo un recurso global después de compartirlo. Puede acceder a él en las Cuentas de AWS de cualquier región desde la que podría acceder a él en la Cuenta de AWS original.

Consideraciones

- Para crear un recurso compartido en la consola de AWS RAM, debe utilizar 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 central WAN en la nube de AWS, debe crear el recurso compartido en la región `us-east-1`.
- Para ver o modificar un recurso compartido en la consola de AWS RAM, debe usar la región que contiene el recurso compartido. Del mismo modo, las operaciones de AWS CLI y SDK de AWS RAM 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 consola de AWS RAM e incluirlo en un recurso compartido, debe usar la región que contiene el recurso regional.
- Para ver un recurso global en la consola de AWS RAM e incluirlo en un recurso compartido, debe usar la región de origen designada, Este de EE. UU. (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 desea 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 desea 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

Use 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 al recurso 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 AWS Management Console.
   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 desea 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 corresponde 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 sus recursos compartidos en AWS RAMe

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. 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. 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 las entidades principales con las que comparte 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. 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. 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 las entidades principales a las que hace referencia en los recursos compartidos que haya creado en la Región de AWS actual para la cuenta de llamada.

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, las entidades principales son la organización de la cuenta de llamada y una Cuenta de AWS independiente, que forman parte de dos recursos compartidos distintos. Debe usar el punto de conexión del servicio para la 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 recurso de AWS**
>
> Si necesita eliminar un recurso de AWS que haya incluido en un recurso compartido, AWS le recomienda que primero se asegure de eliminar el recurso individual de cualquier recurso compartido que lo incluya, o bien el recurso compartido en su totalidad.

El recurso eliminado permanece visible en la consola de AWS RAM durante un breve periodo de tiempo tras 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. 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. 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 comando delete-resource-share para eliminar un recurso compartido que ya no necesite.

En el siguiente ejemplo, se usa en primer lugar el comando get-resource-shares para obtener el nombre de recurso de Amazon (ARN) del recurso compartido que se desea eliminar. A continuación, se usa el comando delete-resource-share para 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
}
```

# Acceda a AWS los recursos que compartimos con usted

Con AWS Resource Access Manager (AWS RAM), puede ver los recursos compartidos a los que se le ha agregado, los recursos compartidos a los que puede acceder y los Cuentas de AWS que han compartido recursos 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 Los directores de servicio también tienen acceso automático a los recursos compartidos sin necesidad de 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 su 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: 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 responder a una invitación a un recurso compartido

1. Ve a la página Compartido conmigo: recursos compartidos en la AWS RAM consola.
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. 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. 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. (Opcional) Ayúdese de los filtros para 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) que se muestren solo los recursos compartidos cuyo nombre incluya dicho texto. Resalte el cuadro de texto para ver una lista desplegable de campos de atributo sugeridos. Después de elegir uno, puede elegir de la lista de valores disponibles para ese campo. Puede añadir otros atributos o palabras clave hasta que encuentre el recurso que busca.

4. La consola de AWS RAM muestra información similar a la siguiente:

   - 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. Entre los valores posibles se incluyen:
     - `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 comando get-resource-shares con el parámetro `--resource-owner`establecido en `OTHER-ACCOUNTS`.

En el siguiente ejemplo, se muestra la lista de recursos compartidos en la Región de AWS especificada con la cuenta de llamada por otras 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. Abra la consola de AWS RAM en https://console.aws.amazon.com/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. 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 entidades principales que comparten recursos con su Cuenta de AWS.

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

```
$  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 puede abandonar un recurso compartido si quien le añadió fue una Cuenta de AWS de su organización y está habilitado el uso compartido con AWS Organizations. 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` |

| Servicio | Tipo de recurso |
| --- | --- |
| | `ec2:DedicatedHost` |
| AWS License Manager | `license-manager:LicenseConfiguration` |
| AWS Outposts | `ec2:LocalGatewayRouteTable`<br>`outposts:Outpost`<br>`outposts:Site` |
| Amazon Route 53 | `route53resolver:ResolverRule` |
| Amazon VPC | `ec2:CoipPool`<br>`ec2:PrefixList`<br>`ec2:Subnet`<br>`ec2:TrafficMirrorTarget`<br>`ec2:TransitGateway`<br>`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. 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. 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 comando disassociate-resource-share para abandonar un recurso compartido.

Los siguientes comandos de ejemplo hacen que la Cuenta de AWS que realiza la llamada al comando pierda el acceso a los recursos compartidos por el recurso 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

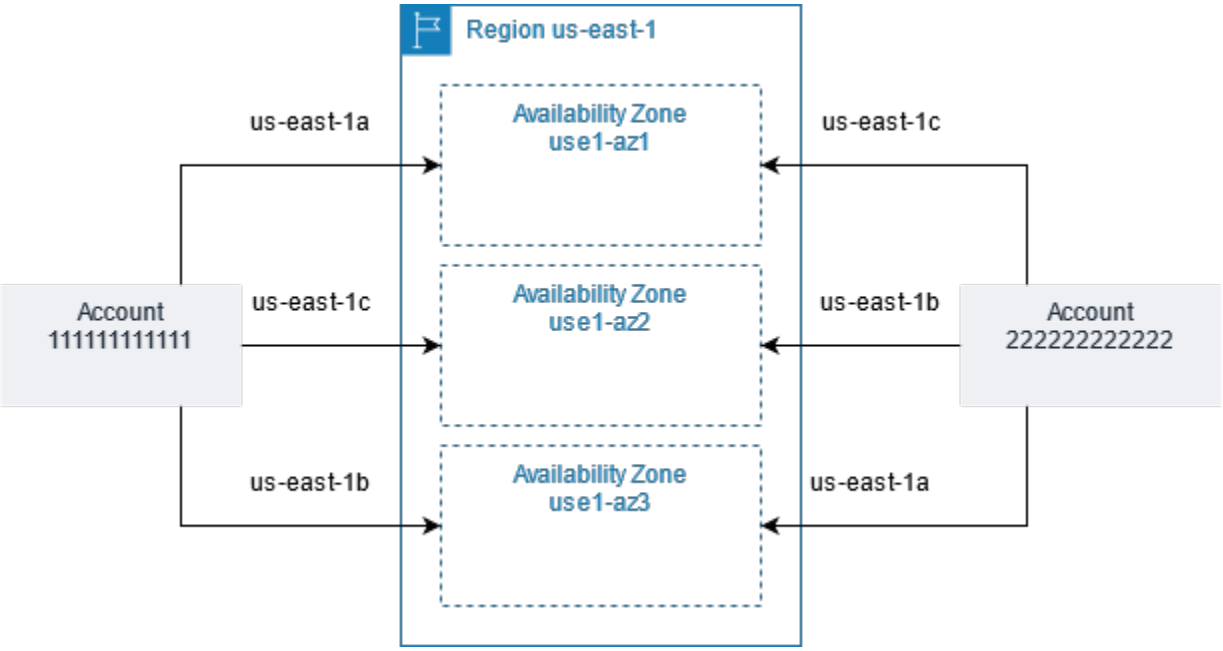
principal para desvincularse del recurso compartido especificado, compartido por la cuenta `111111111111`.

```
$ 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 recursos creados y administrados por otros Servicios de AWS. Puede compartir los recursos con una persona Cuentas de AWS. También puede compartir recursos con las cuentas de una organización o con unidades organizativas (OU) 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. | Sí, |
| | solo puede compartir recursos de este tipo con cuentas. | 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 |
|---|---|---|---|---|---|
| Malla<br><br>`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<br><br>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 |
|---|---|---|---|---|---|
| API de GraphQL<br><br>`appsync:Apis` | Gestione las API de AWS AppSync GraphQL de forma centralizada y compártalas con otras personas Cuentas de AWS o con su organización. Esto permite que varias cuentas compartan AWS AppSync las API como parte de la creación de una API AWS AppSync combinada unificada que puede acceder a los datos de varias API de subesquemas en diferentes cuentas de la misma región. Para obtener más información, consulta las API combinadas en la Guía para AWS AppSync desarrolladores. | S | S<br><br>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<br>`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<br>Puede compartir con cualquier Cuenta de AWS. | N | No |

# AWS Private Certificate Authority

Puede compartir los siguientes Autoridad de certificación privada de AWS 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 |
|---|---|---|---|---|---|
| Entidad de certificación (CA) privada<br><br>`acm-pca:CertificateAuthority` | Cree y administre autoridades de certificación (CA) privadas para la infraestructura de clave pública (PKI) interna de su organización y comparta esas CA 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<br><br>Puede compartir con cualquier Cuenta de AWS. | N | Sí |

# 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 Dominio<br><br>`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<br><br>Puede compartir con cualquier Cuenta de AWS. | N | No |

# AWS CodeBuild

Puedes compartir los siguientes AWS CodeBuild 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 |
|---|---|---|---|---|---|
| Proyecto<br><br>`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<br><br>Puede compartir con cualquier Cuenta de AWS. | S | No |
| Grupo de informes<br><br>`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<br><br>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. | | |

# 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<br><br>`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 Cómo trabajar con reservas de capacidad compartidas en la Guía del usuario de Amazon EC2.<br><br>**Important**<br>Si no cumple todos los requisitos previos para | N | S<br><br>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 |
|---|---|---|---|---|---|
| | 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 compartida | | | | |

| 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 |
|---|---|---|---|---|---|
| | 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<br><br>`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<br><br>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<br><br>`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 de ubicación en la Guía del usuario de Amazon EC2. | S | S<br><br>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<br><br>`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<br><br>Puede compartir con cualquier Cuenta de AWS. | S | No |
| Recetas de contenedor<br><br>`imagebuilder:ContainerRecipe` | Cree y gestione sus recetas de contenedores de forma centralizada y compártalas con otras personas Cuentas de AWS o con su organizac | S | S<br><br>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<br><br>`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<br><br>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 imagen<br>`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<br>Puede compartir con cualquier Cuenta de AWS. | S | No |

# Amazon FSx para OpenZFS

Puede compartir los siguientes recursos de Amazon FSx para 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 |
|---|---|---|---|---|---|
| Volumen de FSx<br><br>`fsx:Volume` | Cree y gestione volúmenes de FSx para OpenZFS de forma centralizada y compártalos con otras Cuentas de AWS personas o con su organización. Esto permite a varias cuentas realizar la replicación de datos mediante OpenZfs instantáneas en volúmenes compartidos a través de las API de FSx `CreateVolume` o. `CopySnapshotAndUpdateVolume` Para obtener más información, consulte Replicación de datos bajo demanda en la Guía del usuario de Amazon FSx para OpenZFS. | S | S<br><br>Puede compartir con cualquier Cuenta de AWS. | S | No |

# AWS Glue

Puede compartir los siguientes AWS Glue 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 |
|---|---|---|---|---|---|
| Catálogos de datos<br><br>`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<br><br>Puede compartir con cualquier Cuenta de AWS. | N | No |
| Bases de datos<br><br>`glue:Database` | 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 |
|---|---|---|---|---|---|
| | 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 |
|---|---|---|---|---|---|
| Tablas<br><br>`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<br><br>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<br><br>`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<br><br>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 |
|---|---|---|---|---|---|
| Entidad de catálogo de Marketplace<br><br>`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<br><br>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<br><br>`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<br><br>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 |
|---|---|---|---|---|---|
| Políticas de firewall<br><br>`network-firewall:FirewallPolicy` | Cree y administre políticas de firewall de forma centralizada y compártalas 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 políticas y grupos de reglas de firewall en la Guía del desarrollador de AWS Network Firewall . | S | S<br><br>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 reglas<br><br>`network-firewall:StatefulRuleGroup`<br><br>`network-firewall:StatelessRuleGroup` | Cree y gestione grupos de reglas con y sin 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 políticas y grupos de reglas de firewall en la Guía del desarrollador de AWS Network Firewall . | S | S<br><br>Puede compartir con cualquier Cuenta de AWS. | 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<br><br>`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<br><br>Puede compartir solo con Cuentas de AWS de su propia organización. | S | No |
| Tabla de enrutamiento de puerta de enlace local<br><br>`ec2:LocalGatewayRouteTable` | Cree y gestione asociaciones de VPC a una puerta de enlace local de forma centralizada y compártalas con otros miembros de su Cuentas de | N | N<br><br>Puede compartir solo con Cuentas | 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 |
|---|---|---|---|---|---|
| | 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 . | | 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<br><br>`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<br><br>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<br><br>`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<br><br>Puede compartir solo con Cuentas de AWS de su propia organización. | S | No |

# Explorador de recursos de AWS

Puede compartir los siguientes Explorador de recursos de AWS 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 |
|---|---|---|---|---|---|
| Vistas<br><br>`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<br><br>Puede compartir solo con Cuentas de AWS de su propia organización. | N | No |

# AWS Resource Groups

Puede compartir los siguientes AWS Resource Groups 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<br><br>`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<br><br>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 DNS Firewall de Route 53 Resolver<br><br>`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 del desarrollador de Amazon Route 53. | S | S<br><br>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 |
|---|---|---|---|---|---|
| Route 53 Profiles<br><br>`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 VPC. Para obtener más información, consulte Amazon Route 53 Profiles en la Guía para desarrolladores de Amazon Route 53. | S | S<br><br>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<br><br>`route53resolver:ResolverRule` | Cree y gestione 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 consultas de DNS desde sus nubes privadas virtuales (VPC) a las direcciones IP de destino definidas en 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<br><br>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 |
|---|---|---|---|---|---|
| Registros de consultas<br><br>`route53resolver:ResolverQueryLogConfig` | Cree y administre registros de consultas de forma centralizada, y compártalos con otras Cuentas de AWS o con su organización. Esto permite que varias Cuentas de AWS registren las consultas de DNS que se originan en sus VPC en un registro de consultas administrado de forma centralizada. 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. | S | S<br><br>Puede compartir con cualquier Cuenta de AWS. | S | No |

## Controlador de recuperación de aplicaciones de Amazon Route 53

Puede compartir los siguientes recursos del Controlador de recuperación de aplicaciones 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 |
|---|---|---|---|---|---|
| Clúster de Route 53 ARC<br><br>`route53-recovery-control:Cluster` | Cree y administre los clústeres ARC de Route 53 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 del desarrollador del Controlador de recuperación de aplicaciones de Amazon Route 53. | S | S<br><br>Puede compartir con cualquier Cuenta de AWS. | S | 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<br><br>`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<br><br>Puede compartir con cualquier Cuenta de AWS. | S | Sí |

# Amazon SageMaker

Puedes compartir los siguientes SageMaker 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 |
|---|---|---|---|---|---|
| SageMaker Catálogo<br><br>`sagemaker:SagemakerCatalog` | Para facilitar la detección: permite a los propietarios de las cuentas conceder permisos de detección a otras cuentas para todos los recursos del grupo de funciones del SageMaker catálogo. 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 SageMaker desarrolladores de Amazon. | N | S<br><br>Puede compartir con cualquier Cuenta de AWS. | 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 |
|---|---|---|---|---|---|
| | **Note**<br>La visibilidad y el acceso son permisos independientes en. 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 Grupo de funciones<br><br>`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 SageMaker desarrolladores de Amazon.<br><br>**Note**<br>La visibilidad y el acceso son permisos | S | S<br><br>Puede compartir con cualquier Cuenta de AWS. | 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 |
|---|---|---|---|---|---|
| | independientes en. 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 |
|---|---|---|---|---|---|
| Grupo de linaje<br><br>`sagemaker:LineageGroup` | Amazon te SageMaker permite crear grupos de linajes de los metadatos de tu 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, consulta el seguimiento del linaje entre cuentas en la Guía para SageMaker desarrolladores de Amazon. | S | S<br><br>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<br><br>`sagemaker:ModelCard` | Amazon SageMaker crea tarjetas modelo para documentar los 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<br><br>Puede compartir con cualquier Cuenta de AWS. | 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 Amazon SageMaker Model Cards en la Guía para SageMaker desarrolladores de Amazon. | | | | |

| 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 canalización<br><br>`sagemaker:Pipeline` | Con Amazon SageMaker 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<br><br>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, consulta Cross-Account Support for SageMaker Pipelines en la Guía para SageMaker desarrolladores de Amazon. | | | | |

# 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 |
|---|---|---|---|---|---|
| Aplicación<br><br>`servicecatalog:Application` | Cree una aplicación y utilícela para realizar un seguimiento de los recursos que pertenecen a esa aplicación en todo el AWS entorno. Comparta la aplicació | N | N<br><br>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 |
|---|---|---|---|---|---|
| Grupo de atributos<br><br>`servicecatalog:AttributeGroup` | 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<br><br>Puede compartir solo con Cuentas de AWS de su propia organización. | S | No |

# AWS Systems Manager Incident Manager

Puede compartir los siguientes AWS Systems Manager Incident 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<br><br>`ssm-contacts:Contact` | Cree y administre contactos y planes de escalamiento de forma centralizada y comparta los detalles de contacto con otras personas Cuentas de AWS o con su organización. Esto permite a muchos Cuentas de AWS ver las interacciones que se producen durante un incidente. 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. | S | S<br><br>Puede compartir con cualquier Cuenta de AWS. | S | No |
| Planes de respuesta<br><br>`ssm-incidents:ResponsePlan` | Cree y gestione planes de respuesta de forma centralizada y compártalos con otras personas Cuentas | S | S<br><br>Puede compartir | 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 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 incidentes de AWS Systems Manager. | | con cualquier Cuenta de AWS. | | |

# AWS Systems Manager Almacén de parámetros

Puede compartir los siguientes recursos del almacén de AWS Systems Manager parámetros 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 |
|---|---|---|---|---|---|
| Parámetro<br><br>`ssm:Parameter` | Cree un parámetro y utilícelo para almacenar datos de configuración a los que pueda hacer referencia en sus scripts, comandos, documentos 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 varios Cuentas de AWS usuarios ver información sobre la cadena y mejorar la seguridad al separar los datos del código. Para obtener más información, consulte Trabajar con | S | S<br><br>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 |
|---|---|---|---|---|---|
| | parámetros compartidos en la Guía del AWS Systems Manager usuario. | | | | |

# 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 |
|---|---|---|---|---|---|
| Direcciones IPv4 propiedad del cliente<br>`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 | N | N<br>Puede compartir solo con Cuentas | 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 información que proporcione sobre la red local.<br><br>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, 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 | | 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 |
|---|---|---|---|---|---|
| | la Guía del usuario de AWS Outposts . | | | | |
| Grupos del Administrador de direcciones IP (IPAM)<br><br>`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 los CIDR del grupo a los AWS recursos, como las VPC, 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<br><br>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 del Administrador de direcciones IP (IPAM)<br><br>`ec2:IpamResourceDiscovery` | Comparta los descubrimientos de recursos con otras personas. 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<br><br>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<br><br>`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<br><br>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<br><br>`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<br><br>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**<br>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 |
|---|---|---|---|---|---|
| Destinos de reflejo de tráfico<br><br>`ec2:TrafficMirrorTarget` | Cree y gestione los objetivos duplicados de tráfico de forma centralizada y compártalos con otros Cuentas de AWS usuarios 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<br><br>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<br><br>`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 varias Cuentas de AWS enruten el tráfico entre sus VPC y las redes de sus instalaciones a través de una puerta de enlace de tránsito compartida y administrada de forma centralizada. Para obtener más información, consulte Compartir una puerta de enlace de tránsito en Puertas de enlace de tránsito de Amazon VPC.<br><br>Note<br>Para incluir una puerta | N | S<br><br>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 |
|---|---|---|---|---|---|
| | de enlace de 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<br><br>`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<br><br>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 grupo<br><br>`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<br><br>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 |
|---|---|---|---|---|---|
| Servicio Amazon VPC Lattice<br><br>`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<br><br>Puede compartir con cualquier Cuenta de AWS. | S | No |
| Red de servicios de Amazon VPC Lattice | Cree y gestione las redes de servicios Amazon VPC Lattice | N | 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 |
|---|---|---|---|---|---|
| `vpc-lattice:ServiceNetwork` | 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. | | Puede compartir con cualquier Cuenta de AWS. | | |

# 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 |
|---|---|---|---|---|---|
| Red central WAN en la nube<br><br>`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<br><br>Puede compartir con cualquier Cuenta de AWS. | N | No |

# Administrar permisos en AWS RAM

En AWS RAM, existen dos tipos de permisos administrados, los permisos administrados de AWS 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 de recurso de Amazon (ARN) del recurso y el ARN de las entidades principales asociadas al recurso compartido completan los elementos de una política basada en recursos. AWS RAM crea entonces la política basada en recursos que se adjunta a todos los recursos de dicho recurso compartido.

Cada permiso administrado puede tener una o más versiones. Se designa una versión como versión predeterminada del permiso administrado. En ocasiones, AWS actualiza un permiso administrado de AWS para un tipo de recurso creando una nueva versión y designándola como versión 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 administrado de AWS lo antes posible. Por lo general, estas actualizaciones añaden compatibilidad para Servicios de AWS nuevos o actualizados que pueden compartir tipos de recursos adicionales utilizando 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"
    }
}
```

# Crear y usar permisos administrados por el cliente en AWS RAM

AWS Resource Access Manager (AWS RAM) proporciona al menos un permiso administrado de AWS para cada tipo de recurso que puede 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 administrados proporcionados por AWS no funciona, puede crear su propio 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 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 IP, 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 administrados por el cliente son específicos de una 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 operación create-permission-version 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. Busque el número de versión que desea establecer como versión predeterminada llamando a 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 la versión que desea establecer como predeterminada, puede llamar a la operación set-default-permission-version.

```
$ 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 volver a ejecutar list-permission-versions y comprobar que el campo `defaultVersion` de la versión seleccionada esté ahora definido como `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 operación list-permission-versions para recuperar los números de las versiones disponibles.
2. Una vez que tenga el número de versión, indíquelo como parámetro en 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 volver a ejecutar list-permission-versions y comprobar que la versión ya no aparece en el resultado.

# 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"
}
```

# Actualizar los permisos administrados de AWS a una versión más reciente

AWS actualiza puntualmente los permisos administrados de AWS disponibles para asociarlos a un recurso compartido para un tipo de recurso específico. Al hacerlo, AWS crea una versión nueva del permiso administrado de AWS. 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 administrado de AWS

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 los detalles de cada recurso compartido que usa el permiso administrado predeterminado de AWS 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 administrados por el cliente en AWS RAM

Los permisos administrados por el cliente solo están disponibles en la Región de AWS en la que las haya creado. No todos los tipos de recursos admiten permisos administrados por el cliente. Para obtener una lista de los tipos de recursos admitidos en AWS Resource Access Manager, consulte Recursos 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:

- Relacionadas con la entidad principal de la organización:
  - `aws:PrincipalOrgId`

  - `aws:PrincipalOrgPaths`
  - `aws:PrincipalAccount`

- Relacionadas con la entidad principal de un servicio especificado:
  - `aws:SourceArn`
  - `aws:SourceAccount`
- Etiquetas del sistema:
  - `aws:PrincipalTag/aws:`
  - `aws:ResourceTag/aws:`
  - `aws:RequestTag/aws:`

## 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 administrado de AWS a cada tipo de recurso que se desea 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.

Acción

La lista de operaciones para las que se concede permiso a la entidad principal. Puede tratarse de una acción en la AWS Management Console o de una operación en la AWS Command Line Interface (AWS CLI) o en la API de AWS. 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 acerca de las condiciones específicas del servicio, consulte Acciones, recursos y claves de condición de los servicios de AWS en la Referencia de autorizaciones de servicio.

> **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 administrados por el cliente en AWS RAM.

# Tipos de permisos administrados

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

- Permiso administrado de AWS: hay un permiso administrado disponible para cada tipo de recurso admitido por 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 administrados predeterminados de AWS utilizan el siguiente formato: `AWSRAMDefaultPermission`*`ShareableResourceType`*. Por ejemplo, para el tipo de recurso `ec2:Subnet`, el nombre del permiso administrado predeterminado de AWS 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 servicios de AWS que funcionan con 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 admitan permisos administrados adicionales, al crear un recurso compartido, AWS RAM aplica automáticamente el permiso predeterminado definido para el tipo de recurso seleccionado. 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 RAM

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

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

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta servicios de AWS en Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información acerca de los programas de conformidad que se aplican a AWS 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 servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida a la hora de utilizar AWS RAM. En los siguientes temas, se le mostrará cómo configurar AWS RAM para satisfacer sus objetivos de seguridad y conformidad. También puede aprender a utilizar otros servicios de AWS que lo ayuden a supervisar y proteger los recursos de AWS RAM.

Temas



## Protección de los datos en AWS RAM

El modelo de responsabilidad compartida de AWS se aplica a la protección de datos de AWS Resource Access Manager. Como se describe en este modelo, AWS es responsable de proteger

la infraestructura global que ejecuta toda la Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Este contenido incluye la configuración de seguridad y las tareas de administración para el que utiliza Servicios de AWS. 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 AWSShared Responsibility Model and GDPR en el Blog de seguridad de AWS.

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

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

Se recomienda encarecidamente no ingresar 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. Incluye las situaciones en las que debe trabajar con la AWS RAM u otros Servicios de AWS a través de la consola, la API, la AWS CLI o los SDK de AWS. Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para 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 identidades y accesos en AWS RAM

AWS Identity and Access Management (IAM) es un servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quiénes pueden autenticarse (iniciar sesión) y obtener autorización (permisos) para hacer uso de los recursos de AWS. El uso de IAM le permite crear entidades principales, como roles, usuarios y grupos, en su Cuenta de AWS. Así, puede controlar los permisos que tienen dichas entidades principales para realizar tareas con recursos de 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 funciona AWS RAM con IAM

De manera predeterminada, las entidades principales de IAM no tienen permiso para crear ni modificar recursos de 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 proporcionar acceso, agregue permisos a sus usuarios, grupos o roles:

- Usuarios y grupos de AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Create a permission set (Creación de un conjunto de permisos) en la Guía del usuario de AWS IAM Identity Center.
- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones de 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 asumir. Siga las instrucciones de 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 que se indican en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

AWS RAM ofrece varias políticas administradas de AWS que puede utilizar para satisfacer las necesidades de un gran número de usuarios. Para obtener más información al respecto, consulte Políticas administradas de AWS para AWS RAM.

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 proporciona información específica de AWS RAM 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`.

Acción

La instrucción Action especifica las acciones de API de AWS RAM 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 instrucción Resource especifica los recursos de AWS RAM 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 precisar en mayor medida 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. Una entidad principal externa es una Cuenta de AWS externa a su organización en 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.

# Políticas administradas de AWS para AWS RAM

En la actualidad, AWS Resource Access Manager proporciona varias políticas administradas de AWS RAM y que describiremos en este tema.

Políticas administradas de AWS

- Política administrada de AWS: AWSResourceAccessManagerReadOnlyAccess
- Política administrada de AWS: AWSResourceAccessManagerFullAccess
- Política administrada de AWS: AWSResourceAccessManagerResourceShareParticipantAccess
- Política administrada de AWS: AWSResourceAccessManagerServiceRolePolicy
- Actualizaciones de AWS RAM en las políticas administradas de 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 administrada de AWS es una política independiente creada y administrada por AWS. Las políticas administradas de AWS se diseñan para proporcionar permisos para muchos casos de uso frecuentes, por lo que puede empezar a asignar permisos a usuarios, grupos y roles.

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

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

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

## Política administrada de AWS: AWSResourceAccessManagerReadOnlyAccess

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*` `oList*`. 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.

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

## Política administrada de AWS: AWSResourceAccessManagerFullAccess

Puede vincular la política `AWSResourceAccessManagerFullAccess` a sus 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.

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

## Política administrada de AWS: AWSResourceAccessManagerResourceShareParticipantAccess

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

Esta política proporciona a las entidades principales la capacidad de aceptar o rechazar los recursos compartidos con esta Cuenta de AWS, así como de ver los detalles relativos a estos recursos compartidos. 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.

```
{
    "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": "*"
        }
    ]
}
```

## Política administrada de AWS: AWSResourceAccessManagerServiceRolePolicy

La política administrada de AWS `AWSResourceAccessManagerServiceRolePolicy` solo se puede usar con el rol vinculado a servicio para AWS RAM. No puede vincular, desvincular, modificar ni eliminar esta política.

Esta política proporciona a AWS RAM acceso de solo lectura a la estructura de su organización. Al habilitar la integración entre AWS RAM y AWS Organizations, AWS RAM crea automáticamente un rol vinculado a servicio denominado AWSServiceRoleForResourceAccessManager que el servicio asume cuando necesita buscar información sobre su organización y sus cuentas; por ejemplo, al visualizar la estructura de la organización en la consola de 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.

```
{
```

```
    "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/*"
            ]
        }
    ]
}
```

## Actualizaciones de AWS RAM en las políticas administradas de AWS

Consulte los detalles relativos a las actualizaciones de las políticas administradas de AWS para AWS RAM desde que este servicio empezara a realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos AWS RAM.

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| AWS Resource Access Manager comenzó a hacer el seguimiento de los cambios | AWS RAM documentó sus políticas administradas existentes y comenzó a | 16 de septiembre de 2021 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| | hacer un seguimiento de los cambios. | |

## Usar roles vinculados a servicios en AWS RAM

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

Un rol vinculado a un servicio facilita la configuración de AWS RAM, ya que no requiere añadir los permisos necesarios manualmente. AWS RAM define los permisos de los roles vinculados a su propio servicio y, salvo que se defina lo contrario, solo AWS RAM puede asumir los roles vinculados a su 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 sobre 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 servicios. Seleccione una opción Sí con un enlace para ver la documentación relativa al rol vinculado al servicio en cuestión.

### Permisos de roles vinculados a servicios para AWS RAM

AWS RAM usa el rol vinculado a servicio denominado `AWSServiceRoleForResourceAccessManager` cuando se habilita el uso compartido con AWS Organizations. Este rol concede permisos al servicio de AWS RAM para ver los detalles de la organización, como la lista de cuentas de miembros y las unidades organizativas en las que figura 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 AWSResourceAccessManagerServiceRolePolicy está asociada a este rol vinculado a permisos, y permite a AWS RAM llevar a cabo las siguientes acciones en los recursos especificados:

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

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

## Crear un rol vinculado a servicios para AWS RAM

No necesita crear manualmente un rol vinculado a servicios. Cuando activa el uso compartido de AWS RAM dentro de su organización en la AWS Management Console o ejecuta EnableSharingWithAWSOrganization en su cuenta mediante la AWS CLI o una API de AWS, AWS RAM crea automáticamente para usted el rol vinculado al servicio.

Si elimina este rol vinculado al servicio, AWS RAM dejará de tener permisos para ver los detalles de la estructura de su organización.

## Editar un rol vinculado a un servicio para AWS RAM

AWS RAM no le permite editar el rol vinculado al servicio AWSResourceAccessManagerServiceRolePolicy. Una vez que crea un rol vinculado a un servicio, no puede cambiar el nombre del rol, ya que varias entidades podrían hacer referencia a dicho rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a un servicio en la Guía del usuario de IAM..

## Eliminar un rol vinculado a un servicio para AWS RAM

También puede usar la consola de IAM, la AWS CLI o la API de AWS para eliminar manualmente el rol vinculado al servicio.

Para eliminar manualmente el rol vinculado al servicio con IAM

Puede usar la consola de IAM, la AWS CLI o la API de AWS para eliminar el rol vinculado al servicio `AWSResourceAccessManagerServiceRolePolicy`. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

### Regiones admitidas para los roles vinculados a servicios de AWS RAM

AWS RAM admite el uso de roles vinculados a servicios en todas las regiones en las que el servicio esté 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 de AWS RAM

En este tema se incluyen ejemplos de políticas de IAM de AWS RAM que explican 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 Cuentas de AWS externas

### 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 operadores `...IfExists`, consulte Operadores de condición ...IfExists en la Guía del usuario de IAM.

```
{
    "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.

Por ejemplo, la siguiente política solo permite a las entidades principales compartir reglas de solucionador.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["ram:CreateResourceShare", "ram:AssociateResourceShare"],
        "Resource": "*",
        "Condition": {
            "StringEqualsIfExists": {
                "ram:RequestedResourceType": "route53resolver:ResolverRule"
            }
        }
    }]
}
```

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

Puede usar una política de IAM para impedir que las entidades principales compartan recursos con Cuentas de AWS que no pertenezcan a su organización de AWS.

Por ejemplo, la siguiente política de IAM impide que las entidades principales añadan Cuentas de AWS externas a recursos compartidos.

```
{
```

```
    "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 (SCP). Las SCP son políticas que se asocian a elementos de una organización para administrar los permisos dentro de esa organización. Una SCP se aplica a todas las Cuentas de AWS incluidas en el elemento al que se asocia la SCP. Las políticas de control de servicios (SCP) permiten un control centralizado de los máximos permisos disponibles para todas las cuentas de la organización. Le ayudan a asegurarse de que sus Cuentas de AWS cumplan en todo momento las directrices de control de acceso de la organización. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations.

## Requisitos previos

Para usar políticas de control de servicios, 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 el uso de SCP en la organización. Para obtener más información, consulte Habilitar y deshabilitar tipos de políticas en la Guía del usuario de AWS Organizations.
- Cree las SCP que sean necesarias. Para obtener más información sobre cómo crear SCP, consulte Crear y actualizar SCP en la Guía del usuario de AWS Organizations.

## Ejemplo de políticas de control de servicios

### Contenido

- Ejemplo 1: Impedir la posibilidad de compartir externamente
- Ejemplo 2: Impedir que los usuarios acepten invitaciones a recursos compartidos desde cuentas externas a la organización
- Ejemplo 3: Permitir que determinadas cuentas compartan tipos de recursos específicos
- Ejemplo 4: Impedir que se comparta con toda la organización o con unidades organizativas
- Ejemplo 5: Permitir compartir solo con determinadas entidades principales

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.

```
{
    "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.

```
{
    "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.

```
{
    "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 Cuentas de AWS concretas de la organización, o bien con roles o usuarios de IAM.

```
{
    "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`.

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

```
                "ram:AssociateResourceShare",
                "ram:CreateResourceShare"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "ram:Principal": [
                        "arn:aws:organizations::123456789012:organization/
o-12345abcdef",
                        "arn:aws:organizations::123456789012:ou/o-12345abcdef/
ou-98765fedcba",
                        "111111111111"
                    ]
                }
            }
        }
    ]
}
```

## Deshabilitar el uso compartido de recursos con AWS Organizations

Si ha habilitado anteriormente el uso compartido con AWS Organizations y ya no necesita compartir recursos con toda la organización o con las unidades organizativas (OU), puede deshabilitar el uso compartido. Al deshabilitar el uso compartido con AWS Organizations, todas las organizaciones o unidades organizativas se eliminan de los recursos compartidos que haya creado y pierden el acceso dichos recursos.

Para deshabilitar el uso compartido con AWS Organizations

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

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

   > **Important**
   >
   > Cuando deshabilita el acceso de confianza a AWS Organizations, las entidades principales de sus organizaciones se eliminan de todos los recursos compartidos y pierden el acceso a dichos recursos.

2. Utilice la consola de IAM, AWS CLI o las operaciones de API de IAM para eliminar el rol vinculado a servicio AWSServiceRoleForResourceAccessManager. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

# Registro y monitorización en AWS RAM

La monitorización es una parte 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 CloudWatch Events

Proporciona un flujo de eventos del sistema prácticamente en tiempo real que describen los cambios en los recursos de AWS. CloudWatch Events habilita la informática basada en eventos automatizada, ya que puede escribir reglas que vigilen determinados eventos y desencadenen acciones automatizadas en otros servicios de AWS cuando estos eventos se produzcan. Para obtener más información, consulte Monitorizar AWS RAM mediante eventos de CloudWatch.

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 API de AWS RAM con AWS CloudTrail.

## Monitorizar AWS RAM mediante eventos de CloudWatch

Con Eventos de Amazon CloudWatch, puede configurar notificaciones automáticas para eventos específicos en AWS RAM. Los eventos de AWS RAM se entregan a Eventos de CloudWatch prácticamente en tiempo real. Puede configurar eventos de CloudWatch para monitorizar eventos e invocar destinos en respuesta a eventos que indican 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 cuando AWS RAM intenta emitir un evento, el servicio hará varios intentos más. Sin embargo, puede agotarse el tiempo de espera y provocar la pérdida de ese evento en concreto.

Para obtener más información, consulte la Guía del usuario de Eventos de Amazon CloudWatch.

## 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 monitorizar los errores de recursos compartidos, configure una regla de Eventos de Amazon CloudWatch que le avise cada vez que se produzca un error en un recurso compartido de AWS RAM. El procedimiento descrito en el siguiente tutorial utiliza un tema de Amazon Simple Notification Service (SNS) para notificar a todos los suscriptores del tema cada vez que 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. Abra la consola de Amazon EventBridge.
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 fallo de un recurso compartido de AWS RAM generará una alerta de SNS para los destinatarios del tema en el que ha publicado.

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 API de AWS RAM con AWS CloudTrail

AWS RAM se integra con AWS CloudTrail, un servicio que proporciona un registro de las acciones hechas por un usuario, un rol o un servicio de AWS en AWS RAM. CloudTrail captura todas las llamadas a la API de AWS RAM como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de AWS RAM y las llamadas desde el código a las operaciones de la API de AWS RAM. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3 que especifique, incluidos los eventos para AWS RAM. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de

CloudTrail en el Historial de eventos. Utilice la información que CloudTrail recopila para determinar la solicitud que se envió a AWS RAM, la dirección IP desde la que se realizó la solicitud, quién la realizó, cuándo la realizó y otros detalles.

Para obtener más información acerca de CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

## Información de AWS RAM en CloudTrail

CloudTrail se habilita en su Cuenta de AWS cuando se crea la cuenta. Cuando se produce actividad en AWS RAM, dicha actividad se registra en un evento de CloudTrail junto con otros eventos de servicio de AWS en el Historial de eventos. Puede ver, buscar y descargar eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de eventos en la Cuenta de AWS, incluidos los eventos de AWS RAM, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte lo siguiente:

- Creación de un registro de seguimiento para su Cuenta de AWS
- Integraciones de Servicio de AWS con registros de CloudTrail
- Configurar notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de registro de CloudTrail desde varias regiones y Recibir archivos de registro de CloudTrail desde varias cuentas

Todas las acciones de AWS RAM las registra CloudTrail y se documentan en la Referencia de la API de AWS RAM. Por ejemplo, las llamadas a las acciones `CreateResourceShare`, `AssociateResourceShare` y `EnableSharingWithAwsOrganization` 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.

- credenciales raíz de Cuenta de AWS

- Credenciales de seguridad temporales de un rol de AWS Identity and Access Management (IAM) o de un usuario federado.
- Credenciales de seguridad a largo plazo de un usuario de IAM.
- Otro servicio de AWS.

Para obtener más información, consulte Elemento userIdentity de CloudTrail.

## Descripción de las entradas de los archivos de registro de AWS RAM

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que especifique. Los archivos de registro de CloudTrail pueden contener una o varias entradas de registro. Un evento representa una solicitud específica realizada desde un origen cualquiera, y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

En el ejemplo siguiente se muestra una entrada de registro de CloudTrail para la acción `CreateResourceShare`.

```
{
    "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"
}
```

# Resiliencia en AWS RAM

La infraestructura global de AWS se divide en Regiones de AWS y zonas de disponibilidad. Las Regiones de AWS proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre las Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global de AWS.

# Seguridad de la infraestructura en AWS RAM

Como se trata de un servicio administrado, AWS Resource Access Manager está protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y cómo AWS protege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS con las prácticas recomendadas de seguridad de infraestructura, consulte Protección de la infraestructura en Portal de seguridad de AWS Well-Architected Framework.

Puede utilizar llamadas a la API publicadas en AWS para obtener acceso a AWS RAM a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Nosotros exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) tales como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

# Solución de problemas con AWS RAM

Utilice la información incluida en esta sección de la guía para diagnosticar y solucionar problemas frecuentes cuando trabaje con AWS Resource Access Manager (AWS RAM).

Temas



## Error: "Su ID de cuenta no existe en una organización de AWS"

### Escenario

Obtiene el error "Su ID de cuenta no existe en una organización de AWS" al intentar compartir un recurso con cuentas o unidades organizativas (OU) de su organización.

### Causa

Este error se puede producir cuando el rol vinculado al servicio AWSServiceRoleForResourceAccessManager no se crea correctamente al activar la integración entre AWS Resource Access Manager y 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.

1. Inicie sesión en la cuenta de administración de su organización con un rol o usuario de IAM que disponga de permisos administrativos.
2. Vaya a la página Servicios de la consola de AWS Organizations.

3. Seleccione RAM.
4. Seleccione Deshabilitar el acceso de confianza.
5. Vaya a la página Configuración de la consola de AWS RAM.
6. Seleccione la casilla Habilitar el uso compartido con AWS Organizations y, a continuación, seleccione Guardar configuración.

Ahora debería poder usar AWS RAM para compartir sus recursos con las cuentas y unidades organizativas de 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 que no se otorgan permisos suficientes en las políticas adjuntadas a su entidad principal de AWS Identity and Access Management (IAM). También puede deberse a las restricciones impuestas por una política de control de servicio (SCP) de AWS Organizations que afecte a su Cuenta de AWS.

## Solución

Para proporcionar acceso, añada permisos a sus usuarios, grupos o roles:

- Usuarios y grupos de AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones descritas en Crear un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center.
- Usuarios administrados 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 asumir. 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 añada 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, las SCP de su organización no deben bloquear los permisos.

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 reemplazarlo por el permiso "PutPolicy" (o equivalente) para el 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.

```
{
    "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-*xxxx* no encontrada"
- "CannotUpdateResourceShare: UnknownResourceException: OrganizationalUnit ou-*xxxx* no encontrada".

## Causa

Estos errores pueden producirse si habilita la integración entre AWS RAM y AWS Organizations utilizando la consola de Organizations o la API EnableAWSServiceAccess de Organizations en lugar la consola de AWS RAM. 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. Puesto que el rol no se crea, AWS RAM no puede acceder a los detalles relativos a las cuentas o unidades organizativas (OU) de su organización.

## Solución

Para resolver el problema, desactive la integración entre AWS RAM y AWS Organizations. A continuación, vuelva a activarla llamando a la operación EnableSharingWithAWSOrganization de la API de AWS RAM o utilizando la AWS Management Console para realizar los siguientes pasos.

1. Inicie sesión en la cuenta de administración de su organización con un rol o usuario de IAM que disponga de permisos administrativos.
2. Vaya a la página Servicios de la consola de AWS Organizations.
3. Seleccione RAM.
4. Seleccione Deshabilitar el acceso de confianza.
5. Vaya a la página Configuración de la consola de AWS RAM.
6. Seleccione la casilla Habilitar el uso compartido con AWS Organizations y, a continuación, seleccione Guardar configuración.

Ahora debería poder usar AWS RAM para compartir sus recursos con las cuentas y unidades organizativas de 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 intenta compartir solo se puede compartir dentro de su organización de AWS".
- "InvalidParameterException: el ID de cuenta de la entidad principal no pertenece a su organización de AWS. 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 organización de AWS".

## 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 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 AWS RAM y 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.

1. Inicie sesión en la cuenta de administración de su organización con un rol o usuario de IAM que disponga de permisos administrativos.
2. Vaya a la página Servicios de la consola de AWS Organizations.
3. Seleccione RAM.
4. Seleccione Deshabilitar el acceso de confianza.
5. Vaya a la página Configuración de la consola de AWS RAM.
6. Seleccione la casilla Habilitar el uso compartido con AWS Organizations y, a continuación, seleccione 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

### La opción de compartir con AWS Organizations se activó utilizando Organizations en lugar de AWS RAM

Si AWS Organizations se activó utilizando Organizations en lugar de 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 está 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.

1. Inicie sesión en la cuenta de administración de su organización con un rol o usuario de IAM que disponga de permisos administrativos.
2. Vaya a la página Servicios de la consola de AWS Organizations.
3. Seleccione RAM.
4. Seleccione Deshabilitar el acceso de confianza.
5. Vaya a la página Configuración de la consola de AWS RAM.
6. Seleccione la casilla Habilitar el uso compartido con AWS Organizations y, a continuación, seleccione 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 creó el recurso compartido, visualice el recurso compartido en la consola de AWS RAM. 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).

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

```
                "ram:Get*",
                "ram:List*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:<service>:<Region-code>:<Account-A-ID>:<resource-id>"
        }
    ]
}
```

### El recurso está en una Región de AWS diferente a la que figura en la configuración actual de la consola

AWS RAM es un servicio regional. Los recursos son específicos de determinadas Región de AWS y, para verlos, la AWS Management Console debe estar configurada para ver los recursos de dicha región.

La Región de AWS a la que la consola está accediendo 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

Obtiene el mensaje de error "Ha alcanzado el límite de recursos que puede compartir" o "ResourceShareLimitExceededException" al intentar compartir recursos.

### Causa

Estos errores se producen cuando se alcanza el número máximo de recursos que se pueden compartir utilizando el servicio de AWS RAM o el Servicio de AWS que creó el recurso que intenta 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 sus cuotas, en la Cuenta de AWS donde aparece el error, acceda a una de las siguientes páginas, dependiendo del tipo de cuota que haya alcanzado:
   - 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 su cuenta no tiene activado el uso compartido dentro de la organización de AWS, cuando comparta con otras cuentas, aunque pertenezcan a la misma organización de AWS, estas 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 intenta usar AWS RAM para compartir una subred de VPC con otra cuenta, la operación de compartir se realiza correctamente. Sin embargo, la cuenta consumidora muestra `LIMIT EXCEEDED` en relación con dicho recurso en la consola de AWS RAM.

## Causa

Algunos tipos de recursos individuales tienen restricciones específicas del servicio que son independientes de las restricciones impuestas por 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 por 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 AWS Support.

> **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 | 5000 |

| Recurso | Límite predeterminado |
| --- | --- |
| Número máximo de asociaciones de entidades principales por recurso compartido | 5000 |
| 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<br><br>**Note**<br>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<br><br>**Note**<br>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<br><br>• Esta cuota se aplica únicamente a las cuentas de envío que comparten con cuentas que no forman parte de la misma AWS Organizations.<br>• No existe una cuota que limite el número de invitaciones pendientes que puede tener una cuenta de recepción.<br>• 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 SKD de AWS

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 for C++ | Ejemplos de código de AWS SDK for C++ |
| AWS SDK for Go | Ejemplos de código de AWS SDK for Go |
| AWS SDK for Java | Ejemplos de código de AWS SDK for Java |
| AWS SDK for JavaScript | Ejemplos de código de AWS SDK for JavaScript |
| AWS SDK for .NET | Ejemplos de código de AWS SDK for .NET |
| AWS SDK for PHP | Ejemplos de código de AWS SDK for PHP |
| AWS SDK for Python (Boto3) | Ejemplos de código de AWS SDK for Python (Boto3) |
| AWS SDK for Ruby | Ejemplos de código de AWS SDK for Ruby |

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 ha añadido 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 su organización Cuentas de AWS o dentro de ella. | 21 de febrero de 2024 |
| Se ha agregado compatibilidad para compartir instantáneas de Amazon FSx para OpenZFS. | Ahora puede compartir las instantáneas de Amazon FSx para 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 | 14 de noviembre de 2023 |

| | | |
|---|---|---|
| | personas Cuentas de AWS de su organización. | |
| Se ha ampliado la compatibilidad para compartir recursos del Controlador de recuperación de aplicaciones de Amazon Route 53. | Ahora puede compartir los clústeres de Amazon Route 53 Application Recovery Controller con otras personas Cuentas de AWS o con las de su organización AWS RAM. | 18 de octubre de 2023 |
| Se ha añadido 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 |
| Se ha ampliado la compatibilidad 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 ha añadido compatibilidad con los grupos de SageMaker funciones y el SageMaker catálogo de Amazon Feature Store como recursos que se pueden compartir. | Ahora puedes compartir los grupos de SageMaker funciones y los recursos del SageMaker catálogo de Amazon Feature Store con otras personas Cuentas de AWS o con tu organización. | 20 de julio de 2023 |

| | | |
|---|---|---|
| Se ha incrementado el límite de cuota de servicio de 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 compatibilidad con las API de AWS AppSync GraphQL como recursos que se pueden compartir. | Ahora puedes compartir las API de AWS AppSync GraphQL con otras Cuentas de AWS personas con. AWS RAM | 24 de mayo de 2023 |
| Se agregó soporte para Acceso verificado de AWS grupos como recursos que se pueden compartir. | 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 compatibilidad con 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 |
| Se ha ampliado la compatibilidad con el servicio de Amazon VPC Lattice y los recursos de la red de servicios 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 |
| Actualización de las prácticas recomendadas de IAM. | Se ha actualizado la guía para adaptarla a las prácticas recomendadas de IAM. Para obtener más información, consulte prácticas recomendadas de seguridad en IAM. | 3 de enero de 2023 |
| Se ha ampliado la compatibilidad de 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 descripción general que describen AWS RAM y proporcionan una guía sobre cómo compartir un recurso con otros. Cuentas de AWS | 29 de agosto de 2022 |
| Se ha añadido soporte para Amazon SageMaker Pipelines. | Ahora puedes compartir SageMaker canalizaciones con otras personas. Cuentas de AWS | 2 de agosto de 2022 |

| | | |
|---|---|---|
| Se ha añadido compatibilidad con las AWS Service Catalog AppRegistry aplicaciones y los 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. | 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 se ha comprobado que cumple 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 externas 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 otros. Cuentas de AWS | 2 de diciembre de 2021 |
| Se agregó compatibilidad con 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 SageMaker los recursos de Amazon | Se puede utilizar AWS RAM para compartir grupos de SageMaker linaje. 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 la suya. 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 usarlo 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 (CA) Autoridad de certificación privada de AWS privadas con otras Cuentas de AWS. | 17 de agosto de 2020 |
| Se ha añadido compatibilidad 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 ha ampliado la compatibilidad 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 IPv4 AWS Outposts propiedad de los clientes. | Ahora puede utilizarlas AWS RAM para compartir las direcciones IPv4 AWS Outposts propiedad de los clientes con otras personas. Cuentas de AWS | 22 de abril de 2020 |
| Se agregó 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 usarlo AWS RAM para compartir hosts dedicados de Amazon EC2, grupos de AWS Resource Groups 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.