Manual do usuário

AWS Resource Access Manager

AWS Resource Access Manager: Manual do usuário

Table of Contents

O que é AWS Resource Access Manager?

AWS Resource Access Manager (AWS RAM) ajuda você a compartilhar com segurança seus recursos entre Contas da AWS, dentro de sua organização ou unidades organizacionais (OUs) e com funções e usuários AWS Identity and Access Management (IAM) para tipos de recursos compatíveis. Se você tiver vários Contas da AWS, poderá criar um recurso uma vez e usá-lo AWS RAM para tornar esse recurso utilizável por essas outras contas. Se sua conta for gerenciada por AWS Organizations, você poderá compartilhar recursos com todas as outras contas da organização ou somente com as contas contidas em uma ou mais unidades organizacionais especificadas (OUs). Você também pode compartilhar com um ID Contas da AWS de conta específico, independentemente de a conta fazer parte de uma organização. Alguns tipos de recursos compatíveis também permitem compartilhá-los com usuários e perfis especificados do IAM.

Conteúdo

Visões gerais do vídeo

O vídeo a seguir fornece uma breve introdução AWS RAM e descreve como criar um compartilhamento de recursos. Para obter mais informações, consulte ???.

O vídeo a seguir demonstra como aplicar permissões AWS gerenciadas aos seus AWS recursos. Para obter mais informações, consulte ???.

Este vídeo demonstra como criar e associar permissões gerenciadas pelo cliente seguindo as práticas recomendadas de privilégio mínimo. Para obter mais informações, consulte, ???.

Benefícios do AWS RAM

Por que usar AWS RAM? Oferece os seguintes benefícios:

- Reduz sua sobrecarga operacional — Crie um recurso uma vez e use-o AWS RAM para compartilhar esse recurso com outras contas. Isso elimina a necessidade de provisionar recursos duplicados em todas as contas, o que reduz a sobrecarga operacional. Dentro da conta proprietária do recurso, AWS RAM simplifica a concessão de acesso a todas as funções e usuários dessa conta sem precisar usar políticas de permissão baseadas em identidade.
- Fornece segurança e consistência: simplifique o gerenciamento da segurança de seus recursos compartilhados usando um único conjunto de políticas e permissões. Se, em vez disso, você criasse recursos duplicados em todas as suas contas separadas, teria a tarefa de implementar políticas e permissões idênticas e, em seguida, mantê-las idênticas em todas essas contas. Em vez disso, todos os usuários de um compartilhamento de AWS RAM recursos são gerenciados por um único conjunto de políticas e permissões. AWS RAM oferece uma experiência consistente para compartilhar diferentes tipos de AWS recursos.
- Fornece visibilidade e auditabilidade — Visualize os detalhes de uso de seus recursos compartilhados por meio da integração AWS RAM com a Amazon CloudWatch e. AWS CloudTrail AWS RAM fornece visibilidade abrangente de recursos e contas compartilhados.

E quanto ao acesso entre contas com políticas baseadas em recursos?

Você pode compartilhar alguns tipos de AWS recursos com outras pessoas Contas da AWS anexando uma política baseada em recursos que identifica AWS Identity and Access Management (IAM) principais (funções e usuários do IAM) fora da sua. Conta da AWS No entanto, compartilhar um recurso anexando uma política não tira proveito dos benefícios adicionais que ela AWS RAM oferece. Ao usar, AWS RAM você obtém os seguintes recursos:

- Você pode compartilhar com uma organização ou unidade organizacional (OU) sem precisar enumerar cada uma delas. Conta da AWS IDs
- Os usuários podem ver os recursos compartilhados com eles diretamente no console do AWS service (Serviço da AWS) de origem e nas operações da API, como se esses recursos estivessem diretamente na conta do usuário. Por exemplo, se você costuma AWS RAM compartilhar uma sub-rede da Amazon VPC com outra conta, os usuários dessa conta podem ver a sub-rede no console da Amazon VPC e nos resultados das operações da API da Amazon VPC realizadas nessa conta. Os recursos compartilhados ao anexar uma política baseada em recursos não são visíveis dessa

forma; em vez disso, você precisa descobrir e se referir explicitamente ao recurso pelo nome do recurso da Amazon (ARN).

- Os proprietários de um recurso podem ver quais entidades principais têm acesso a cada recurso individual que eles compartilharam.
- Se você compartilha recursos com uma conta que não faz parte da sua organização, AWS RAM inicia um processo de convite. O destinatário deve aceitar o convite antes que a entidade principal possa acessar os recursos compartilhados. Depois de ativar a capacidade de compartilhar dentro da sua organização, o compartilhamento com contas na organização não exige convites.

Se você tiver recursos compartilhados usando uma política de permissão baseada em recursos, poderá promovê-los a recursos totalmente AWS RAM gerenciados fazendo o seguinte:

- Use a operação de API PromoteResourceShareCreatedFromPolicy.
- Use o equivalente da operação da API, que é o promote-resource-share-created-from-policycomando AWS Command Line Interface (AWS CLI).

Como funciona o compartilhamento de recursos

Quando você compartilha um recurso na conta proprietária com outra Conta da AWS, a conta consumidora, você está concedendo acesso aos diretores da conta consumidora ao recurso compartilhado. Quaisquer políticas e permissões aplicáveis a usuários e perfis na conta de consumo também se aplicam ao recurso compartilhado. Os recursos no compartilhamento parecem recursos nativos no local com o Contas da AWS qual você os compartilhou.

Você pode compartilhar recursos globais e regionais. Para obter mais informações, consulte Compartilhamento de recursos regionais em comparação com recursos globais.

Compartilhar seus recursos da

Com AWS RAM, você compartilha recursos de sua propriedade criando um compartilhamento de recursos. Para criar um compartilhamento de recurso, especifique o seguinte:

- O Região da AWS no qual você deseja criar o compartilhamento de recursos. No console, escolha a Região na lista suspensa no canto superior direito do console. No AWS CLI, você usa o `--region` parâmetro.
  - Um compartilhamento de recurso pode conter somente recursos regionais que estão na mesma Região da AWS que o compartilhamento de recurso.

  - Um compartilhamento de recursos pode conter recursos globais somente se o compartilhamento de recursos estiver na região de origem designada para recursos globais, Leste dos EUA (Norte da Virgínia), `us-east-1`.
- Um nome para o compartilhamento de recursos.
- A lista de recursos aos quais você deseja conceder acesso como parte desse compartilhamento de recursos.
- As entidades principais às quais você concede acesso ao compartilhamento de recurso. Os diretores podem ser individuais Contas da AWS, as contas em uma organização ou unidade organizacional (OU) ou funções ou usuários individuais AWS Identity and Access Management (IAM). AWS Organizations

  > **Note**
  >
  > Nem todos os tipos de recursos podem ser compartilhados com perfis e usuários do IAM. Para obter informações sobre os recursos que você pode compartilhar com essas entidades principais, consulte Recursos compartilháveis AWS.

- Uma permissão gerenciada para associar a cada tipo de recurso incluído em um compartilhamento de recursos. A permissão gerenciada determina o que as entidades principais das outras contas podem fazer com os recursos no compartilhamento de recursos.

  O comportamento da permissão depende do tipo de entidade principal:

  - Se a entidade principal estiver em uma conta diferente daquela que possui o recurso, as permissões anexadas ao compartilhamento de recursos são as permissões máximas disponíveis para serem concedidas a usuários e perfis nessas contas. O administrador dessas contas deve então conceder aos papéis individuais e aos usuários acesso ao recurso compartilhado com políticas baseadas em identidade do IAM. As permissões concedidas nessas políticas não podem exceder as definidas nas permissões anexadas ao compartilhamento de recursos.

A conta proprietária do recurso mantém a propriedade total dos recursos que ela compartilha.

Uso dos recursos compartilhados

Quando o proprietário de um recurso o compartilha com sua conta, você pode acessar o recurso compartilhado como faria se ele pertencesse à sua conta. Você pode acessar o recurso usando o

console, os AWS CLI comandos e as operações de API do serviço relevante. As operações de API que as entidades principais da sua conta podem realizar variam de acordo com o tipo de recurso e são especificadas pelo AWS RAM permissão anexada ao compartilhamento de recursos. Todas as políticas do IAM e as políticas de controle de serviço configuradas em sua conta se aplicam, o que permite utilizar os investimentos existentes em controles de governança e segurança.

Quando você acessa um recurso compartilhado usando o serviço desse recurso, você tem as mesmas habilidades e limitações do Conta da AWS proprietário do recurso.

- Se o recurso for regional, você poderá acessá-lo somente a partir da Região da AWS em que ele existe na conta proprietária.
- Se o recurso for global, você poderá acessá-lo de qualquer Região da AWS que o console de serviço e as ferramentas do recurso suportem. Você pode visualizar e gerenciar o compartilhamento de recursos e seus recursos globais no AWS RAM console e nas ferramentas somente na região de origem designada, Leste dos EUA (Norte da Virgínia)`us-east-1`.

Acessando AWS RAM

Você pode trabalhar com AWS RAM qualquer uma das seguintes formas:

AWS RAM console

AWS RAM fornece uma interface de usuário baseada na web, o AWS RAM console. Se você se inscreveu em um Conta da AWS, você pode acessar o AWS RAM console entrando Console de gerenciamento da AWSe escolhendo na página inicial AWS RAM do console.

Você também pode navegar no seu navegador diretamente para o console do AWS RAM. Se você ainda não fez login, será pedido que faça isso antes que o console seja exibido.

AWS CLI e ferramentas para Windows PowerShell

O AWS CLI e Ferramentas da AWS para PowerShell fornece acesso direto às operações AWS RAM públicas da API. AWS suporta essas ferramentas em WindowsmacOS, Linux e. Para obter mais informações sobre os conceitos básicos, consulte o Guia do usuário do AWS Command Line Interface ou o Guia do usuário do AWS Tools for Windows PowerShell. Para obter mais informações sobre os comandos do AWS RAM, consulte a Referência de AWS CLI Comandos ou a Referência de AWS Tools for Windows PowerShell Cmdlet.

AWS SDKs

AWS fornece comandos de API para um amplo conjunto de linguagens de programação. Para obter mais informações sobre como começar, consulte o Guia de referência de ferramentas AWS SDKs e ferramentas.

API de consulta

Se você não usa uma das linguagens de programação suportadas, a API de consulta AWS RAM HTTPS fornece acesso programático a AWS RAM e. AWS Com a AWS RAM API, você pode emitir solicitações HTTPS diretamente para o serviço. Ao usar a AWS RAM API, você deve incluir um código para assinar digitalmente as solicitações usando suas credenciais. Para obter mais informações, consulte a Referência da API do AWS RAM.

Preços para AWS RAM

Não há cobranças adicionais pelo uso AWS RAM ou pela criação de compartilhamentos de recursos e pelo compartilhamento de seus recursos entre contas. As cobranças de uso de recursos variam de acordo com o tipo de recurso. Para obter mais informações sobre como AWS faturar recursos compartilháveis, consulte a documentação do serviço proprietário do recurso.

Conformidade e padrões internacionais

PCI DSS

AWS RAM suporta o processamento, armazenamento e transmissão de dados de cartão de crédito por um comerciante ou provedor de serviços e foi validado como compatível com o Padrão de Segurança de Dados (DSS) do Setor de Cartões de Pagamento (PCI).

Para obter mais informações sobre o PCI DSS, incluindo como solicitar uma cópia do pacote de conformidade com o PCI Compliance Package AWS , consulte Nível 1 do PCI DSS.

FedRAMP

AWS RAM está autorizado como FedRAMP Moderado nas Regiões da AWS seguintes áreas: Leste dos EUA (Norte da Virgínia), Leste dos EUA (Ohio), Oeste dos EUA (Norte da Califórnia) e Oeste dos EUA (Oregon).

AWS RAM está autorizado como FedRAMP High nas Regiões da AWS seguintes condições AWS GovCloud : (Oeste dos EUA) e (Leste dos EUA) AWS GovCloud .

O Federal Risk and Authorization Management Program (FedRAMP – Programa federal de gerenciamento de autorização e risco) é um programa do governo dos EUA que disponibiliza uma abordagem padronizada para avaliação de segurança, autorização e monitoramento contínuo de produtos e serviços na nuvem.

Para obter mais informações sobre conformidade com FedRAMP, consulte FedRAMP.

SOC e ISO

AWS RAM pode ser usado para cargas de trabalho sujeitas à conformidade com o Service Organization Control (SOC) e com os padrões ISO 9001, ISO 27001, ISO 27017, ISO 27018 e ISO 27701 da Organização Internacional de Padronização (ISO). Clientes de finanças, saúde e outros setores regulamentados podem obter informações sobre os processos e controles de segurança que protegem os dados dos clientes, que podem ser encontrados nos relatórios do SOC e nos certificados ISO e CSA STAR da AWS no AWS Artifact.

Para obter mais informações sobre a conformidade do SOC, consulte SOC.

Para obter mais informações sobre a conformidade com a ISO, consulte ISO 9001, ISO 27001, ISO 27017, ISO 27018 e ISO 27701.

Começando com AWS RAM

Com AWS Resource Access Manager, você pode compartilhar recursos que você possui com outras pessoas Contas da AWS. Se sua conta for gerenciada por AWS Organizations, você também poderá compartilhar recursos com as outras contas da sua organização. Você também pode usar recursos que foram compartilhados com você por outras Contas da AWS.

Se você não habilitar o compartilhamento interno AWS Organizations, não poderá compartilhar recursos com sua organização ou com as unidades organizacionais (OU) em sua organização. No entanto, você ainda pode compartilhar recursos com pessoas Contas da AWS da sua organização. Para tipos de recursos compatíveis, você também pode compartilhar recursos com usuários ou perfis individuais do AWS Identity and Access Management (IAM) em sua organização. Nesse caso, essas entidades principais são tratadas como se fossem contas externas, e não como parte de sua organização. Caso contrário, os consumidores receberão um convite para participar do compartilhamento de recursos e acesso ao compartilhado depois de aceitar o convite.

Conteúdo

Termos e conceitos para AWS RAM

Os conceitos a seguir ajudam a explicar como você pode usar AWS Resource Access Manager (AWS RAM) para compartilhar seus recursos.

Compartilhamento de recursos

Você compartilha recursos usando AWS RAM criando um compartilhamento de recursos. Um compartilhamento de recursos tem os três elementos a seguir:

- Uma lista de um ou mais AWS recursos a serem compartilhados.
- Uma lista de uma ou mais entidades principais às quais conceder acesso.
- Uma permissão gerenciada para cada tipo de recurso que você inclui no compartilhamento. Cada permissão gerenciada se aplica a todos os recursos desse tipo nesse compartilhamento de recursos.

Depois de usar AWS RAM para criar um compartilhamento de recursos, os principais especificados no compartilhamento de recursos podem ter acesso aos recursos do compartilhamento.

- Se você ativar o AWS RAM compartilhamento e os diretores com AWS Organizations quem você compartilha estiverem na mesma organização da conta de compartilhamento, esses diretores poderão receber acesso assim que o administrador da conta lhes conceder permissões para usar os recursos usando uma política de permissão AWS Identity and Access Management (IAM).
- Se você não ativar o AWS RAM compartilhamento com Organizations, ainda poderá compartilhar recursos com pessoas Contas da AWS que estão na sua organização. O administrador da conta consumidora recebe um convite para participar do compartilhamento de recursos e deve aceitar o convite antes que as entidades principais especificados no compartilhamento de recursos possam acessar os recursos compartilhados.
- Você também pode compartilhar com contas fora da sua organização, se o tipo de recurso for compatível. O administrador da conta consumidora recebe um convite para participar do compartilhamento de recursos e deve aceitar o convite antes que as entidades principais especificados no compartilhamento de recursos possam acessar os recursos compartilhados. Para obter informações sobre quais tipos de recursos oferecem suporte a esse tipo de compartilhamento, consulte Recursos compartilháveis AWS e visualize a coluna Pode compartilhar com contas fora da organização.

Contas compartilhadas

A conta de compartilhamento contém o recurso que é compartilhado e no qual o AWS RAM administrador cria o compartilhamento de AWS recursos usando AWS RAM.

Um AWS RAM administrador é um diretor do IAM que tem permissões para criar e configurar compartilhamentos de recursos no Conta da AWS. Como AWS RAM funciona anexando uma política baseada em recursos aos recursos em um compartilhamento de recursos, o AWS RAM administrador também deve ter permissões para chamar a `PutResourcePolicy` operação no AWS service (Serviço da AWS) para cada tipo de recurso incluído em um compartilhamento de recursos.

Entidades principais de consumo

A conta consumidora é Conta da AWS aquela com a qual um recurso é compartilhado. O compartilhamento de recursos pode especificar uma conta inteira como entidade principal ou, para alguns tipos de recursos, perfis ou usuários individuais na conta. Para obter informações sobre

quais tipos de recursos oferecem suporte a esse tipo de compartilhamento, consulte Recursos compartilháveis AWS e visualize a coluna Pode compartilhar com perfis do IAM e usuários.

AWS RAM também oferece suporte aos diretores de serviços como consumidores de compartilhamentos de recursos. Para obter informações sobre quais tipos de recursos oferecem suporte a esse tipo de compartilhamento, consulte Recursos compartilháveis AWS e visualize a coluna Pode compartilhar com entidades principais de serviço.

As entidades principais da conta consumidora podem realizar somente as ações permitidas pelas duas permissões a seguir:

- As permissões gerenciadas anexadas ao compartilhamento de recursos. Eles especificam as permissões máximas que podem ser concedidas às entidades principais na conta consumidora.
- As políticas baseadas em identidade do IAM anexadas a perfis ou usuários individuais pelo administrador do IAM na conta consumidora. Essas políticas devem conceder o acesso `Allow` às ações especificadas e ao Nome do recurso da Amazon (ARN) de um recurso na conta de compartilhamento.

AWS RAM é compatível com os seguintes tipos principais do IAM como consumidores de compartilhamentos de recursos:

- Outro Conta da AWS — O compartilhamento de recursos disponibiliza os recursos incluídos na conta de compartilhamento para a conta consumidora.
- Perfis individuais do IAM ou usuários em outra conta: alguns tipos de recursos oferecem suporte ao compartilhamento direto com usuários perfis individuais do IAM. Especifique esse tipo de entidade principal por seu ARN.
  - Perfil do IAM: `arn:aws:iam::123456789012:role/rolename`
  - Usuário do IAM: `arn:aws:iam::123456789012:user/username`
- Principal do serviço — Compartilhe um recurso com um AWS serviço para conceder ao serviço acesso a um compartilhamento de recursos. O compartilhamento principal do AWS serviço permite que um serviço execute ações em seu nome para aliviar a carga operacional.

  Para compartilhar com uma entidade principal de serviço, escolha permitir o compartilhamento com qualquer pessoa e, em Selecionar tipo de entidade principal, escolha Entidade principal de serviço na lista suspensa. Especifique o perfil da entidade principal de serviço no seguinte formato:
  - *`service-id`*`.amazonaws.com`

Para mitigar o risco de um substituto confuso, a política de recursos mostra o ID da conta do proprietário do recurso na chave de condição `aws:SourceAccount`.

- Contas em uma organização — Se a conta de compartilhamento for gerenciada por AWS Organizations, o compartilhamento de recursos poderá especificar a ID da organização para compartilhar com todas as contas da organização. Como alternativa, o compartilhamento de recursos pode especificar um ID de unidade organizacional (OU) para compartilhar com todas as contas dessa OU. Uma conta de compartilhamento só pode ser compartilhada com sua própria organização ou OU IDs dentro de sua própria organização. Especifique as contas em uma organização pelo ARN da organização ou da OU.
  - Todas as contas em uma organização: a seguir está um exemplo de ARN de uma organização no: AWS Organizations

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

  - Todas as contas em uma unidade organizacional: a seguir está um exemplo de ARN de um ID de OU:

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

> **Important**
>
> Quando você compartilha com uma organização ou uma OU, e esse escopo inclui a conta que possui o compartilhamento de recursos, todas as entidades principais na conta de compartilhamento obtêm acesso automático aos recursos no compartilhamento. O acesso concedido é definido pelas permissões gerenciadas associadas ao compartilhamento. Isso ocorre porque a política baseada em recursos AWS RAM anexada a cada recurso no compartilhamento usa. `"Principal": "*"` Para obter mais informações, consulte Implicações do uso de "Principal": "*" em uma política baseada em recursos.
> As entidades principais das outras contas consumidoras não têm acesso imediato aos recursos do compartilhamento. Os administradores das outras contas devem primeiro anexar políticas de permissão baseadas em identidade às entidades principais apropriadas. Essas políticas devem conceder `Allow` acesso aos ARNs recursos individuais no compartilhamento de recursos. As permissões nessas políticas não podem exceder as especificadas na permissão gerenciada associada ao compartilhamento de recursos.

Política baseada em recursos

Políticas baseadas em recurso são documentos de texto JSON que implementam a linguagem de políticas do IAM. Ao contrário das políticas baseadas em identidade que você anexa ao principal, como uma função ou usuário do IAM, você anexa políticas baseadas em recursos ao recurso. AWS RAM cria políticas baseadas em recursos em seu nome com base nas informações que você fornece para seu compartilhamento de recursos. Você deve especificar um elemento de política `Principal` que determine quem pode acessar o recurso. Para obter mais informações, consulte Políticas baseadas em identidade e em recurso no Guia do usuário do IAM.

As políticas baseadas em recursos geradas pelo AWS RAM são avaliadas junto com todos os outros tipos de políticas do IAM. Isso inclui todas as políticas baseadas em identidade do IAM anexadas aos diretores que estão tentando acessar o recurso, e as políticas de controle de serviço (SCPs) para AWS Organizations isso podem se aplicar ao. Conta da AWS As políticas baseadas em recursos geradas pela AWS RAM participam da mesma lógica de avaliação de políticas de todas as outras políticas do IAM. Para obter detalhes completos sobre a avaliação de políticas e como determinar as permissões resultantes, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

AWS RAM fornece uma experiência de compartilhamento de recursos simples e segura, fornecendo políticas de easy-to-use abstração baseadas em recursos.

Para os tipos de recursos que oferecem suporte a políticas baseadas em recursos, constrói e gerencia AWS RAM automaticamente as políticas baseadas em recursos para você. Para um determinado recurso, o AWS RAM cria a política baseada em recursos combinando as informações de todos os compartilhamentos de recursos que incluem esse recurso. Por exemplo, considere um pipeline de SageMaker IA da Amazon que você compartilha usando AWS RAM e inclui em dois compartilhamentos de recursos diferentes. Você pode usar um compartilhamento de recursos para fornecer acesso somente de leitura a toda a sua organização. Em seguida, você poderia usar o outro compartilhamento de recursos para conceder somente permissões de execução de SageMaker IA a uma única conta. AWS RAM combina automaticamente esses dois conjuntos diferentes de permissões em uma única política de recursos com várias declarações. Em seguida, anexa a política combinada baseada em recursos ao recurso do pipeline. Você pode ver essa política de recursos subjacente chamando a GetResourcePolicyoperação. Serviços da AWS em seguida, use essa política baseada em recursos para autorizar qualquer diretor que tente realizar uma ação no recurso compartilhado.

Embora você possa criar manualmente as políticas baseadas em recursos e anexá-las aos seus recursos por meio de uma chamada `PutResourcePolicy`, recomendamos que você use o AWS RAM , porque elas oferecem as seguintes vantagens:

- Possibilidade de descoberta para consumidores de ações — se você compartilha recursos usando AWS RAM, os usuários podem ver todos os recursos compartilhados com eles diretamente no console do serviço proprietário do recurso e nas operações de API, como se esses recursos estivessem diretamente na conta do usuário. Por exemplo, se você compartilhar um AWS CodeBuild projeto com outra conta, os usuários da conta consumidora poderão ver o projeto no CodeBuild console e nos resultados das operações de CodeBuild API realizadas. Os recursos compartilhados pela anexação direta de uma política baseada em recursos não são visíveis dessa forma. Em vez disso, você deve descobrir e se referir explicitamente ao recurso por meio de seu ARN.
- Capacidade de gerenciamento para proprietários de ações — Se você compartilha recursos usando AWS RAM, os proprietários de recursos na conta de compartilhamento podem ver centralmente quais outras contas têm acesso aos seus recursos. Se você compartilhar um recurso usando uma política baseada em recursos, poderá ver as contas consumidoras somente examinando a política de recursos individuais no console de serviço ou na API relevante.
- Eficiência — Se você compartilhar recursos usando AWS RAM, poderá compartilhar vários recursos e gerenciá-los como uma unidade. Recursos compartilhados usando somente políticas baseadas em recursos exigem políticas individuais anexadas a cada recurso que você compartilha.
- Simplicidade — Com isso AWS RAM, você não precisa entender a linguagem de política do IAM baseada em JSON. AWS RAM fornece permissões ready-to-use AWS gerenciadas que você pode escolher para anexar aos seus compartilhamentos de recursos.

Ao usar AWS RAM, você pode até mesmo compartilhar alguns tipos de recursos que ainda não oferecem suporte a políticas baseadas em recursos. Para esses tipos de recursos, gera AWS RAM automaticamente uma política baseada em recursos como uma representação das permissões reais. Os usuários podem ver essa representação chamando GetResourcePolicy. Esse recurso inclui as seguintes informações:

- Amazon Aurora: clusters de banco de dados
- Amazon EC2: reservas de capacidade e hosts dedicados
- AWS License Manager — Configurações de licença
- AWS Outposts — Tabelas de rotas de gateway local, postos avançados e sites

- Amazon Route 53: regras de encaminhamento
- Amazon Virtual Private Cloud — IPv4 Endereços de propriedade do cliente, listas de prefixos, sub-redes, alvos de espelhamento de tráfego, gateways de trânsito e domínios multicast de gateway de trânsito

Exemplos de políticas baseadas em recursos AWS RAM geradas

Se você compartilhar um recurso de imagem do EC2 Image Builder com uma conta individual AWS RAM , gera uma política semelhante ao exemplo a seguir e a anexa a todos os recursos de imagem incluídos no compartilhamento de recursos.

JSON

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

Se você compartilhar um recurso de imagem do EC2 Image Builder com uma função ou usuário do IAM em Conta da AWS outra AWS RAM , gera uma política semelhante ao exemplo a seguir e a anexa a todos os recursos de imagem incluídos no compartilhamento de recursos.

JSON

```
{
```

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

Se você compartilhar um recurso de imagem do EC2 Image Builder com todas as contas em uma organização ou com as contas de uma OU AWS RAM , gera uma política semelhante ao exemplo a seguir e a anexa a todos os recursos de imagem incluídos no compartilhamento de recursos.

> **Note**
>
> Essa política usa `"Principal": "*"` e, em seguida, usa o elemento `"Condition"` para restringir as permissões às identidades que correspondam às `PrincipalOrgID` especificadas. Para obter mais informações, consulte Implicações do uso de "Principal": "*" em uma política baseada em recursos.

JSON

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

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

Implicações do uso de "Principal": "*" em uma política baseada em recursos

Quando você inclui `"Principal": "*"` em uma política baseada em recursos, a política concede acesso a todas as entidades principais do IAM na conta que contém o recurso, sujeita a quaisquer restrições impostas por um elemento `Condition`, se ele existir. Declarações `Deny` explícitas em qualquer política que se aplique à entidade principal da chamada substituem as permissões concedidas por essa política. No entanto, uma `Deny` implícita (ou seja, a falta de uma `Allow` explícita) em qualquer política de identidade, políticas de limite de permissões ou políticas de sessão aplicáveis não resulta em uma `Deny` para o acesso de concessão às entidades principais a uma ação por meio dessa política baseada em recursos.

Se esse comportamento não for desejável para seu cenário, você pode limitar esse comportamento adicionando uma declaração `Deny` explícita a uma política de identidade, limite de permissões ou política de sessão que afete os perfis e os usuários relevantes.

Permissões gerenciadas

As permissões gerenciadas definem quais ações as entidades principais podem realizar sob quais condições nos tipos de recursos compatíveis em um compartilhamento de recursos. Ao criar um compartilhamento de recursos, você deve especificar qual permissão gerenciada usar para cada tipo de recurso incluído no compartilhamento de recursos. Uma permissão gerenciada lista o conjunto `actions` e as condições que os diretores podem executar com o recurso compartilhado usando AWS RAM.

Você pode anexar somente uma permissão gerenciada para cada tipo de recurso em um compartilhamento de recursos. Você não pode criar um compartilhamento de recursos no qual alguns recursos de um determinado tipo usem uma permissão gerenciada e outros recursos do

mesmo tipo usem uma permissão gerenciada diferente. Para fazer isso, você precisaria criar dois compartilhamentos de recursos diferentes e dividir os recursos entre eles, dando a cada conjunto uma permissão gerenciada diferente. Há dois tipos diferentes de permissões gerenciadas:

AWS permissões gerenciadas

AWS as permissões gerenciadas são criadas e mantidas AWS e concedem permissões para cenários comuns de clientes. AWS RAM define pelo menos uma permissão AWS gerenciada para cada tipo de recurso compatível. Alguns tipos de recursos oferecem suporte a mais de uma permissão AWS gerenciada, com uma permissão gerenciada designada como AWS padrão. A permissão AWS gerenciada padrão está associada, a menos que você especifique o contrário.

Pode usar permissões gerenciadas pelo cliente

As permissões gerenciadas pelo cliente são permissões gerenciadas que você cria e mantém especificando com precisão quais ações podem ser executadas sob quais condições com recursos compartilhados usando o AWS RAM. Por exemplo, você quer limitar o acesso de leitura aos seus grupos do Gerenciador de endereços IP (IPAM) da Amazon VPC, que ajudam você a gerenciar seus endereços IP em grande escala. Você pode criar permissões gerenciadas pelo cliente para que seus desenvolvedores atribuam endereços IP, mas não visualizem o intervalo de endereços IP que outras contas de desenvolvedor atribuem. É possível seguir as práticas recomendadas de privilégio mínimo, conceda apenas as permissões necessárias para executar tarefas em recursos compartilhados.

Você define sua própria permissão para um tipo de recurso em um compartilhamento de recursos com a opção de adicionar condições como chaves de contexto global e chaves específicas do serviço para especificar as condições sob as quais as entidades principais têm acesso ao recurso. Essas permissões podem ser usadas em um ou mais AWS RAM compartilhamentos. As permissões gerenciadas pelo cliente são específicas da região.

AWS RAM usa permissões gerenciadas como uma entrada para criar as políticas baseadas em recursos para os recursos que você compartilha.

Versão da permissão gerenciada

Qualquer alteração em uma permissão gerenciada é representada como uma nova versão dessa permissão gerenciada. A nova versão é a padrão para todos os novos compartilhamentos de recursos. Cada permissão gerenciada sempre tem uma versão designada como padrão. Ao AWS criar ou criar uma nova versão de permissão gerenciada, você deve atualizar explicitamente a

permissão gerenciada para cada compartilhamento de recursos existente. Você pode avaliar as alterações antes de aplicá-las ao seu compartilhamento de recursos nesta etapa. Todos os novos compartilhamentos de recursos usarão automaticamente a nova versão da permissão gerenciada para o tipo de recurso correspondente.

AWS versões de permissão gerenciada

AWS lida com todas as alterações nas permissões AWS gerenciadas. Essas mudanças abordam novas funcionalidades ou eliminam as deficiências descobertas. Você só pode aplicar a versão de permissão gerenciada padrão aos seus compartilhamentos de recursos.

Versões de permissão gerenciadas pelo cliente

Você gerencia todas as alterações nas permissões gerenciadas pelo cliente. Você pode criar uma nova versão padrão, definir uma versão mais antiga como padrão ou excluir versões que não estão mais associadas a nenhum compartilhamento de recursos. Cada permissão gerenciada pelo cliente pode ter até cinco versões.

Ao criar ou atualizar um compartilhamento de recursos, você pode anexar somente a versão padrão da permissão gerenciada especificada. Para obter mais informações, consulte Atualização de permissões AWS gerenciadas para uma versão mais recente.

Compartilhando seus AWS recursos

Para compartilhar um recurso que você possui usando AWS RAM, faça o seguinte:

- Habilite o compartilhamento de recursos dentro AWS Organizations (opcional)
- Criar o compartilhamento de um recurso

Observações

- Compartilhar um recurso com diretores fora dos Conta da AWS proprietários do recurso não altera as permissões ou as cotas que se aplicam ao recurso na conta que o criou.
- AWS RAM é um serviço regional. Os diretores com os quais você compartilha podem acessar compartilhamentos de recursos somente no local Regiões da AWS em que os recursos foram criados.

- Alguns recursos têm considerações e pré-requisitos especiais para compartilhamento. Para obter mais informações, consulte Recursos compartilháveis AWS.

Habilite o compartilhamento de recursos dentro AWS Organizations

Quando sua conta é gerenciada por AWS Organizations, você pode aproveitar isso para compartilhar recursos com mais facilidade. Com ou sem Organizações, um usuário pode compartilhar com contas individuais. No entanto, se a sua conta estiver em uma organização, você poderá compartilhar com contas individuais ou com todas as contas na organização ou em uma UO sem precisar enumerar cada conta.

Para compartilhar recursos dentro de uma organização, você deve primeiro usar o AWS RAM console ou AWS Command Line Interface (AWS CLI) para habilitar o compartilhamento com AWS Organizations. Quando você compartilha recursos em sua organização, AWS RAM não envia convites aos diretores. As entidades principais da organização obtêm acesso a recursos compartilhados sem trocar convites.

Quando você ativa o compartilhamento de recursos em sua organização, AWS RAM cria uma função vinculada ao serviço chamada. **`AWSServiceRoleForResourceAccessManager`** Essa função pode ser assumida somente pelo AWS RAM serviço e concede AWS RAM permissão para recuperar informações sobre a organização da qual é membro, usando a política AWS `AWSResourceAccessManagerServiceRolePolicy` gerenciada.

> **Note**
>
> Por padrão, quando você ativa o compartilhamento com AWS Organizations, o compartilhamento de recursos em sua organização restringe o acesso aos consumidores dentro da mesma organização. Se uma conta de consumidor sair da organização, essa conta perderá o acesso aos recursos no compartilhamento de recursos. Essa restrição se aplica se você compartilha recursos com uma OU, com toda a organização ou com uma conta individual na organização.
> Para account-to-account compartilhar dentro da sua organização,
> você pode manter o acesso ao compartilhamento quando as contas `RetainSharingOnAccountLeaveOrganization` saírem configurando como `True` quando você cria um novo compartilhamento de recursos. Com essa configuração ativada, AWS RAM envia um convite para a conta consumidora (semelhante ao compartilhamento

com contas externas). A conta mantém o acesso aos recursos compartilhados mesmo que saia da organização.
A `RetainSharingOnAccountLeaveOrganization` configuração tem os seguintes requisitos e limitações:

- `allowExternalPrincipals`Requer ser `True`
- Só pode ser definido ao criar novos compartilhamentos de recursos
- Não se aplica ao compartilhamento com OUs ou com toda a organização
- Quando `RetainSharingOnAccountLeaveOrganization` está definido como`True`, você não pode usar compartilhamentos de recursos para compartilhar recursos que só podem ser compartilhados dentro de uma organização.

Se você não precisar mais compartilhar recursos com toda a organização ou OUs desabilitar o compartilhamento de recursos. Para obter mais informações, consulte Desativando o compartilhamento de recursos com AWS Organizations.

Permissões mínimas

Para executar os procedimentos abaixo, você deve fazer login como entidade principal na conta de gerenciamento da organização que tem as seguintes permissões:

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

Requisitos

- Você pode executar essas etapas somente quando tiver feito login como entidade principal na conta de gerenciamento da organização.
- A organização deve ter todos os atributos habilitados. Para obter mais informações, consulte Enabling all features in your organization no Manual do usuário do AWS Organizations .

> **Important**
>
> Você deve habilitar o compartilhamento com AWS Organizations usando o AWS RAM console ou o AWS CLI comando enable-sharing-with-aws-organization. Isso garante que a função vinculada ao serviço `AWSServiceRoleForResourceAccessManager` seja criada. Se você habilitar o acesso confiável AWS Organizations usando o AWS Organizations console ou o enable-aws-service-access AWS CLI comando, a função `AWSServiceRoleForResourceAccessManager` vinculada ao serviço não será criada e você não poderá compartilhar recursos em sua organização.

Console

Para ativar o compartilhamento de recursos em sua organização

1. Abra a página Configurações no AWS RAM console.
2. Escolha Habilitar compartilhamento com e AWS Organizations, em seguida, escolha Salvar configurações.

AWS CLI

Para ativar o compartilhamento de recursos em sua organização

Use o comando enable-sharing-with-aws-organization.

Esse comando pode ser usado em qualquer Região da AWS um e permite o compartilhamento com AWS Organizations todas as regiões nas quais AWS RAM é suportado.

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

Criar o compartilhamento de um recurso

Para compartilhar recursos de sua propriedade, crie um compartilhamento de recursos. Aqui está uma visão geral do processo:

1. Adicione os recursos que você deseja compartilhar.

2. Para cada tipo de recurso que você incluir no compartilhamento, especifique a permissão gerenciada a ser usada para esse tipo de recurso.
   - Você pode escolher entre uma das permissões AWS gerenciadas disponíveis, uma permissão gerenciada pelo cliente existente ou criar uma nova permissão gerenciada pelo cliente.
   - AWS as permissões gerenciadas são criadas por AWS para cobrir casos de uso padrão.
   - As permissões gerenciadas pelo cliente permitem que você personalize suas próprias permissões gerenciadas para atender às suas necessidades comerciais e de segurança.

   > **Note**
   >
   > Se a permissão gerenciada selecionada tiver várias versões, AWS RAM anexará automaticamente a versão padrão. Você pode anexar somente a versão designada como padrão.

3. Especifique as entidades principais que você deseja que tenham acesso aos recursos.

Considerações

- Se, posteriormente, você precisar excluir um AWS recurso incluído em um compartilhamento, recomendamos que primeiro remova o recurso de qualquer compartilhamento de recursos que o inclua ou exclua o compartilhamento de recursos.
- Os tipos de recursos que você pode incluir em um compartilhamento de recursos estão listados em Recursos compartilháveis AWS.
- Você só poderá compartilhar um recurso se for o proprietário dele. Não é possível compartilhar um recurso compartilhado com você.
- AWS RAM é um serviço regional. Quando você compartilha um recurso com entidades principais em outras Contas da AWS, essas entidades principais devem acessar cada recurso da mesma Região da AWS em que foi criado. Para recursos globais compatíveis, você pode acessar esses recursos de qualquer um Região da AWS que seja compatível com o console de serviço e as ferramentas desse recurso. Você pode visualizar esses compartilhamentos de recursos e seus recursos globais no console do AWS RAM e nas ferramentas somente na região de origem designada, Leste dos EUA (Norte da Virgínia), `us-east-1`. Para obter mais informações AWS RAM e recursos globais, consulteCompartilhamento de recursos regionais em comparação com recursos globais.
- Se a conta da qual você está compartilhando fizer parte de uma organização AWS Organizations e o compartilhamento dentro da sua organização estiver ativado, todos os diretores da organização

com a qual você compartilha recebem automaticamente acesso aos compartilhamentos de recursos sem o uso de convites. Uma entidade principal em uma conta com a qual você compartilha fora do contexto de uma organização recebe um convite para ingressar no compartilhamento de recursos e acesso aos recursos compartilhados somente após aceitar o convite.

- Se você compartilhar com uma entidade principal de serviço, não poderá associar nenhuma outra entidade principal ao compartilhamento de recursos.
- Se o compartilhamento for entre contas ou entidades principais que fazem parte de uma organização, qualquer alteração na associação à organização afetará dinamicamente o acesso ao compartilhamento de recursos.
  - Se você adicionar um Conta da AWS à organização ou a uma OU que tenha acesso a um compartilhamento de recursos, essa nova conta de membro automaticamente terá acesso ao compartilhamento de recursos. O administrador da conta com a qual você compartilhou pode então conceder às entidades principais individuais dessa conta acesso aos recursos desse compartilhamento.
  - Se você remover uma conta da organização ou de uma OU que tenha acesso a um compartilhamento de recursos, todas as entidades principais dessa conta perderão automaticamente o acesso aos recursos que foram acessados por meio desse compartilhamento de recursos.
  - Se você compartilhou diretamente com uma conta membro ou com perfis do IAM ou usuários na conta membro e depois remover essa conta da organização, todas as entidades principais dessa conta perderão o acesso aos recursos que foram acessados por meio desse compartilhamento de recursos.

> **Important**
>
> Quando você compartilha com uma organização ou uma OU, e esse escopo inclui a conta que possui o compartilhamento de recursos, todas as entidades principais na conta de compartilhamento obtêm acesso automático aos recursos no compartilhamento. O acesso concedido é definido pelas permissões gerenciadas associadas ao compartilhamento. Isso ocorre porque a política baseada em recursos AWS RAM anexada a cada recurso no compartilhamento usa. `"Principal": "*"` Para obter mais informações, consulte Implicações do uso de "Principal": "*" em uma política baseada em recursos.
> As entidades principais das outras contas consumidoras não têm acesso imediato aos recursos do compartilhamento. Os administradores das outras contas devem primeiro anexar políticas de permissão baseadas em identidade às entidades principais

apropriadas. Essas políticas devem conceder `Allow` acesso aos ARNs recursos individuais no compartilhamento de recursos. As permissões nessas políticas não podem exceder as especificadas na permissão gerenciada associada ao compartilhamento de recursos.

- Você pode adicionar somente a organização da qual sua conta é membro e OUs dessa organização aos seus compartilhamentos de recursos. Você não pode adicionar organizações OUs de fora da sua própria organização a um compartilhamento de recursos como diretores. No entanto, você pode adicionar funções individuais Contas da AWS ou, para serviços compatíveis, usuários e funções do IAM de fora da sua organização como diretores de um compartilhamento de recursos.

  Note

  Nem todos os tipos de recursos podem ser compartilhados com perfis e usuários do IAM. Para obter informações sobre os recursos que você pode compartilhar com essas entidades principais, consulte Recursos compartilháveis AWS.

- Para os seguintes tipos de recursos, você tem sete dias para aceitar o convite para participar do compartilhamento para os seguintes tipos de recursos. Se você não aceitar o convite antes que ele expire, ele será automaticamente recusado.

  Important

  Para tipos de recursos compartilhados que não estão na lista a seguir, você tem 12 horas para aceitar o convite para participar do compartilhamento de recursos. Depois de 12 horas, o convite expira e o usuário final da entidade principal no compartilhamento de recursos é desassociado. O convite não pode mais ser aceito pelos usuários finais.

  - Amazon Aurora: clusters de banco de dados
  - Amazon EC2: reservas de capacidade e hosts dedicados
  - AWS License Manager — Configurações de licença
  - AWS Outposts — Tabelas de rotas de gateway local, postos avançados e sites
  - Amazon Route 53: regras de encaminhamento

- Amazon VPC — IPv4 endereços de propriedade do cliente, listas de prefixos, sub-redes, alvos de espelhamento de tráfego, gateways de trânsito, domínios multicast de gateway de trânsito

Console

Criar o compartilhamento de um recurso

1. Abra o console do AWS RAM.
2. Como existem compartilhamentos de AWS RAM recursos específicos Regiões da AWS, escolha o apropriado na Região da AWS lista suspensa no canto superior direito do console. Para ver os compartilhamentos de recursos que contêm recursos globais, você deve Região da AWS definir o como Leste dos EUA (Norte da Virgínia), (`us-east-1`). Para obter mais informações sobre o compartilhamento de recursos globais, consulte Compartilhamento de recursos regionais em comparação com recursos globais. Se você quiser incluir recursos globais no compartilhamento de recursos, deverá escolher a região de origem designada, Leste dos EUA (Norte da Virgínia), `us-east-1`.
3. Se você é novato AWS RAM, escolha Criar um compartilhamento de recursos na página inicial. Caso contrário, escolha Criar compartilhamento de recursos na página Compartilhado por mim: compartilhamentos de recursos.
4. Na Etapa 1: Especificar detalhes do compartilhamento de recursos, faça o seguinte:

   a. Em Nome, insira um nome descritivo para o compartilhamento de recursos.

   b. Em Recursos, escolha recursos para adicionar ao compartilhamento de recursos da seguinte forma:

      - Em Selecionar tipo de recurso, selecione o tipo de recurso para compartilhar. Isso filtra a lista de recursos compartilháveis para os recursos do tipo selecionado.
      - Na lista de recursos resultante, marque as caixas de seleção ao lado dos recursos individuais que você deseja compartilhar. Os recursos selecionados são movidos para Recursos selecionados.

        Se você estiver compartilhando recursos associados a uma zona de disponibilidade específica, usar o ID da zona de disponibilidade (ID de AZ) ajudará a determinar a localização relativa desses recursos nas contas. Para obter mais informações, consulte IDs de zona de disponibilidade para seus recursos da AWS.

c. (Opcional) Para anexar tags ao compartilhamento de recursos, em Tags, insira uma chave e um valor de tag. Adicione outras escolhendo Adicionar nova tag. Repita esta etapa conforme necessário. Essas tags se aplicam somente ao compartilhamento de recursos em si, não aos recursos no compartilhamento de recursos.

5. Escolha Próximo.

6. Na Etapa 2: Associar uma permissão gerenciada a cada tipo de recurso, você pode optar por associar uma permissão gerenciada criada por AWS ao tipo de recurso, escolher uma permissão gerenciada pelo cliente existente ou criar sua própria permissão gerenciada pelo cliente para os tipos de recursos compatíveis. Para obter mais informações, consulte Tipos de permissões gerenciadas.

   Escolha Criar permissão gerenciada pelo cliente para criar uma permissão gerenciada pelo cliente que atenda aos requisitos do seu caso de uso de compartilhamento. Para obter mais informações, consulte Criar uma permissão gerenciada pelo cliente. Depois de concluir o processo, escolha

   e selecione sua nova permissão gerenciada pelo cliente na lista suspensa Permissões gerenciadas.

   > **Note**
   >
   > Se a permissão gerenciada selecionada tiver várias versões, o AWS RAM anexará automaticamente a versão padrão. Você pode anexar somente a versão designada como padrão.

   Para exibir as ações que a permissão gerenciada permite, expanda Exibir o modelo de política dessa permissão gerenciada.

7. Escolha Próximo.

8. Na Etapa 3: Conceder acesso às entidades principais, faça o seguinte:

   a. Por padrão, a opção Permitir compartilhamento com qualquer pessoa está selecionada, o que significa que, para os tipos de recursos que o suportam, você pode compartilhar recursos com pessoas Contas da AWS que estão fora da sua organização. Isso não afeta os tipos de recursos que podem ser compartilhados somente dentro de uma

organização, como as sub-redes da Amazon VPC. Você também pode compartilhar alguns tipos de recursos compatíveis com perfis e usuários do IAM.

Para restringir o compartilhamento de recursos somente a contas e entidades principais em sua organização, escolha Permitir compartilhamento somente dentro de sua organização.

b. Para entidades principais, faça o seguinte:

- Para adicionar a organização, uma unidade organizacional (OU) ou uma Conta da AWS que faça parte de uma organização, ative Exibir estrutura organizacional. Isso exibe uma visualização em árvore da sua organização. Em seguida, marque a caixa de seleção ao lado de cada entidade principal que você deseja adicionar.

> **Important**
>
> Quando você compartilha com uma organização ou uma OU, e esse escopo inclui a conta que possui o compartilhamento de recursos, todas as entidades principais na conta de compartilhamento obtêm acesso automático aos recursos no compartilhamento. O acesso concedido é definido pelas permissões gerenciadas associadas ao compartilhamento. Isso ocorre porque a política baseada em recursos AWS RAM anexada a cada recurso no compartilhamento usa. `"Principal": "*"` Para obter mais informações, consulte Implicações do uso de "Principal": "*" em uma política baseada em recursos.
>
> As entidades principais das outras contas consumidoras não têm acesso imediato aos recursos do compartilhamento. Os administradores das outras contas devem primeiro anexar políticas de permissão baseadas em identidade às entidades principais apropriadas. Essas políticas devem conceder `Allow` acesso aos ARNs recursos individuais no compartilhamento de recursos.
>
> As permissões nessas políticas não podem exceder as especificadas na permissão gerenciada associada ao compartilhamento de recursos.

- Se você selecionar a organização (o ID começa com `o-`), as entidades principais de todas as Contas da AWS na organização poderão acessar o compartilhamento de recursos.

- Se você selecionar uma OU (a ID começa com `ou-`), os diretores de toda Contas da AWS a UO e seu filho OUs poderão acessar o compartilhamento de recursos.
- Se você selecionar um indivíduo Conta da AWS, somente os diretores dessa conta poderão acessar o compartilhamento de recursos.

> **Note**
>
> A opção Exibir estrutura organizacional aparecerá somente se o compartilhamento com o AWS Organizations estiver ativado e você estiver conectado à conta de gerenciamento da organização.
> Você não pode usar esse método para especificar uma Conta da AWS externa à sua organização ou um usuário ou perfil do IAM. Em vez disso, você deve desativar Exibir estrutura organizacional e usar a lista suspensa e a caixa de texto para inserir o ID ou o ARN.

- Para especificar uma entidade principal por ID ou ARN, incluindo entidades principais que estão fora da organização, selecione o tipo de entidade principal para cada entidade principal. Em seguida, insira o ID (para uma Conta da AWS organização ou OU) ou o ARN (para uma função ou usuário do IAM) e escolha Adicionar. Os tipos de entidades principais e formatos de ID e ARN disponíveis são os seguintes:
  - Conta da AWS— Para adicionar um Conta da AWS, insira o ID da conta de 12 dígitos. Por exemplo:

    ```
    123456789012
    ```

  - Organização — Para adicionar todos os Contas da AWS da sua organização, insira o ID da organização. Por exemplo:

    ```
    o-abcd1234
    ```

  - Unidade organizacional (OU): para adicionar uma OU, insira a ID da OU. Por exemplo:

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

  - Perfil do IAM: para adicionar um perfil do IAM, insira o ARN do perfil. Use a seguinte sintaxe:

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

Por exemplo:

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

> **Note**
>
> Para obter o ARN exclusivo para uma função do IAM, veja a lista de funções no console do IAM, use o AWS CLI comando get-role ou a ação da API. GetRole

- Usuário do IAM: para adicionar um usuário do IAM, insira o ARN do usuário. Use a seguinte sintaxe:

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

  Por exemplo:

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

  > **Note**
  >
  > Para obter o ARN exclusivo para um usuário do IAM, visualize a lista de usuários no console do IAM, use o get-user AWS CLI comando ou a ação da GetUserAPI.

- Entidade principal de serviço: para adicionar uma entidade principal de serviço, escolha Entidade principal de serviço na caixa Selecionar do tipo de entidade principal. Insira o nome da entidade principal do serviço da AWS . Use a seguinte sintaxe:
  - *service-id*.amazonaws.com

    Por exemplo:

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

c. Em Entidades principais selecionadas, verifique se as entidades principais que você especificou aparecem na lista.

9. Escolha Próximo.

10. Na Etapa 4: revisar e criar, revise os detalhes da configuração do seu compartilhamento de recursos. Para alterar a configuração de qualquer etapa, escolha o link que corresponde à etapa à qual você deseja voltar e faça as alterações necessárias.
11. Depois de concluir a revisão do compartilhamento de recursos, escolha Criar compartilhamento de recursos.

    Pode levar alguns minutos para que as associações de entidades principais entre recurso e principal sejam concluídas. Permita que esse processo seja concluído antes de tentar usar o compartilhamento de recursos.
12. É possível adicionar e remover recursos e entidades principais ou aplicar tags personalizadas ao recurso a qualquer momento. Você pode alterar a permissão gerenciada para tipos de recursos incluídos em seu compartilhamento de recursos, para aqueles tipos que oferecem suporte a mais do que a permissão gerenciada padrão. É possível excluir o recurso quando você não quiser mais compartilhar os recursos. Para obter mais informações, consulte Compartilhar seus recursos da AWS.

AWS CLI

Criar o compartilhamento de um recurso

Use o comando create-resource-share. O comando a seguir cria um compartilhamento de recursos que é compartilhado com todos Contas da AWS na organização. O compartilhamento contém uma configuração de AWS License Manager licença e concede as permissões gerenciadas padrão para esse tipo de recurso.

> **Note**
>
> Se quiser usar uma permissão gerenciada pelo cliente com um tipo de recurso nesse compartilhamento de recursos, você pode usar uma permissão gerenciada pelo cliente existente ou criar uma nova permissão gerenciada pelo cliente. Anote o ARN da permissão gerenciada pelo cliente e crie o compartilhamento de recursos. Para obter mais informações, consulte Criar uma permissão gerenciada pelo 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"
    }
}
```

Usando AWS recursos compartilhados

Para começar a usar recursos que foram compartilhados com sua conta usando AWS Resource Access Manager, conclua as tarefas a seguir.

Tarefas

- Responder ao convite de compartilhamento de recursos
- Uso dos recursos compartilhados com você

Responder ao convite de compartilhamento de recursos

Se você receber um convite para participar de um compartilhamento de recurso, deverá aceitá-lo para obter acesso aos recursos compartilhados.

Esse procedimento pode ocorrer nos seguintes cenários:

- Se você faz parte de uma organização AWS Organizations e o compartilhamento em sua organização está ativado, os diretores da organização obtêm acesso automático aos recursos compartilhados sem convites.
- Se você compartilhar com o Conta da AWS proprietário do recurso, os diretores dessa conta terão acesso automático aos recursos compartilhados sem convites.

Console

Para responder a um convite

1. Abra a página Compartilhado comigo: compartilhamentos de recursos no console do AWS RAM .

   > **Note**
   >
   > Um compartilhamento de recursos é visível somente no Região da AWS local em que foi criado. Se um compartilhamento de recursos esperado não aparecer no console, talvez seja necessário alternar para outro Região da AWS usando o controle suspenso no canto superior direito.

2. Revise a lista de compartilhamentos de recursos aos quais você recebeu acesso.

   A coluna Status indica seu status atual de participação no compartilhamento de recursos. O status `Pending` indica que você foi adicionado a um compartilhamento de recursos, mas ainda não aceitou ou rejeitou o convite.

3. Para responder ao convite de compartilhamento de recursos, selecione o ID do compartilhamento de recursos e escolha Aceitar compartilhamento de recursos para aceitar o convite ou Rejeitar compartilhamento de recursos para recusá-lo. Se você rejeitar o convite, não terá acesso aos recursos. Se você aceitar o convite, terá acesso aos recursos.

AWS CLI

Para começar, obtenha uma lista dos convites de compartilhamento de recursos que estão disponíveis para você. O comando de exemplo a seguir foi executado no `us-west-2` região e mostra que um compartilhamento de recursos está disponível no 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"
        }
    ]
}
```

Você pode usar o nome do recurso da Amazon (ARN) do convite do comando anterior como um parâmetro no próximo comando para aceitar esse convite.

```
$ 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"
    }
}
```

A saída mostra que o `status` foi alterado para `ACCEPTED`. Os recursos incluídos nesse compartilhamento de recursos agora estão disponíveis para as entidades principais na conta de aceitação.

Uso dos recursos compartilhados com você

Após aceitar o convite para fazer parte de um recurso compartilhado, você será capaz de executar ações específicas nos recursos compartilhados. Essas ações variam de acordo com o tipo de recurso. Para obter mais informações, consulte Recursos compartilháveis AWS. Os recursos estão disponíveis diretamente no console de serviço e nas API/CLI operações de cada recurso. Se o recurso for regional, você deverá usar o correto no console de serviço ou Região da AWS no comando API/CLI. Se o recurso for global, você deverá usar a região de origem designada, Leste

dos EUA (Norte da Virgínia). `us-east-1` Para visualizar o recurso em AWS RAM, você deve abrir o AWS RAM console no Região da AWS qual o compartilhamento de recursos foi criado.

Trabalhar com recursos compartilhados da AWS

Você pode usar o AWS Resource Access Manager (AWS RAM) para compartilhar recursos da AWS de sua propriedade e acessar recursos da AWS que são compartilhados com você.

Sumário

Compartilhamento de recursos regionais em comparação com recursos globais

Este tópico discute as diferenças em como AWS Resource Access Manager (AWS RAM) trabalha com recursos regionais e globais.

Os recursos são regionais ou globais. Você pode usar o quarto campo no Nome do recurso da Amazon (ARN) para identificar se um recurso é regional ou global. Os recursos regionais mostram Região da AWS o. Se estiver em branco, o recurso é global.

Quais são as diferenças entre recursos regionais e globais?

Recursos regionais

A maioria dos recursos com os quais você pode compartilhar AWS RAM é regional. Você os cria em uma Região da AWS especificada, e eles existem nessa região. Para ver ou interagir com esses recursos, você deve direcionar suas operações para essa região. Por exemplo, para criar uma instância do Amazon Elastic Compute Cloud (Amazon EC2) com Console de gerenciamento da AWS o, você escolhe aquela na qual deseja criar Região da AWS a instância. Se você usar o AWS Command Line Interface (AWS CLI) para criar a instância, inclua o `--region` parâmetro. AWS SDKs Cada um tem seu próprio mecanismo equivalente para especificar a região que a operação usa.

Há vários motivos para usar recursos regionais. Um dos motivos é garantir que os recursos e os endpoints de serviço que você usa para acessá-los estejam o mais próximos possível do cliente. Isso melhora a performance ao minimizar a latência. Outro motivo é fornecer um limite de isolamento. Isso permite criar cópias independentes de recursos em várias regiões para distribuir a carga e melhorar a escalabilidade. Ao mesmo tempo, ele isola os recursos uns dos outros para melhorar a disponibilidade.

Se você especificar um diferente Região da AWS no console ou em um AWS CLI comando, não poderá mais ver ou interagir com os recursos que podia ver na região anterior.

Quando você analisa o nome do recurso da Amazon (ARN) de um recurso regional, a região que contém o recurso é especificada como o quarto campo no ARN. Por exemplo, uma instância do Amazon EC2 é um recurso regional. Esses recursos são semelhantes ao exemplo a seguir para uma VPC que existe na `us-east-1` região. ARNs

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

Recursos globais

Alguns AWS serviços oferecem suporte a recursos que você pode acessar globalmente, o que significa que você pode usar o recurso de qualquer lugar. Você não especifica um Região da AWS no console de um serviço global. Para acessar um recurso global, você não especifica um `--region` parâmetro ao usar as operações do serviço AWS CLI e do AWS SDK.

Os recursos globais oferecem suporte a casos em que é fundamental que somente uma instância de um recurso específico possa existir por vez. Nesses cenários, a replicação ou sincronização entre cópias em diferentes regiões não é adequada. Ter que acessar um único endpoint global, com o possível aumento na latência, é considerado aceitável para garantir que quaisquer alterações sejam instantaneamente visíveis para os consumidores do recurso. Por exemplo, quando você cria uma rede principal de AWS Cloud WAN como um recurso global, ela é consistente para todos os usuários. Ele aparece como um cluster global único e contínuo em todas as regiões.

O nome do recurso da Amazon (ARN) de um recurso global não inclui uma região. O quarto campo desse ARN está vazio, como o exemplo de ARN a seguir para uma rede principal de WAN em nuvem.

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

Compartilhamentos de recursos e suas regiões

AWS RAM é um serviço regional e um compartilhamento de recursos é regional. Portanto, um compartilhamento de recursos pode conter recursos do Região da AWS mesmo compartilhamento de recursos e quaisquer recursos globais compatíveis. A região em que você criar o compartilhamento de recursos é a região de origem do compartilhamento de recursos.

> **Important**
>
> Atualmente, você pode criar compartilhamentos de recursos com recursos globais somente na região designada Leste dos EUA (Norte da Virgínia), `us-east-1`. Embora você possa criar o compartilhamento de recursos somente nessa única região de origem, qualquer recurso global compartilhado aparece como um recurso global padrão quando visualizado no console do serviço ou nas operações de CLI e SDK. A restrição à região de origem se aplica somente ao compartilhamento de recursos, não aos recursos que ele contém.

Para compartilhar um recurso regional que você criou na `us-west-2` região, você deve configurar o AWS RAM console para usar `us-west-2` e criar o compartilhamento de recursos lá. Você não pode criar um compartilhamento de recursos que inclua recursos regionais de diferentes Regiões da AWS. Isso significa que, para compartilhar recursos de `us-west-2` e `eu-north-1`, você deve criar

dois compartilhamentos de recursos diferentes. Você não pode combinar recursos de duas regiões diferentes em um único compartilhamento de recursos.

Para compartilhar um recurso global no AWS RAM console, você deve configurar o AWS RAM console para usar a região de origem designada, Leste dos EUA (Norte da Virgínia)`us-east-1`. Em seguida, crie o compartilhamento de recursos na região de origem designada. Você pode combinar recursos globais em um compartilhamento de recursos somente com recursos da Região `us-east-1`.

Embora o recurso global possa ser visualizado em um compartilhamento de AWS RAM recursos somente na região de origem designada, ele ainda é um recurso global depois que você o compartilha. Você pode acessá-lo no compartilhado Contas da AWS de qualquer região da qual possa acessá-lo no original Conta da AWS.

Considerações

- Para criar um compartilhamento de recursos no AWS RAM console, você deve usar a Região que contém os recursos que você deseja compartilhar. Se você quiser incluir um recurso global, deverá usar a região de origem designada para criar o compartilhamento. Por exemplo, para compartilhar uma rede principal do AWS Cloud WAN, você deve criar o compartilhamento de recursos na `us-east-1` região.
- Para visualizar ou modificar um compartilhamento de recursos no AWS RAM console, você deve usar a Região que contém o compartilhamento de recursos. Da mesma forma, as operações do SDK AWS RAM AWS CLI e do SDK permitem que você interaja somente com compartilhamentos de recursos que estão na região especificada em sua operação. Para visualizar ou modificar compartilhamentos de recursos que contêm recursos globais, use a região de origem designada, Leste dos EUA (Norte da Virgínia), `us-east-1`.
- Para visualizar um recurso regional no AWS RAM console e incluí-lo em um compartilhamento de recursos, você deve usar a região que contém o recurso regional.
- Para visualizar um recurso global no AWS RAM console e incluí-lo em um compartilhamento de recursos, você deve usar a região de origem designada, Leste dos EUA (Norte da Virgínia),`us-east-1`.
- Você pode criar um compartilhamento de recursos com recursos regionais e globais somente na região de origem designada, Leste dos EUA (Norte da Virgínia), `us-east-1`.

Compartilhar seus recursos da AWS

Você pode usar o AWS Resource Access Manager (AWS RAM) para compartilhar os recursos que você especifica com as entidades principais que você especifica. Esta seção descreve como você pode criar novos compartilhamentos de recursos, modificar compartilhamentos de recursos existentes e excluir compartilhamentos de recursos que não são mais necessários.

Tópicos

Visualizando compartilhamentos de recursos que você criou no AWS RAM

É possível visualizar uma lista de todos os recursos compartilhados que você criou. É possível ver quais recursos você está compartilhando e as entidades com quem eles estão sendo compartilhados.

Console

Para ver seus compartilhamentos de recursos

1. Abra a página Compartilhado por mim: compartilhamentos de recursos no console do AWS RAM.
2. Como os compartilhamentos de recursos do AWS RAM existem em Regiões da AWS específicas, escolha a Região da AWS apropriada na lista suspensa no canto superior direito do console. Para ver os compartilhamentos de recursos que contêm recursos globais, defina a Região da AWS como Leste dos EUA (Norte da Virgínia), (`us-east-1`). Para obter mais informações sobre o compartilhamento de recursos globais, consulte Compartilhamento de recursos regionais em comparação com recursos globais.
3. Se alguma das permissões gerenciadas usadas pelos compartilhamentos de recursos nos resultados tiver uma nova versão da permissão gerenciada designada como padrão, a página exibirá um banner para alertar você. Você pode optar por atualizar todas as versões

de permissões gerenciadas de uma só vez escolhendo Revisar e atualizar tudo na parte superior da página.

Como alternativa, para compartilhamentos de recursos individuais com uma ou mais novas versões de permissões gerenciadas, a coluna Status exibe Atualização disponível. A escolha desse link inicia o processo de revisão das versões atualizadas de permissões gerenciadas e permite que você as atribua como versões para os tipos de recursos relevantes nesse compartilhamento de recursos.

4. (Opcional) Aplique um filtro para encontrar recursos compartilhados específicos. É possível aplicar vários filtros para restringir a pesquisa. Você pode digitar uma palavra-chave, como parte do nome de um compartilhamento de recursos, para listar somente os compartilhamentos de recursos que incluem esse texto no nome. Escolha a caixa de texto para ver uma lista suspensa dos campos de atributos sugeridos. Depois de escolher um, você pode escolher na lista de valores disponíveis para esse campo. Você pode adicionar outros atributos ou palavras-chave até encontrar o recurso desejado.
5. Escolha o nome do compartilhamento de recursos a ser revisado. O console exibe as seguintes informações sobre o compartilhamento de recursos:

   - Resumo: indica o nome do compartilhamento de recursos, ID, proprietário, nome do recurso da Amazon (ARN), data de criação, se ele permite o compartilhamento com contas externas e seu status atual.
   - Permissões gerenciadas: indica as permissões gerenciadas que estão anexadas a esse compartilhamento de recursos. É possível que haja no máximo uma permissão gerenciada por tipo de recurso incluído no compartilhamento de recursos. Cada permissão gerenciada exibe a versão dessa permissão gerenciada associada ao compartilhamento de recursos. Se não for a versão padrão, o console exibirá um link Atualizar para a versão padrão. Se você escolher esse link, terá a oportunidade de atualizar o compartilhamento de recursos para usar a versão padrão.
   - Recursos compartilhados: indica os recursos individuais incluídos no compartilhamento de recursos. Escolha o ID de um recurso para abrir uma nova guia do navegador e visualizar o recurso no console do serviço nativo.
   - Entidades compartilhadas: indica as entidades com as quais os recursos são compartilhados.
   - Tags: indica os pares de chave-valor da tag que estão anexados ao próprio compartilhamento de recursos; essas não são as tags anexadas aos recursos individuais incluídos no compartilhamento de recursos.

AWS CLI

Para ver seus compartilhamentos de recursos

Você pode usar o comando get-resource-shares com o parâmetro `--resource-owner` definido como `SELF` para exibir detalhes dos compartilhamentos de recursos criados na sua Conta da AWS.

O exemplo a seguir mostra os compartilhamentos de recursos que são compartilhados na Região da AWS (`us-east-1`) atual para a Conta da AWS que faz a chamada. Para criar os compartilhamentos de recursos em uma região diferente, use o parâmetro `--region` *<region-code>*. Para incluir compartilhamentos de recursos que contenham recursos globais, você deve especificar a Região Leste dos EUA (Norte da Virgínia), `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"
        }
    ]
}
```

Criar um compartilhamento de recursos no AWS RAM

Para compartilhar recursos de sua propriedade, crie um compartilhamento de recursos. Aqui está uma visão geral do processo:

1. Adicione os recursos que você deseja compartilhar.
2. Para cada tipo de recurso que você incluir no compartilhamento, especifique a permissão gerenciada a ser usada para esse tipo de recurso.
   - Você pode escolher entre uma das permissões gerenciadas da AWS disponíveis, uma permissão gerenciada pelo cliente existente ou criar uma nova permissão gerenciada pelo cliente.
   - As permissões gerenciadas da AWS são criadas pela AWS para abranger casos de uso padrão.
   - As permissões gerenciadas pelo cliente permitem que você personalize suas próprias permissões gerenciadas para atender às suas necessidades comerciais e de segurança.

   > **Note**
   >
   > Se a permissão gerenciada selecionada tiver várias versões, o AWS RAM anexará automaticamente a versão padrão. Você pode anexar somente a versão designada como padrão.

3. Especifique as entidades principais que você deseja que tenham acesso aos recursos.

Considerações

- Se você precisar excluir posteriormente um recurso da AWS incluído em um compartilhamento, recomendamos que primeiro remova o recurso de qualquer compartilhamento de recursos que o inclua ou exclua o compartilhamento de recursos.
- Os tipos de recursos que você pode incluir em um compartilhamento de recursos estão listados em Recursos compartilháveis AWS.
- Você só poderá compartilhar um recurso se for o proprietário dele. Não é possível compartilhar um recurso compartilhado com você.
- O AWS RAM é um serviço regional. Quando você compartilha um recurso com entidades principais em outras Contas da AWS, essas entidades principais devem acessar cada recurso da mesma Região da AWS em que foi criado. Para recursos globais compatíveis, você pode acessar esses recursos de qualquer Região da AWS que seja compatível com o console de serviço e

as ferramentas desse recurso. Você pode visualizar esses compartilhamentos de recursos e seus recursos globais no console do AWS RAM e nas ferramentas somente na região de origem designada, Leste dos EUA (Norte da Virgínia), `us-east-1`. Para obter mais informações sobre o AWS RAM e recursos globais, consulte Compartilhamento de recursos regionais em comparação com recursos globais.

- Se a conta da qual você estiver compartilhando fizer parte de uma organização no AWS Organizations e o compartilhamento estiver habilitado na organização, todas as entidades principais da organização com a qual você compartilhar os recursos receberão acesso automaticamente aos compartilhamentos de recursos sem o uso de convites. Uma entidade principal em uma conta com a qual você compartilha fora do contexto de uma organização recebe um convite para ingressar no compartilhamento de recursos e acesso aos recursos compartilhados somente após aceitar o convite.
- Se você compartilhar com uma entidade principal de serviço, não poderá associar nenhuma outra entidade principal ao compartilhamento de recursos.
- Se o compartilhamento for entre contas ou entidades principais que fazem parte de uma organização, qualquer alteração na associação à organização afetará dinamicamente o acesso ao compartilhamento de recursos.
  - Se você adicionar uma Conta da AWS à organização ou a uma OU que tenha acesso a um compartilhamento de recursos, essa nova conta de membro automaticamente terá acesso ao compartilhamento de recursos. O administrador da conta com a qual você compartilhou pode então conceder às entidades principais individuais dessa conta acesso aos recursos desse compartilhamento.
  - Se você remover uma conta da organização ou de uma OU que tenha acesso a um compartilhamento de recursos, todas as entidades principais dessa conta perderão automaticamente o acesso aos recursos que foram acessados por meio desse compartilhamento de recursos.
  - Se você compartilhou diretamente com uma conta membro ou com perfis do IAM ou usuários na conta membro e depois remover essa conta da organização, todas as entidades principais dessa conta perderão o acesso aos recursos que foram acessados por meio desse compartilhamento de recursos.

> **Important**
>
> Quando você compartilha com uma organização ou uma OU, e esse escopo inclui a conta que possui o compartilhamento de recursos, todas as entidades principais na conta de compartilhamento obtêm acesso automático aos recursos no compartilhamento. O acesso

concedido é definido pelas permissões gerenciadas associadas ao compartilhamento. Isso ocorre porque a política baseada em recursos que o AWS RAM anexa a cada recurso no compartilhamento usa `"Principal": "*"`. Para obter mais informações, consulte Implicações do uso de "Principal": "*" em uma política baseada em recursos.
As entidades principais das outras contas consumidoras não têm acesso imediato aos recursos do compartilhamento. Os administradores das outras contas devem primeiro anexar políticas de permissão baseadas em identidade às entidades principais apropriadas. Essas políticas devem conceder acesso `Allow` aos ARNs de recursos individuais no compartilhamento de recursos. As permissões nessas políticas não podem exceder as especificadas na permissão gerenciada associada ao compartilhamento de recursos.

- Você pode adicionar somente a organização da qual sua conta é membro e OUs dessa organização aos seus compartilhamentos de recursos. Você não pode adicionar OUs ou organizações de fora da sua própria organização a um compartilhamento de recursos como entidades principais. No entanto, você pode adicionar Contas da AWS individuais ou, no caso de serviços compatíveis, usuários e perfis do IAM de fora da sua organização como entidades de um compartilhamento de recursos.

  Note

  Nem todos os tipos de recursos podem ser compartilhados com perfis e usuários do IAM. Para obter informações sobre os recursos que você pode compartilhar com essas entidades principais, consulte Recursos compartilháveis AWS.

- Para os seguintes tipos de recursos, você tem sete dias para aceitar o convite para participar do compartilhamento para os seguintes tipos de recursos. Se você não aceitar o convite antes que ele expire, ele será automaticamente recusado.

  Important

  Para tipos de recursos compartilhados que não estão na lista a seguir, você tem 12 horas para aceitar o convite para participar do compartilhamento de recursos. Depois de 12 horas, o convite expira e o usuário final da entidade principal no compartilhamento de recursos é desassociado. O convite não pode mais ser aceito pelos usuários finais.

- Amazon Aurora: clusters de banco de dados
- Amazon EC2: reservas de capacidade e hosts dedicados
- AWS License Manager: configurações de licença
- AWS Outposts: tabelas de rotas de gateway local, postos avançados e sites
- Amazon Route 53: regras de encaminhamento
- Amazon VPC: endereços IPv4 de propriedade do cliente, listas de prefixos, sub-redes, alvos de espelhamento de tráfego, gateways de trânsito, domínios multicast de gateway de trânsito

Console

Criar o compartilhamento de um recurso

1. Abra o console de AWS RAM.
2. Como os compartilhamentos de recursos do AWS RAM existem em Regiões da AWS específicas, escolha a Região da AWS apropriada na lista suspensa no canto superior direito do console. Para ver os compartilhamentos de recursos que contêm recursos globais, defina a Região da AWS como Leste dos EUA (Norte da Virgínia), (`us-east-1`). Para obter mais informações sobre o compartilhamento de recursos globais, consulte Compartilhamento de recursos regionais em comparação com recursos globais. Se você quiser incluir recursos globais no compartilhamento de recursos, deverá escolher a região de origem designada, Leste dos EUA (Norte da Virgínia), `us-east-1`.
3. Se você for novo no AWS RAM, selecione Criar um compartilhamento de recursos na página inicial. Caso contrário, escolha Criar compartilhamento de recursos na página Compartilhado por mim: compartilhamentos de recursos.
4. Na Etapa 1: Especificar detalhes do compartilhamento de recursos, faça o seguinte:

   a. Em Nome, insira um nome descritivo para o compartilhamento de recursos.

   b. Em Recursos, escolha recursos para adicionar ao compartilhamento de recursos da seguinte forma:

      - Em Selecionar tipo de recurso, selecione o tipo de recurso para compartilhar. Isso filtra a lista de recursos compartilháveis para os recursos do tipo selecionado.

- Na lista de recursos resultante, marque as caixas de seleção ao lado dos recursos individuais que você deseja compartilhar. Os recursos selecionados são movidos para Recursos selecionados.

  Se você estiver compartilhando recursos associados a uma zona de disponibilidade específica, usar o ID da zona de disponibilidade (ID de AZ) ajudará a determinar a localização relativa desses recursos nas contas. Para obter mais informações, consulte IDs de zona de disponibilidade para seus recursos da AWS.

c. (Opcional) Para anexar tags ao compartilhamento de recursos, em Tags, insira uma chave e um valor de tag. Adicione outras escolhendo Adicionar nova tag. Repita esta etapa conforme necessário. Essas tags se aplicam somente ao compartilhamento de recursos em si, não aos recursos no compartilhamento de recursos.

5. Escolha Próximo.

6. Na Etapa 2: Associar uma permissão gerenciada a cada tipo de recurso, você pode escolher associar uma permissão gerenciada criada pela AWS ao tipo de recurso, escolher uma permissão gerenciada pelo cliente existente ou criar sua própria permissão gerenciada pelo cliente para os tipos de recursos compatíveis. Para obter mais informações, consulte Tipos de permissões gerenciadas.

   Escolha Criar permissão gerenciada pelo cliente para criar uma permissão gerenciada pelo cliente que atenda aos requisitos do seu caso de uso de compartilhamento. Para obter mais informações, consulte Criar uma permissão gerenciada pelo cliente. Depois de concluir o processo, escolha

   e selecione sua nova permissão gerenciada pelo cliente na lista suspensa Permissões gerenciadas.

   > **Note**
   >
   > Se a permissão gerenciada selecionada tiver várias versões, o AWS RAM anexará automaticamente a versão padrão. Você pode anexar somente a versão designada como padrão.

   Para exibir as ações que a permissão gerenciada permite, expanda Exibir o modelo de política dessa permissão gerenciada.

7. Escolha Próximo.
8. Na Etapa 3: Conceder acesso às entidades principais, faça o seguinte:

   a. Por padrão, Permitir compartilhamento com qualquer pessoa está selecionado, o que significa que, para os tipos de recursos que o suportam, você pode compartilhar recursos com as Contas da AWS que estão fora da sua organização. Isso não afeta os tipos de recursos que podem ser compartilhados somente dentro de uma organização, como as sub-redes da Amazon VPC. Você também pode compartilhar alguns tipos de recursos compatíveis com perfis e usuários do IAM.

      Para restringir o compartilhamento de recursos somente a contas e entidades principais em sua organização, escolha Permitir compartilhamento somente dentro de sua organização.

   b. Para entidades principais, faça o seguinte:

      - Para adicionar a organização, uma unidade organizacional (OU) ou uma Conta da AWS que faça parte de uma organização, ative Exibir estrutura organizacional. Isso exibe uma visualização em árvore da sua organização. Em seguida, marque a caixa de seleção ao lado de cada entidade principal que você deseja adicionar.

        Important

        Quando você compartilha com uma organização ou uma OU, e esse escopo inclui a conta que possui o compartilhamento de recursos, todas as entidades principais na conta de compartilhamento obtêm acesso automático aos recursos no compartilhamento. O acesso concedido é definido pelas permissões gerenciadas associadas ao compartilhamento. Isso ocorre porque a política baseada em recursos que o AWS RAM anexa a cada recurso no compartilhamento usa `"Principal": "*"`. Para obter mais informações, consulte Implicações do uso de "Principal": "*" em uma política baseada em recursos.
        As entidades principais das outras contas consumidoras não têm acesso imediato aos recursos do compartilhamento. Os administradores das outras contas devem primeiro anexar políticas de permissão baseadas em identidade às entidades principais apropriadas. Essas políticas devem conceder acesso `Allow` aos ARNs de recursos individuais no compartilhamento de recursos.

As permissões nessas políticas não podem exceder as especificadas na permissão gerenciada associada ao compartilhamento de recursos.

- Se você selecionar a organização (o ID começa com `o-`), as entidades principais de todas as Contas da AWS na organização poderão acessar o compartilhamento de recursos.
- Se você selecionar uma OU (o ID começa com `ou-`), as entidades principais de todas as Contas da AWS nessa OU e suas OUs secundárias poderão acessar o compartilhamento de recursos.
- Se você selecionar uma Conta da AWS individual, somente as entidades principais dessa conta poderão acessar o compartilhamento de recursos.

> **Note**
>
> A opção Exibir estrutura organizacional aparecerá somente se o compartilhamento com o AWS Organizations estiver ativado e você estiver conectado à conta de gerenciamento da organização.
> Você não pode usar esse método para especificar uma Conta da AWS externa à sua organização ou um usuário ou perfil do IAM. Em vez disso, você deve desativar Exibir estrutura organizacional e usar a lista suspensa e a caixa de texto para inserir o ID ou o ARN.

- Para especificar uma entidade principal por ID ou ARN, incluindo entidades principais que estão fora da organização, selecione o tipo de entidade principal para cada entidade principal. Em seguida, insira o ID (para uma Conta da AWS, organização ou OU) ou o ARN (para um usuário ou perfil do IAM) e escolha Adicionar. Os tipos de entidades principais e formatos de ID e ARN disponíveis são os seguintes:
  - Conta da AWS: para adicionar uma Conta da AWS, insira o ID da conta de 12 dígitos. Por exemplo:

    ```
    123456789012
    ```

  - Organização: para adicionar todas as Contas da AWS da sua organização, insira o ID da organização. Por exemplo:

    ```
    o-abcd1234
    ```

- Unidade organizacional (OU): para adicionar uma OU, insira a ID da OU. Por exemplo:

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

- Perfil do IAM: para adicionar um perfil do IAM, insira o ARN do perfil. Use a seguinte sintaxe:

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

  Por exemplo:

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

  > **Note**
  >
  > Para obter o ARN exclusivo para um perfil do IAM, veja a lista de perfis no console do IAM use o comando get-role da AWS CLI ou a ação da API GetRole.

- Usuário do IAM: para adicionar um usuário do IAM, insira o ARN do usuário. Use a seguinte sintaxe:

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

  Por exemplo:

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

  > **Note**
  >
  > Para obter o ARN exclusivo para um usuário do IAM, veja a lista de usuários no console do IAM, use o comando get-user da AWS CLI ou a ação GetUser da API.

- Entidade principal de serviço: para adicionar uma entidade principal de serviço, escolha Entidade principal de serviço na caixa Selecionar do tipo de entidade principal. Insira o nome da entidade principal do serviço da AWS. Use a seguinte sintaxe:

- *service-id*.amazonaws.com

  Por exemplo:

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

c. Em Entidades principais selecionadas, verifique se as entidades principais que você especificou aparecem na lista.

9. Escolha Próximo.
10. Na Etapa 4: revisar e criar, revise os detalhes da configuração do seu compartilhamento de recursos. Para alterar a configuração de qualquer etapa, escolha o link que corresponde à etapa à qual você deseja voltar e faça as alterações necessárias.
11. Depois de concluir a revisão do compartilhamento de recursos, escolha Criar compartilhamento de recursos.

    Pode levar alguns minutos para que as associações de entidades principais entre recurso e principal sejam concluídas. Permita que esse processo seja concluído antes de tentar usar o compartilhamento de recursos.
12. É possível adicionar e remover recursos e entidades principais ou aplicar tags personalizadas ao recurso a qualquer momento. Você pode alterar a permissão gerenciada para tipos de recursos incluídos em seu compartilhamento de recursos, para aqueles tipos que oferecem suporte a mais do que a permissão gerenciada padrão. É possível excluir o recurso quando você não quiser mais compartilhar os recursos. Para obter mais informações, consulte Compartilhar seus recursos da AWS.

AWS CLI

Criar o compartilhamento de um recurso

Use o comando create-resource-share. O comando a seguir cria um compartilhamento de recursos que é compartilhado com todas as Contas da AWS na organização. O compartilhamento contém uma configuração de licença da AWS License Manager e concede as permissões gerenciadas padrão para esse tipo de recurso.

> **Note**
>
> Se quiser usar uma permissão gerenciada pelo cliente com um tipo de recurso nesse compartilhamento de recursos, você pode usar uma permissão gerenciada pelo cliente

existente ou criar uma nova permissão gerenciada pelo cliente. Anote o ARN da permissão gerenciada pelo cliente e crie o compartilhamento de recursos. Para obter mais informações, consulte Criar uma permissão gerenciada pelo 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"
    }
}
```

Atualizar o compartilhamento de um recurso no AWS RAM

Você pode atualizar um compartilhamento de recursos do AWS RAM a qualquer momento das seguintes formas:

- É possível adicionar recursos de uma entidade principal, ou tags para um compartilhamento de recursos que você criou.
- Para tipos de recursos que oferecem suporte a mais do que a permissão gerenciada da AWS padrão, você pode escolher qual permissão gerenciada se aplica aos recursos de cada tipo.
- Quando uma permissão gerenciada anexada ao compartilhamento de recursos tem uma nova versão padrão, você pode atualizar a permissão gerenciada para usar a nova versão.

- É possível revogar o acesso a recursos compartilhados removendo entidades principais ou recursos de um recurso compartilhado. Se você revogar o acesso, as entidades principais não terão mais acesso aos recursos compartilhados.

> **Note**
>
> As entidades principais com quem você compartilha recursos poderão sair do compartilhamento de recursos se o compartilhamento estiver vazio ou contiver apenas tipos de recursos que dão suporte à saída de um compartilhamento de recursos. Se o compartilhamento de recursos contiver tipos de recursos que não suportam a saída, uma mensagem será exibida informando às entidades principais que devem entrar em contato com o proprietário do compartilhamento. Nesse caso, você, como proprietário do compartilhamento de recursos, deve remover as entidades principais do seu compartilhamento de recursos. Para obter uma lista de tipos de recursos que não oferecem suporte a essa ação, consulte Pré-requisitos para deixar o compartilhamento de um recurso.

Console

Atualizar o compartilhamento de um recurso

1. Navegue até a página Compartilhado por mim: compartilhamentos de recursos no console do AWS RAM.
2. Como os compartilhamentos de recursos do AWS RAM existem em Regiões da AWS específicas, escolha a Região da AWS apropriada na lista suspensa no canto superior direito do console. Para ver os compartilhamentos de recursos que contêm recursos globais, defina a Região da AWS como Leste dos EUA (Norte da Virgínia), (`us-east-1`). Para obter mais informações sobre o compartilhamento de recursos globais, consulte Compartilhamento de recursos regionais em comparação com recursos globais.
3. Selecione o compartilhamento de recursos e escolha Modificar.
4. Na Etapa 1: Especifique os detalhes do compartilhamento de recursos, revise os detalhes do compartilhamento de recursos e, se necessário, atualize qualquer um dos seguintes:

    a. (Opcional) Para alterar o nome do compartilhamento de recurso, edite Nome.

    b. (Opcional) Para adicionar um recurso ao compartilhamento de recursos, em Recursos, escolha o tipo de recurso e marque a caixa de seleção ao lado do recurso para adicioná-

lo ao compartilhamento de recursos. Os recursos globais aparecem somente se você definir a região como Leste dos EUA (Norte da Virgínia), (`us-east-1`) no Console de gerenciamento da AWS.

c. (Opcional) Para remover um recurso do compartilhamento de recursos, localize o recurso em Recursos selecionados e escolha o X ao lado da ID do recurso.

d. (Opcional) Para adicionar uma tag ao compartilhamento de recursos, em Tags, insira a chave e o valor da tag nas caixas de texto vazias. Para adicionar mais de um par de chave e valor de tag, escolha Adicionar nova tag. É possível adicionar até 50 tags.

e. Para remover uma tag do compartilhamento de recursos, em Tags, localize a tag e escolha Remover ao lado dela.

5. Escolha Próximo.

6. (Opcional) Na Etapa 2: Associar uma permissão gerenciada a cada tipo de recurso, você pode escolher associar uma permissão gerenciada criada pela AWS ao tipo de recurso, escolher uma permissão gerenciada pelo cliente existente ou criar sua própria permissão gerenciada pelo cliente. Para obter mais informações, consulte Tipos de permissões gerenciadas.

   Você também pode escolher Criar permissão gerenciada pelo cliente para criar uma permissão gerenciada pelo cliente que atenda aos requisitos do seu caso de uso de compartilhamento. Para obter mais informações, consulte Criar uma permissão gerenciada pelo cliente. Depois de concluir o processo, escolha

   e selecione sua nova permissão gerenciada pelo cliente na lista suspensa Permissão gerenciada.

   Para exibir as ações que a permissão gerenciada permite, expanda Exibir o modelo de política dessa permissão gerenciada.

7. Se a versão da permissão gerenciada atualmente atribuída ao compartilhamento de recursos não for a versão padrão atual, você poderá atualizar para a versão padrão escolhendo Atualizar para a versão padrão.

> **Note**
>
> Até salvar suas alterações no compartilhamento de recursos após a etapa final, você pode cancelar a atualização da versão escolhendo Reverter para a versão

anterior. No entanto, para permissões gerenciadas da AWS, depois de salvar o compartilhamento de recursos, a alteração é definitiva e você não pode mais retornar à versão anterior.

8. Escolha Próximo.
9. Na Etapa 3: Escolher as entidades principais que têm permissão para acessar, revise os principais selecionados e, se necessário, atualize qualquer um dos seguintes:

   a. (Opcional) Para alterar se o compartilhamento está habilitado com entidades principais de dentro ou de fora da organização, escolha uma das seguintes opções:

      - Para compartilhar recursos com Contas da AWS ou usuários ou perfis individuais do IAM que estão fora da sua organização, escolha Permitir compartilhamento com entidades principais externas.
      - Para restringir o compartilhamento de recursos somente às entidades principais da sua organização no AWS Organizations, escolha Permitir compartilhamento somente com as entidades principais da sua organização.

   b. Para entidades principais, faça o seguinte:

      - (Opcional) Para adicionar uma organização, unidade organizacional (OU) ou Conta da AWS membro dentro da sua organização, ative Exibir estrutura organizacional para exibir uma visualização em árvore da sua organização. Em seguida, marque a caixa de seleção ao lado de cada entidade principal que você deseja adicionar.

        Important

        Quando você compartilha com uma organização ou uma OU, e esse escopo inclui a conta que possui o compartilhamento de recursos, todas as entidades principais na conta de compartilhamento obtêm acesso automático aos recursos no compartilhamento. O acesso concedido é definido pelas permissões gerenciadas associadas ao compartilhamento. Isso ocorre porque a política baseada em recursos que o AWS RAM anexa a cada recurso no compartilhamento usa `"Principal": "*"`. Para obter mais informações, consulte Implicações do uso de "Principal": "*" em uma política baseada em recursos.

        As entidades principais das outras contas consumidoras não têm acesso imediato aos recursos do compartilhamento. Os administradores das outras

contas devem primeiro anexar políticas de permissão baseadas em identidade às entidades principais apropriadas. Essas políticas devem conceder acesso `Allow` aos ARNs de recursos individuais no compartilhamento de recursos. As permissões nessas políticas não podem exceder as especificadas na permissão gerenciada associada ao compartilhamento de recursos.

> **Note**
>
> A opção Exibir estrutura organizacional aparece somente se o compartilhamento com o AWS Organizations estiver ativado e você estiver conectado como entidade principal na conta de gerenciamento da organização.
> Você não pode usar esse método para especificar uma Conta da AWS externa à sua organização ou um usuário ou perfil do IAM. Em vez disso, você deve adicionar essas entidades principais inserindo seus identificadores, que são mostrados na caixa de texto abaixo da opção Exibir estrutura organizacional. Veja o próximo bullet point.

- (Opcional) Para adicionar um principal por meio de seu identificador, escolha o tipo entidade principal na lista suspensa e, em seguida, insira o ID ou o ARN da entidade principal. Por fim, escolha Adicionar.

  Se você selecionar uma Conta da AWS individual, somente essa conta poderá acessar o compartilhamento de recursos. Escolha uma das seguintes opções.

  - Outra Conta da AWS (que não seja o proprietária do recurso): disponibiliza o recurso para a outra conta. O administrador dessa conta deve concluir o processo concedendo acesso ao recurso compartilhado usando políticas de permissão baseadas em identidade para usuários e perfis individuais. Essas permissões não podem exceder as definidas nas permissões gerenciadas anexadas ao compartilhamento de recursos.
  - Esta Conta da AWS (proprietária do recurso): todas as usuários e perfis na conta proprietária do recurso recebem automaticamente o acesso definido pelas permissões gerenciadas anexadas ao compartilhamento de recursos.
- A adição aparece imediatamente na lista de entidades principais selecionadas.

Em seguida, você pode adicionar outras contas, OUs ou sua organização repetindo essa etapa.

- (Opcional) Para remover uma entidade principal, localize-a em Entidades principais selecionadas, marque sua caixa de seleção e escolha Desmarcar.

10. Escolha Avançar.
11. Na Etapa 4: revisar e atualizar, revise os detalhes da configuração do seu compartilhamento de recursos.
12. Para alterar a configuração de qualquer etapa, escolha o link que corresponde à etapa para a qual você deseja voltar e, em seguida, faça as alterações necessárias.

    Se alguma permissão gerenciada ainda estiver usando versões diferentes da padrão, você terá outra oportunidade de resolver isso escolhendo Atualizar para a versão padrão.
13. Escolha Atualizar compartilhamento de recursos quando terminar de fazer alterações.

AWS CLI

Atualizar o compartilhamento de um recurso

Você pode usar os seguintes comandos da AWS CLI para modificar um compartilhamento de recursos:

- Para renomear um compartilhamento de recursos ou alterar se as entidades principais externas são permitidas, use o comando update-resource-share. O exemplo a seguir renomeia o compartilhamento de recursos especificado e o define para permitir somente entidades principais de sua organização. Você deve usar o endpoint de serviço para a Região da AWS que contém o compartilhamento de recursos.

```
$ 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 adicionar um recurso a um compartilhamento de recursos, use o comando associate-resource-share. O exemplo a seguir adiciona uma sub-rede ao compartilhamento de recursos 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 adicionar ou substituir uma permissão gerenciada para um tipo de recurso em um compartilhamento de recursos, use os comandos list-permissions e associate-resource-share-permission. Você pode atribuir somente uma permissão gerenciada para cada tipo de recurso em um compartilhamento de recursos. Se você tentar adicionar uma permissão gerenciada a um tipo de recurso que já tem uma permissão gerenciada, deverá incluir a opção `--replace`, ou o comando falhará com um erro.

  O comando de exemplo a seguir lista os ARNs para as permissões gerenciadas disponíveis para uma sub-rede do Amazon Elastic Compute Cloud (Amazon EC2) e, em seguida, usa um desses ARNs para substituir a permissão gerenciada da AWS atualmente atribuída para esse tipo de recurso no compartilhamento de recursos 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 remover um recurso de um compartilhamento de recursos, use o comando disassociate-resource-share. O exemplo a seguir remove a sub-rede do Amazon EC2 com o ARN especificado do compartilhamento de recursos 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 as tags anexadas a um compartilhamento de recursos, use os comandos tag-resource e untag-resource. O exemplo a seguir adiciona a tag `project=lima` ao compartilhamento de recursos 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
```

O exemplo a seguir remove a tag com uma chave de `project` do compartilhamento de recursos 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
```

Esse comando não gera nenhuma saída quando é bem-sucedido.

Visualizando seus recursos compartilhados no AWS RAM

Você pode ver a lista de recursos individuais compartilhados por você em todos os compartilhamentos de recursos. Isso permite determinar quais recursos você está compartilhando no momento, o número de recursos compartilhados nos quais estão incluídos e o número de entidades que têm acesso a eles.

Console

Para visualizar os recursos que você está compartilhando atualmente

1. Abra a página Compartilhado por mim: recursos compartilhados no console do AWS RAM .
2. Como existem compartilhamentos de AWS RAM recursos específicos Regiões da AWS, escolha o apropriado na Região da AWS lista suspensa no canto superior direito do console.

Para ver os compartilhamentos de recursos que contêm recursos globais, você deve Região da AWS definir o como Leste dos EUA (Norte da Virgínia), (`us-east-1`). Para obter mais informações sobre o compartilhamento de recursos globais, consulte Compartilhamento de recursos regionais em comparação com recursos globais.

3. Para cada recurso compartilhado, as seguintes informações estão disponíveis:

   - ID do recurso: o ID do recurso. Escolha o ID de um recurso para abrir uma nova guia do navegador e visualizar o recurso em seu console de serviço nativo.
   - Tipo de recurso: o tipo de recurso.
   - Data do último compartilhamento: a data na qual o recurso foi compartilhado pela última vez.
   - Compartilhamentos de recurso: o número de compartilhamentos de recursos que incluem o recurso. Para ver a lista dos compartilhamentos de recursos, escolha o número.
   - Entidades principais: o número de entidades principais que podem acessar o recurso. Selecione o valor para visualizar as entidades principais.

AWS CLI

Para visualizar os recursos que você está compartilhando atualmente

Você pode usar o comando list-resources com o parâmetro `--resource-owner` definido como `SELF` para exibir detalhes dos recursos que você compartilha atualmente.

O exemplo a seguir mostra os recursos que estão incluídos nos compartilhamentos de recursos na Região da AWS (`us-east-1`) para a chamada Conta da AWS. Para obter os recursos que você compartilha em uma região diferente, use o parâmetro `--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"
        }
    ]
}
```

Visualizando os diretores com os quais você compartilha recursos em AWS RAM

Você pode visualizar as entidades principais com as quais compartilha seus recursos, em todos os compartilhamentos de recursos. A visualização desta lista de entidades principais ajuda a determinar quem tem acesso aos seus recursos compartilhados.

Console

Visualizar as entidades principais com as quais você está compartilhando

1. Navegue até a página Compartilhado por mim: Entidades principais no console do AWS RAM .
2. Como existem compartilhamentos de AWS RAM recursos específicos Regiões da AWS, escolha o apropriado na Região da AWS lista suspensa no canto superior direito do console. Para ver os compartilhamentos de recursos que contêm recursos globais, você deve Região da AWS definir o como Leste dos EUA (Norte da Virgínia), (`us-east-1`). Para obter mais informações sobre o compartilhamento de recursos globais, consulte Compartilhamento de recursos regionais em comparação com recursos globais.
3. Aplique um filtro para encontrar as entidades específicas. É possível aplicar vários filtros para restringir a pesquisa. Escolha a caixa de texto para ver uma lista suspensa dos campos de atributos sugeridos. Depois de escolher um, você pode escolher na lista de valores disponíveis para esse campo. Você pode adicionar outros atributos ou palavras-chave até encontrar o recurso desejado.

4. Para cada entidade principal na lista, o console exibe as seguintes informações:

   - ID principal: o ID da entidade principal. Escolha o ID para abrir uma nova guia do navegador e visualizar a entidade principal em seu console nativo.
   - Compartilhamentos de recursos: o número de compartilhamentos de recursos que você compartilhou com a entidade principal especificada. Escolha o número para visualizar a lista de compartilhamentos de recursos.
   - Recursos: o número de recursos que você compartilhou com a entidade principal. Selecione o número para visualizar os recursos compartilhados.

AWS CLI

Visualizar as entidades principais com as quais você está compartilhando

Você pode usar o comando list-principals para obter uma lista dos principais que você faz referência nos compartilhamentos de recursos que você criou no atual Região da AWS para a conta de chamada.

O exemplo a seguir lista as entidades que têm acesso aos compartilhamentos criados na região padrão da conta de chamada. Neste exemplo, os principais são a organização da conta chamante e uma separada Conta da AWS, como parte de dois compartilhamentos de recursos diferentes. Você deve usar o endpoint de serviço para o Região da AWS que contém o compartilhamento de recursos.

```
$ 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
        }
    ]
}
```

Excluindo um compartilhamento de recursos no AWS RAM

É possível excluir um compartilhamento de recurso a qualquer momento. Quando você exclui um compartilhamento de recursos, todos as entidades associadas ao compartilhamento de recursos perdem acesso aos recursos compartilhados. A exclusão de um compartilhamento de recursos não exclui os recursos compartilhados.

> **Para excluir um AWS recurso**
>
> Se você precisar excluir um AWS recurso incluído em um compartilhamento de recursos, AWS recomenda que você primeiro remova o recurso de qualquer compartilhamento de recursos que o inclua ou exclua o compartilhamento de recursos.

O compartilhamento de recursos excluído permanece visível no AWS RAM console por um curto período após a exclusão, mas seu status muda para`Deleted`.

Console

Para excluir um compartilhamento de recursos

1. Abra a página Compartilhado por mim: compartilhamentos de recursos no console do AWS RAM .
2. Como existem compartilhamentos de AWS RAM recursos específicos Regiões da AWS, escolha o apropriado na Região da AWS lista suspensa no canto superior direito do console. Para ver os compartilhamentos de recursos que contêm recursos globais, você deve Região da AWS definir o como Leste dos EUA (Norte da Virgínia), (`us-east-1`). Para obter mais informações sobre o compartilhamento de recursos globais, consulte Compartilhamento de recursos regionais em comparação com recursos globais.

3. Selecione o compartilhamento de recursos que você deseja excluir.

> **Warning**
>
> Certifique-se de selecionar o compartilhamento de recursos correto. Não é possível recuperar um compartilhamento de recurso após sua exclusão.

4. Escolha Excluir, digite a mensagem de confirmação e escolha Excluir.
5. O compartilhamento de recursos excluído desaparece após duas horas. Até lá, ele permanece visível no console com status excluído.

AWS CLI

Excluir o compartilhamento de um recurso

Você pode usar o delete-resource-sharecomando para excluir um compartilhamento de recursos que você não precisa mais.

O exemplo a seguir usa primeiro o get-resource-sharescomando para obter o Amazon Resource Name (ARN) do compartilhamento de recursos que você deseja excluir. Em seguida, ele é usado delete-resource-sharepara excluir o compartilhamento de recursos 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
}
```

Acessar os recursos da AWS compartilhados com você

O AWS Resource Access Manager (AWS RAM) permite a você visualizar os recursos aos quais você foi adicionado, os recursos compartilhados que podem ser acessados, e as Contas da AWS que compartilharam recursos com você. Também é possível sair de um compartilhamento de recursos quando não precisar mais acessar os seus recursos compartilhados.

Conteúdo

Aceitar e rejeitar os convites para compartilhamento de recursos

Para acessar recursos compartilhados, o proprietário do compartilhamento de recursos deve adicionar você como entidade principal. O proprietário pode adicionar qualquer um dos itens a seguir como entidade principal ao compartilhamento de recursos.

- A organização da qual sua conta é membro
- Uma unidade organizacional (OU) que contém a conta
- Sua conta individual
- Para tipos de recursos compatíveis, seu usuário ou perfil específico do IAM

Se você for adicionado ao compartilhamento de recursos por meio de um membro de uma organização e o compartilhamento dentro da organização estiver ativado, você terá acesso automático aos recursos compartilhados sem precisar aceitar um convite. Conta da AWS AWS

Organizations As entidades principais de serviços também têm acesso automático aos recursos compartilhados sem aceitar um convite. Se a conta pela qual você recebe acesso for posteriormente removida da organização, todas as entidades principais dessa conta perderão automaticamente o acesso aos recursos que foram acessados por meio desse compartilhamento de recursos.

Se você for adicionado a um compartilhamento de recursos por um dos seguintes itens, receberá um convite para ingressar no compartilhamento de recursos:

- Uma conta fora da sua organização no AWS Organizations
- Uma conta dentro da sua organização ao compartilhar com não AWS Organizations está habilitada

Se você receber um convite para participar de um compartilhamento de recurso, deverá aceitá-lo para acessar os recursos compartilhados. Se você recusar o convite, não poderá acessar os recursos compartilhados.

Para os seguintes tipos de recursos, você tem sete dias para aceitar o convite para participar do compartilhamento para os seguintes tipos de recursos. Se você não aceitar o convite antes que ele expire, ele será automaticamente recusado.

> **Important**
>
> Para tipos de recursos compartilhados que não estão na lista a seguir, você tem 12 horas para aceitar o convite para participar do compartilhamento de recursos. Depois de 12 horas, o convite expira e o usuário final da entidade principal no compartilhamento de recursos é desassociado. O convite não pode mais ser aceito pelos usuários finais.

- Amazon Aurora: clusters de banco de dados
- Amazon EC2: reservas de capacidade e hosts dedicados
- AWS License Manager — Configurações de licença
- AWS Outposts — Tabelas de rotas de gateway local, postos avançados e sites
- Amazon Route 53: regras de encaminhamento
- Amazon VPC — IPv4 endereços de propriedade do cliente, listas de prefixos, sub-redes, alvos de espelhamento de tráfego, gateways de trânsito, domínios multicast de gateway de trânsito

Console

Responder ao convite de compartilhamento de recursos

1. Navegue até a página Compartilhado comigo: compartilhamentos de recursos no AWS RAM console.
2. Como existem compartilhamentos de AWS RAM recursos específicos Regiões da AWS, escolha o apropriado na Região da AWS lista suspensa no canto superior direito do console. Para ver os compartilhamentos de recursos que contêm recursos globais, você deve Região da AWS definir o como Leste dos EUA (Norte da Virgínia), (`us-east-1`). Para obter mais informações sobre o compartilhamento de recursos globais, consulte Compartilhamento de recursos regionais em comparação com recursos globais.
3. Examine a lista de compartilhamentos de recursos aos quais você foi adicionado.

   A coluna Status indica seu status atual de participação no compartilhamento de recursos. O status `Pending` indica que você foi adicionado a um compartilhamento de recursos, mas ainda não aceitou ou rejeitou o convite.
4. Para responder ao convite de compartilhamento de recursos, selecione o ID do compartilhamento de recursos e escolha Aceitar compartilhamento de recursos para aceitar o convite ou Rejeitar compartilhamento de recursos para recusá-lo. Se você rejeitar o convite, não terá acesso aos recursos. Se você aceitar o convite, terá acesso aos recursos.

AWS CLI

Responder ao convite de compartilhamento de recursos

Você pode usar os seguintes comandos para aceitar ou rejeitar convites para um compartilhamento de recursos:

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

1. O exemplo a seguir começa usando o get-resource-share-invitationscomando para recuperar uma lista de todos os convites disponíveis para o usuário. Conta da AWS O AWS CLI `query` parâmetro permite restringir a saída somente aos convites com o parâmetro `status` definido

como. PENDING Este exemplo mostra que um convite da conta 111111111111 é atualmente PENDING para a conta atual 123456789012 na Região da 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. Depois de encontrar o convite que você deseja aceitar, anote o resourceShareInvitationArn na saída para usar no próximo comando para aceitar o convite.

```
$ 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"
```

```
    }
}
```

Se for bem-sucedida, observe que a resposta mostra que o `status` mudou de `PENDING` para `ACCEPTED`.

Se, em vez disso, você quiser rejeitar o convite, execute o reject-resource-share-invitationcomando com os mesmos parâmetros.

```
$ 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"
    }
}
```

Visualizando compartilhamentos de recursos compartilhados com você

Você pode visualizar os compartilhamentos de recursos aos quais você tem acesso. É possível ver quais entidades principais estão compartilhando recursos com você e quais recursos estão sendo compartilhados.

Console

Para ver os compartilhamentos de recursos

1. Navegue até a página Compartilhado comigo: compartilhamentos de recursos no console do AWS RAM .

2. Como existem compartilhamentos de AWS RAM recursos específicos Regiões da AWS, escolha o apropriado na Região da AWS lista suspensa no canto superior direito do console. Para ver os compartilhamentos de recursos que contêm recursos globais, você deve Região da AWS definir o como Leste dos EUA (Norte da Virgínia), (`us-east-1`). Para obter mais informações sobre o compartilhamento de recursos globais, consulte Compartilhamento de recursos regionais em comparação com recursos globais.
3. (Opcional) Aplique um filtro para encontrar recursos compartilhados específicos. É possível aplicar vários filtros para restringir a pesquisa. Você pode digitar uma palavra-chave, como parte do nome de um compartilhamento de recursos, para listar somente os compartilhamentos de recursos que incluem esse texto no nome. Escolha a caixa de texto para ver uma lista suspensa dos campos de atributos sugeridos. Depois de escolher um, você pode escolher na lista de valores disponíveis para esse campo. Você pode adicionar outros atributos ou palavras-chave até encontrar o recurso desejado.
4. O AWS RAM console exibe as seguintes informações:

   - Nome: o nome do compartilhamento de recursos.
   - ID: o ID do compartilhamento de recursos. Escolha o ícone para exibir a página de detalhes para aquele recurso.
   - Proprietário: o ID da Conta da AWS que criou o compartilhamento de recursos.
   - Status: o status atual do compartilhamento de recursos. Os possíveis valores incluem:
     - `Active`: o compartilhamento de recursos está ativo e disponível para uso.
     - `Deleted`: o compartilhamento de recursos foi excluído e não está mais disponível para uso.
     - `Pending`: um convite para aceitar o compartilhamento de recurso está aguardando uma resposta.

AWS CLI

Para ver os compartilhamentos de recursos

Use o get-resource-sharescomando com o `--resource-owner` parâmetro definido como`OTHER-ACCOUNTS`.

O exemplo a seguir mostra a lista de compartilhamentos de recursos compartilhados no especificado Região da AWS com a conta de chamada por outros Contas da 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"
        }
    ]
}
```

Acessar recursos compartilhados com você

É possível visualizar os recursos compartilhados que você pode acessar. Você pode ver quais entidades principais compartilharam os recursos com você e quais compartilhamentos de recursos incluem os recursos.

Console

Para ver os recursos compartilhados com você

1. Navegue até a página Compartilhado comigo: recursos compartilhados no console do AWS RAM.
2. Como os compartilhamentos de recursos do AWS RAM existem em Regiões da AWS específicas, escolha a Região da AWS apropriada na lista suspensa no canto superior direito do console. Para ver os compartilhamentos de recursos que contêm recursos globais, defina a Região da AWS como Leste dos EUA (Norte da Virgínia), (`us-east-1`). Para obter mais informações sobre o compartilhamento de recursos globais, consulte Compartilhamento de recursos regionais em comparação com recursos globais.
3. Aplique um filtro para encontrar recursos compartilhados específicos. É possível aplicar vários filtros para restringir a pesquisa.
4. As seguintes informações estão disponíveis:
   - ID do recurso: o ID do recurso. Selecione o ID do recurso para visualizá-lo no console do serviço.
   - Tipo de recurso: o tipo do recurso.
   - Data do último compartilhamento: a data na qual o recurso foi compartilhado com você.
   - Compartilhamentos de recursos: o número de compartilhamentos de recursos nos quais o recurso está incluído. Selecione o valor para visualizar os recursos compartilhados.
   - ID do proprietário: o ID da entidade principal que possui o recurso.

AWS CLI

Para ver os recursos compartilhados com você

Você pode usar o comando list-resources para visualizar os recursos que são compartilhados com você.

O comando de exemplo a seguir exibe detalhes sobre o recurso acessível por meio de um compartilhamento de recursos na Região da AWS especificada de outra Conta da 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"
        }
    ]
}
```

Visualizar as entidades principais que estão compartilhando com você

Visualizar uma lista de todas as entidades principais que estão compartilhando recursos com você. É possível ver quais recursos e compartilhamentos de recursos foram compartilhados com você.

Console

Visualizar uma lista de todas as entidades principais que estão compartilhando recursos com você

1. Abra o AWS RAM console em https://console.aws.amazon.com/ram/casa.
2. Como existem compartilhamentos de AWS RAM recursos específicos Regiões da AWS, escolha o apropriado na Região da AWS lista suspensa no canto superior direito do console. Para ver os compartilhamentos de recursos que contêm recursos globais, você deve Região da AWS definir o como Leste dos EUA (Norte da Virgínia), (`us-east-1`). Para obter mais informações sobre o compartilhamento de recursos globais, consulte Compartilhamento de recursos regionais em comparação com recursos globais.
3. No painel de navegação, selecione Shared with me (Compartilhados comigo), Principals (Principais).
4. (Opcional) É possível aplicar um filtro para encontrar entidades principais específicas. É possível aplicar vários filtros para restringir a pesquisa.
5. O console exibe as seguintes informações:

    - ID da entidade principal: o ID da entidade principal que está compartilhando com você.

- Compartilhamentos de recursos: o número de compartilhamentos de recursos aos quais o diretor adicionou você. Escolha o número para visualizar a lista de compartilhamentos de recursos.
- Recursos: o número de recursos que a entidade principal está compartilhando com você. Selecione o valor para visualizar a lista dos recursos.

AWS CLI

Visualizar uma lista de todas as entidades principais que estão compartilhando recursos com você.

Você pode usar o comando list-principals para recuperar a lista de diretores que estão compartilhando recursos com você. Conta da AWS

O exemplo de comando a Conta da AWS seguir exibe detalhes sobre quem compartilhou um compartilhamento de recursos com a conta usada para chamar a operação no especificado Região da AWS.

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

Sair de um compartilhamento de recursos

Se você não precisar mais de acesso aos recursos compartilhados com você, poderá sair de um compartilhamento de recursos a qualquer momento. Ao sair de um recurso compartilhado, você perderá o acesso aos recursos compartilhados.

Pré-requisitos para deixar o compartilhamento de um recurso

- Você pode deixar um compartilhamento de recursos somente se ele tiver sido compartilhado com você como Conta da AWS individual e não no contexto de uma organização. Você não pode deixar um compartilhamento de recursos se tiver sido adicionado a ele por alguém de Conta da AWS dentro da sua organização e o compartilhamento com AWS Organizations estiver ativado. O acesso aos compartilhamentos de recursos dentro de uma organização é automático.
- Para sair de um compartilhamento de recursos, verifique se o compartilhamento de recursos está vazio ou se contém somente tipos de recursos compatíveis com a saída de um compartilhamento.

  A seguir estão os únicos tipos de recursos que permitem deixar um compartilhamento de recursos.

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

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

Amazon Route 53	`route53resolver:ResolverRule`

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

Serviço	Tipo de atributo
	`ec2:TransitGatewayMulticastDomain`

Como deixar o compartilhamento de um recurso

Console

Deixar o compartilhamento de um recurso

1. Navegue até a página Compartilhado comigo: compartilhamentos de recursos no console do AWS RAM .
2. Como existem compartilhamentos de AWS RAM recursos específicos Regiões da AWS, escolha o apropriado na Região da AWS lista suspensa no canto superior direito do console. Para ver os compartilhamentos de recursos que contêm recursos globais, você deve Região da AWS definir o como Leste dos EUA (Norte da Virgínia), (`us-east-1`). Para obter mais informações sobre o compartilhamento de recursos globais, consulte Compartilhamento de recursos regionais em comparação com recursos globais.
3. Selecione o compartilhamento de recursos que você quer deixar.
4. Escolha Sair do compartilhamento de recursos e, na caixa de diálogo de confirmação, escolha Sair.

AWS CLI

Deixar o compartilhamento de um recurso

Você pode usar o disassociate-resource-sharecomando para deixar um compartilhamento de recursos.

Os comandos de exemplo a seguir fazem com Conta da AWS que o comando que chama o comando perca o acesso aos recursos compartilhados pelo compartilhamento de recursos especificado pelo ARN. Você deve direcionar a solicitação para o endpoint do serviço na Região da AWS que contém o compartilhamento de recursos que você deseja deixar.

1. Primeiro, recupere a lista de compartilhamentos de recursos para recuperar o ARN do compartilhamento de recursos que você deseja deixar.

```
$ 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"
        }
    ]
}
```

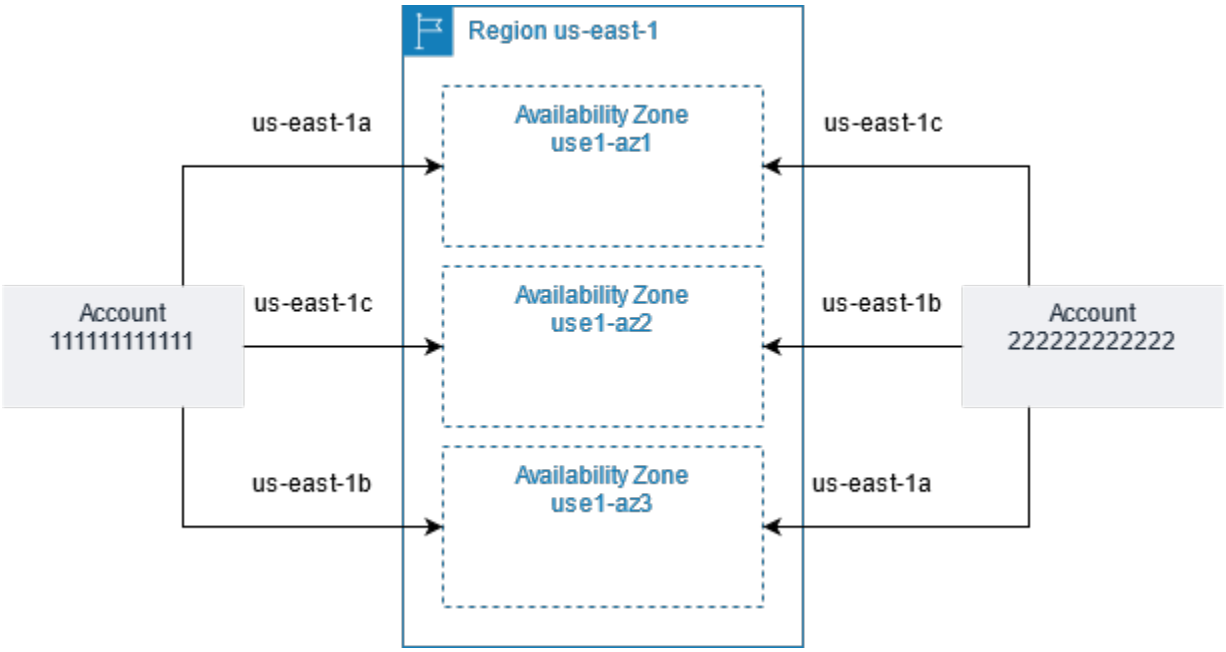
2. Em seguida, você pode executar o comando para deixar o compartilhamento de recursos. Observe que você também deve especificar o ID da sua conta, 123456789012, como entidade principal para se desassociar do compartilhamento de recursos especificado, que é compartilhado por conta 111111111111.

```
$ 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
        }
    ]
}
```

IDs de zona de disponibilidade para seus recursos da AWS

A AWS mapeia as Zonas de Disponibilidade físicas aleatoriamente com os nomes das zonas de disponibilidade de cada Conta da AWS. Essa abordagem ajuda a distribuir recursos pelas Zonas de Disponibilidade em uma Região da AWS, em vez de os recursos provavelmente estarem concentrados na zona de disponibilidade “a” de cada região. Como resultado, a Zona de Disponibilidade `us-east-1a` da sua conta da AWS pode não representar a mesma localização física de `us-east-1a` de outra conta da AWS. Para obter mais informações, consulte Regiões e Zonas de Disponibilidade no Guia do usuário do Amazon EC2.

A ilustração a seguir mostra como os IDs da AZ são os mesmos para todas as contas, embora os nomes das zonas de disponibilidade possam ser mapeados de forma diferente para cada conta.



Para alguns recursos, você deve identificar não apenas a Região da AWS, mas também a Zona de Disponibilidade. Por exemplo, uma sub-rede Amazon VPC. Em uma única conta, o mapeamento de uma Zona de Disponibilidade para um nome específico não é importante. Mas, quando você usa o AWS RAM para compartilhar esse recurso com outras Contas da AWS, o mapeamento é importante. Esse mapeamento aleatório complica a capacidade da conta de acessar o recurso compartilhado de saber qual zona de disponibilidade deve ser referenciada. Para ajudar com isso, esses recursos também permitem que você identifique a localização real de seus recursos em relação às suas contas usando o ID de AZ. O ID de AZ é um identificador exclusivo e consistente de uma Zona de Disponibilidade em todas as Contas da AWS. Por exemplo, `use1-az1` é um ID de Zona de

Disponibilidade da Região `us-east-1` e representa a mesma localização física em todas as contas da AWS.

É possível visualizar os IDs de AZs para determinar o local de recursos em uma conta em relação aos recursos em outra conta. Por exemplo, se você compartilhar uma sub-rede na zona de disponibilidade com o ID de AZ `use1-az2` com outra conta, essa sub-rede estará disponível para essa conta na zona de disponibilidade cujo ID de AZ também é `use1-az2`. O ID de AZ de cada VPC e sub-rede é exibido no console da Amazon VPC e pode ser consultado usando a AWS CLI.

Console

Para visualizar os AZ IDs das zonas de disponibilidade em sua conta

1. Navegue até a página do console do AWS RAM no console do AWS RAM.
2. Você pode ver os IDs de AZ da Região da AWS atual em Seu ID de AZ.

AWS CLI

Para visualizar os AZ IDs das zonas de disponibilidade em sua conta

O exemplo de comando a seguir mostra os IDs de AZ para as zonas de disponibilidade na região us-west-2 e como eles são mapeados para a chamada Conta da AWS.

```
$ 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 compartilháveis AWS

Com AWS Resource Access Manager (AWS RAM), você pode compartilhar recursos criados e gerenciados por outros Serviços da AWS. Você pode compartilhar recursos com indivíduos Contas da AWS. Você também pode compartilhar recursos com as contas em uma organização ou unidades organizacionais (OUs) em AWS Organizations. Alguns tipos de recursos compatíveis também permitem que você compartilhe recursos com funções e usuários individuais AWS Identity and Access Management (IAM).

As seções a seguir listam os tipos de recursos, agrupados por AWS service (Serviço da AWS), que você pode compartilhar usando AWS RAM. As colunas nas tabelas especificam quais recursos cada tipo de recurso suporta:

Pode compartilhar com usuários e perfis do IAM	 — você pode compartilhar recursos desse tipo com funções e usuários individuais AWS Identity and Access Management (IAM), além de contas.	Sim
	 : você pode compartilhar recursos desse tipo somente com contas.	Não
Pode compartilhar com contas fora da organização	 : você só pode compartilhar recursos desse tipo com contas individuais, dentro ou fora da organização. Consulte mais informações em Considerações.	Sim

	 : você pode compartilhar recursos desse tipo somente com contas que sejam membros da mesma organização.	Não
Pode usar permissões gerenciadas pelo cliente	Todos os tipos de recursos suportados pelas permissões AWS gerenciadas AWS RAM oferecem suporte, mas um Sim nesta coluna significa que as permissões gerenciadas pelo cliente também são suportadas para esse tipo de recurso.	
	 : recursos desse tipo oferecem suporte ao uso de permissões gerenciadas pelo cliente.	Sim
	 : recursos desse tipo não oferecem suporte ao uso de permissões gerenciadas pelo cliente.	Não
Pode compartilhar com as entidades principais de serviços	 : você pode compartilhar recursos desse tipo com Serviços da AWS.	Sim
	 : você não pode compartilhar recursos desse tipo com Serviços da AWS.	Não

AWS App Mesh

Você pode compartilhar os seguintes AWS App Mesh recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Malhas `appmesh:Mesh`	Crie e gerencie uma malha centralmente e compartilhe-a com outras Contas da AWS ou com sua organização. Uma malha compartilhada permite que recursos criados por diferentes Contas da AWS se comuniquem entre si na mesma malha. Para obter mais informações, consulte Trabalhar com recursos compartilhados no Guia do usuário do AWS App Mesh .	 S	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

AWS AppSync API do GraphQL

Você pode compartilhar os seguintes recursos da API AWS AppSync GraphQL usando. AWS RAM

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
AppSync GraphyQL APIs `appsync:Apis`	Gerencie o AWS AppSync GraphQL APIs centralmente e compartilhe-o com outras pessoas Contas da AWS ou com sua organização. Isso permite que várias contas sejam compartilhadas AWS AppSync APIs como parte da criação de uma API AWS AppSync mesclada unificada que pode acessar dados de vários subesquemas em diferentes contas na mesma região. Para obter mais informações, consulte Mesclado APIs no Guia do AWS AppSync desenvolvedor.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Amazon API Gateway

Você pode compartilhar os seguintes recursos do Amazon API Gateway usando o AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Domínios personalizados privados do API Gateway `apigateway:Domainnames`	Crie e gerencie nomes de domínio centralmente e compartilhe-os com outras pessoas Contas da AWS ou com sua organização. Isso permite que várias contas invoquem seus nomes de domínio que estão mapeados como privados. APIs Para obter mais informações, consulte Nomes de domínio personalizados para uso privado APIs no API Gateway no Guia do desenvolvedor do Amazon API Gateway.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Amazon Application Recovery Controller (ARC)

Você pode compartilhar os seguintes recursos do Amazon Application Recovery Controller (ARC) usando o AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Cluster do ARC do Route 53 `route53-recovery-control:Cluster`	Crie e gerencie clusters ARC centralmente e compartilhe-os com outras pessoas Contas da AWS ou com sua organização. Isso permite que várias contas criem painéis de controle e controles de roteamento em um único cluster compartilhado, reduzindo a complexidade e o número total de clusters que uma organização exige. Para obter mais informações, consulte Compartilhamento de clusters entre contas no Guia do desenvolvedor do Amazon Applicati	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	on Recovery Controller (ARC).				
Planos de mudança de região do ARC `arc-region-switch:Plan`	Crie e gerencie planos centralmente e compartilhe-os com outras Contas da AWS ou com sua organização. Isso permite que várias contas usem recursos de uma conta diferente da conta que hospeda o plano. Para obter mais informações, consulte Mudança de região no Guia do desenvolvedor do Amazon Application Recovery Controller (ARC).	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Amazon Aurora

Você pode compartilhar os seguintes recursos do Amazon Aurora usando o AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Clusters de bancos de dados Aurora `rds:Cluster`	Crie e gerencie um cluster de banco de dados centralmente e compartilhe-o com outras Contas da AWS ou com sua organização. Isso permite que várias Contas da AWS clonem um cluster de banco de dados compartilhado e gerenciado centralmente. Para obter mais informações, consulte Clonagem entre contas AWS RAM e com o Amazon Aurora no Guia do usuário do Amazon Aurora.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

AWS Backup

Você pode compartilhar os seguintes AWS Backup recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Cofres de backup `backup:BackupVault`	Crie e gerencie centralmente cofres isolados de forma lógica e compartilhe-os com outras pessoas ou com sua organização. Contas da AWS Essa opção permite que várias contas acessem e restaurem backups dos cofres. Para obter mais informações, consulte Visão geral dos cofres logicamente isolados no Guia do desenvolvedor do AWS Backup .	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Amazon Bedrock

Você pode compartilhar os seguintes recursos do Amazon Bedrock usando o AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Modelo personalizado do Bedrock `bedrock:CustomModel`	Crie e gerencie o modelo personalizado centralmente e compartilhe-o com outras Contas da AWS ou com sua organização. Isso permite que várias contas usem o mesmo modelo personalizado para aplicações de IA generativa. Para obter mais informações, consulte Compartilhar um modelo com outra conta no Guia do usuário do Amazon Bedrock.	 Sim	 Não Pode compartilhar apenas com Contas da AWS em sua própria organização.	 Sim	 Não

Gerenciamento de Faturamento e Custos

Você pode compartilhar os seguintes recursos do Billing and Cost Management usando o AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Painéis do BCM `bcm-dashboards:dashboard`	Crie e gerencie painéis do Billing and Cost Management e compartilhe-os com outras Contas da AWS dentro ou fora da sua organização. Ao compartilhar um painel, somente as configurações do painel são compartilhadas, não os dados subjacentes. Os destinatários recebem acesso ao layout do painel e às configurações do widget e verão os dados com base em suas próprias permissões de acesso. Esse recurso de compartilhamento permite que as organizações estabeleçam práticas comuns de geração de relatórios de custos e ajudem diferentes	 N	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	equipes a visualizar os dados de custos de forma consistente. Para obter mais informações, consulte Compartilhamento de painéis no Guia do usuário do Billing and Cost Management.				

AWS Billing Exibir serviço

Você pode compartilhar os seguintes recursos do AWS Billing View Service usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Visualizações de faturamento `billing:billingview`	Crie e gerencie visualizações de faturamento personalizadas de forma	N	N	S	Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	centralizada e compartilhe-as com outras pessoas Contas da AWS ou com sua organização. Isso permite que proprietários de aplicações e unidades de negócios acessem os gastos da AWS no nível da unidade de negócios a partir de uma conta de membro. Para obter mais informações, consulte Compartilhamento de visualizações de faturamento personalizadas no Guia do usuário do AWS Cost Management .		Pode compartilhar apenas com Contas da AWS em sua própria organização.		

AWS Cloud Map

Você pode compartilhar os seguintes AWS Cloud Map recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
AWS Cloud Map Namespaces `servicediscovery:Namespace`	Crie e gerencie namespaces de forma centralizada e compartilhe-os com outras Contas da AWS em sua organização. Isso permite que vários serviços e instâncias de descoberta de Contas da AWS no namespace compartilhado sem a necessidade de credenciais temporárias. Para obter mais informações, consulte Exclusão de namespaces do AWS Cloud Map no Guia de desenvolvedor do AWS Cloud Map .	 S	 N Pode compartilhar apenas com Contas da AWS em sua própria organização.	 S	 Não

AWS WAN em nuvem

Você pode compartilhar os seguintes recursos do AWS Cloud WAN usando AWS RAM o.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Redes de núcleos `networkmanager:CoreNetwork`	Crie e gerencie uma rede central de WAN em nuvem centralmente e compartilhe-a com outras Contas da AWS pessoas. Isso permite que vários hosts Contas da AWS acessem e provision em em uma única rede central de WAN em nuvem. Para obter mais informações, consulte Compartilhar uma rede principal no Guia do usuário do AWS Cloud WAN.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Amazon CloudFront

Você pode compartilhar os seguintes CloudFront recursos da Amazon usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Amazon CloudFront VpcOrigin `cloudfront:VpcOrigin`	Crie e gerencie as origens da CloudFront VPC centralmente e compartilhe-as com outras pessoas Contas da AWS ou com sua organização. Isso permite que vários Contas da AWS usem origens de uma VPC compartilhada para CloudFront distribuições. Para obter mais informações, consulte Como trabalhar com recursos compartilhados CloudFront no Amazon CloudFront Developer Guide.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

AWS CloudHSM

Você pode compartilhar os seguintes AWS CloudHSM recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
AWS CloudHSM Backups `cloudhsm:Backup`	Gerencie AWS CloudHSM os backups centralmente e compartilhe-os com outras pessoas Contas da AWS ou com sua organização. Isso permite que vários Contas da AWS usuários visualizem informações sobre o Backup e as usem para restaurar um AWS CloudHSM cluster. Para ter mais informações, consulte Gerenciamento de backups do AWS CloudHSM no Guia de usuário do AWS CloudHSM .	 S	 S	 S	 Não

AWS CodeBuild

Você pode compartilhar os seguintes AWS CodeBuild recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
CodeBuild Projetos `codebuild:Project`	Crie um projeto e use-o para executar compilações. Compartilhe o projeto com outras pessoas Contas da AWS ou com sua organização. Isso permite que várias Contas da AWS e usuários visualizem informações sobre um projeto e analisem suas construções. Para obter mais informações, consulte Trabalhar com projetos compartilhados no Guia do usuário do AWS CodeBuild .	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não
CodeBuild Grupos de relatórios `codebuild:ReportGroup`	Crie um grupo de relatórios e use-o para criar relatórios ao criar um projeto. Compartilhe o grupo de relatórios com outras pessoas Contas da AWS ou com sua organizaç	 S	 S Pode compartilhar com qualquer	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	ão. Isso permite que vários Contas da AWS usuários visualizem o grupo de relatórios e seus relatórios e os resultados do caso de teste de cada relatório. Um relatório pode ser visualizado por 30 dias após sua criação e, em seguida, ele expira e não está mais disponível para visualização. Para obter mais informações, consulte Trabalhar com projetos compartilhados no Guia do usuário do AWS CodeBuild .		Conta da AWS.		

Conexões de código da AWS

Você pode compartilhar os seguintes CodeConnections recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Conexões de código `codeconnections:Connection`	Gerencie a reutilização de conexões de código em várias contas. Em outras palavras, compartilhar conexões de código reduz a carga do administrador e a necessidade de acesso do administrador em todas as contas que exigem uma conexão de código. Para obter mais informações, consulte Compartilhar conexões com Contas da AWS no Guia de usuário do console de ferramentas do desenvolvedor.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Amazon DataZone

Você pode compartilhar os seguintes DataZone recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
DataZone Domínios `datazone:Domain`	Crie e gerencie domínios centralmente e compartilhe-os com outras Contas da AWS ou com sua organização. Isso permite que várias contas criem DataZone domínios da Amazon. Para obter mais informações, consulte O que é a Amazon DataZone no Guia DataZone do usuário da Amazon.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Amazon EC2

Você pode compartilhar os seguintes recursos do Amazon EC2 usando o AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Reservas de capacidade `ec2:CapacityReservation`	Crie e gerencie reservas de capacidade centralmente e compartilhe a capacidade reservada com outras pessoas Contas da AWS ou com sua organização. Isso permite que várias instâncias do Amazon EC2 Contas da AWS iniciem em uma capacidade reservada gerenciada centralmente. Para obter mais informações, consulte Trabalho com reservas de capacidade compartilhadas no Guia do usuário do Amazon EC2. Compartilhe blocos de capacidade para ML (ainda não UltraServer CBs há suporte) com outras pessoas	 N	Sim para reservas de capacidade (pode compartilhar com qualquer pessoa Conta da AWS). Não para blocos de capacidade (só podem ser compartilhados Contas da AWS em sua própria organização).	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	Contas da AWS ou com sua organização. Esse recurso permite que cargas de trabalho executadas em diferentes Contas da AWS instâncias do Amazon EC2 iniciem seus blocos de capacidade, ajudando você a utilizar melhor sua capacidade reservada e a economizar custos. Para obter mais informações, consulte Como trabalhar com blocos de capacidade compartilhados no Guia do usuário do Amazon EC2. **Important** Se você não atender a todos os pré-requisitos para				

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	compartilhar uma reserva de capacidade, a operação de compartilhamento poderá falhar. Se isso acontecer e um usuário tentar iniciar uma instância do Amazon EC2 nessa reserva de capacidade, ela será iniciada como uma instância sob demanda que pode gerar custos mais altos. Recomendamos que você verifique se pode acessar a reserva de capacidad				

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	e compartilhada tentando visualizá-la no console do Amazon EC2. Você também pode monitorar falhas no compartilhamento de recursos para poder tomar medidas corretivas antes que os usuários iniciem instâncias de forma a aumentar seus custos. Para obter mais informações, consulte Exemplo: alertas sobre falhas no compartil				

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	hamento de recursos.				
Hosts dedicados `ec2:DedicatedHost`	Aloque e gerencie centralmente os hosts dedicados do Amazon EC2 e compartilhe a capacidade da instância do host com Contas da AWS outras pessoas ou com sua organização. Isso permite que várias instâncias do Amazon EC2 Contas da AWS iniciem em hosts dedicados gerenciados centralmente. Para obter mais informações, consulte Trabalho com hosts dedicados compartilhados no Guia de usuário do Amazon EC2.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Grupos de posicionamento `ec2:PlacementGroup`	Compartilhe os grupos de colocação que você possui em toda a sua organização Contas da AWS, dentro e fora da sua organização. Você pode iniciar instâncias do Amazon EC2 de qualquer uma das contas com as quais você compartilha em um grupo de entrada compartilhado. Para obter mais informações, consulte Compartilhar um grupo de entrada no Guia de usuário do Amazon EC2.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

EC2 Image Builder

Você pode compartilhar os seguintes recursos do EC2 Image Builder usando o AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Componentes do Image Builder `imagebuilder:Component`	Crie e gerencie componentes centralmente e compartilhe-os com outras Contas da AWS ou com sua organização. Gerencie quem pode usar componentes predefinidos de criação e teste em suas fórmulas de imagens. Para obter mais informações, consulte Compartilhar recursos do Construtor de imagens EC2 no Guia do usuário do Construtor de imagens EC2.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não
Fórmulas de contêineres do Image Builder `imagebuilder:ContainerRecipe`	Crie e gerencie suas receitas de contêineres de forma centralizada e compartilhe-as com outras pessoas Contas da AWS ou com sua organização. Isso permite que	 S	 S Pode compartilhar com qualquer	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	você gerencie quem pode usar documentos predefinidos para duplicar a criação de imagens de contêiner. Para obter mais informações, consulte Compartilhar recursos do Construtor de imagens EC2 no Guia do usuário do Construtor de imagens EC2.		Conta da AWS.		

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Imagens do Image Builder `imagebuilder:Image`	Crie e gerencie suas imagens douradas de forma centralizada e compartilhe-as com outras pessoas Contas da AWS ou com sua organização. Gerencie quem pode usar imagens criadas com o Construtor de imagens EC2 em toda a sua organização. Para obter mais informações, consulte Compartilhar recursos do Construtor de imagens EC2 no Guia do usuário do Construtor de imagens EC2.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Fórmulas de imagens do Image Builder `imagebuilder:ImageRecipe`	Crie e gerencie suas receitas de imagens centralmente e compartilhe-as com outras pessoas Contas da AWS ou com sua organização. Isso permite que você gerencie quem pode usar documentos predefinidos para duplicar as compilações da AMI. Para obter mais informações, consulte Compartilhar recursos do Construtor de imagens EC2 no Guia do usuário do Construtor de imagens EC2.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Elastic Load Balancing

Você pode compartilhar os seguintes recursos do Elastic Load Balancing usando o AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Armazenamentos confiáveis do ELB `elasticloadbalancing:TrustStore`	Crie e gerencie lojas confiáveis do Elastic Load Balancing de forma centralizada e compartilhe-as com outras pessoas Contas da AWS ou com sua organização. Os administradores de segurança podem manter um número único ou menor de armazenamentos confiáveis e habilitar configurações de TLS mútuo nos Application Load Balancers. Para obter informações, consulte Compartilhar seu armazenamento confiável do Elastic Load Balancing para Application Load Balancers no Guia de usuário de Application Load Balancers.	 S	 S	 N	 Não

AWS End User Messaging SMS

Você pode compartilhar o seguinte AWS End User Messaging SMS recurso usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
AWS SMS Listas de exclusão por voz `sms-voice:OptOutList`	Crie uma lista de exclusão e compartilhe-a com outras pessoas da sua Contas da AWS organização. Você pode compartilhar a lista de exclusão para que as outras aplicações possam excluir números de telefone do usuário de diferentes Contas da AWS ou verifiquem o status do número de telefone do usuário. Para obter mais informações, consulte Trabalhando com recursos compartilhados no Guia AWS End User Messaging SMS do usuário.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
AWS SMS Números de telefone de voz `sms-voice:PhoneNumber`	Crie e gerencie números de telefone e compartilhe-os com outras Contas da AWS ou sua organização. Isso permite que várias Contas da AWS enviem mensagens usando o número de telefone compartilhado. Para obter mais informações, consulte Trabalhando com recursos compartilhados no Guia AWS End User Messaging SMS do usuário.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Sim

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
AWS SMS Pool de voz `sms-voice:Pool`	Crie e gerencie pools para compartilhá-los com outras pessoas Contas da AWS ou com sua organização. Isso permite que várias mensagens sejam Contas da AWS enviadas usando o pool compartilhado. Para obter mais informações, consulte Trabalhando com recursos compartilhados no Guia AWS End User Messaging SMS do usuário.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Sim

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
AWS SMS Remetente de voz IDs `sms-voice:SenderId`	Crie e gerencie o remetente IDs e compartilhe-o com outras pessoas Contas da AWS ou com sua organização. Isso permite que várias Contas da AWS enviem mensagens usando o ID de remetente compartilhado. Para obter mais informações, consulte Trabalhando com recursos compartilhados no Guia AWS End User Messaging SMS do usuário.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Sim

Amazon FSx para OpenZFS

Você pode compartilhar os seguintes recursos do Amazon FSx for OpenZFS usando. AWS RAM

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
FSx Volumes `fsx:Volume`	Crie e FSx gerencie volumes OpenZFS centralmente e compartilhe-os com outras pessoas Contas da AWS ou com sua organização. Isso permite que várias contas realizem a replicação de dados usando OpenZfs instantâneos em volumes compartilhados por meio FSx APIs `CreateVolume` de ou. `CopySnapshotAndUpdateVolume` Para obter mais informações, consulte Replicação de dados sob demanda no Guia do usuário do Amazon FSx for OpenZFS.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

AWS Glue

Você pode compartilhar os seguintes AWS Glue recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
AWS Glue Catálogo `glue:Catalog`	Gerencie um catálogo de dados central e compartilhe metadados sobre bancos de dados e tabelas com Contas da AWS sua organização. Isso permite que os usuários executem consultas sobre dados em várias contas. Para obter mais informações, consulte Compartilhamento de tabelas e bancos de dados do catálogo de dados entre contas da AWS no AWS Lake Formation Guia do desenvolvedor do .	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não
AWS Glue bancos de dados	Crie e gerencie bancos de dados de catálogos de dados de forma centralizada e compartil	 N	 S	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
`glue:Database`	he-os com Contas da AWS sua organização. Bancos de dados são coleções de tabelas de catálogos de dados. Isso permite que os usuários executem consultas e trabalhos de extração, transformação e carregamento (ETL) que podem unir e consultar dados em várias contas. Para obter mais informações, consulte Compartilhamento de tabelas e bancos de dados do catálogo de dados entre contas da AWS no Guia do desenvolvedor do AWS Lake Formation .		Pode compartilhar com qualquer Conta da AWS.		

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
AWS Glue Tabelas `glue:Table`	Crie e gerencie tabelas de catálogos de dados de forma centralizada e compartilhe-as com Contas da AWS sua organização. As tabelas do catálogo de dados contêm metadados sobre tabelas de dados no Amazon S3, fontes de dados JDBC, Amazon Redshift, fontes de streaming e outros armazenamentos de dados. Isso permite que os usuários executem consultas e trabalhos de ETL que podem unir e consultar dados em várias contas. Para obter mais informações, consulte Compartilhamento de tabelas e bancos de dados do catálogo de dados entre contas da AWS	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	no Guia do desenvolvedor do AWS Lake Formation .				

AWS License Manager

Você pode compartilhar os seguintes AWS License Manager recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Configurações de licença `license-manager:LicenseConfiguration`	Crie e gerencie configurações de licenças centralmente e compartilhe-as com outras pessoas Contas da AWS ou com sua organização. Isso permite que você aplique regras de licenciamento	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	gerenciadas centralmente, baseadas nos termos dos contratos empresariais em vários Contas da AWS. Para obter mais informações, consulte Uso de configurações de licença e Configurações no Guia do usuário do License Manager.				

AWS Marketplace

Você pode compartilhar os seguintes AWS Marketplace recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Entidades de catálogo do Marketplace `aws-marketplace:Entity`	Crie, gerencie e compartilhe entidades em Contas da AWS ou dentro de sua organização no AWS Marketplace. Para obter mais informações, consulte Compartilhamento de recursos no AWS RAM na Referência do AWS Marketplace Catalog API .	 S	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

AWS Migration Hub Refactor Spaces

Você pode compartilhar os seguintes AWS Migration Hub Refactor Spaces recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Refatorar ambientes de espaços `refactor-spaces:Environment`	Crie um ambiente para Refatorar ambientes de espaços e use-o para conter seus aplicativos de Refatorar ambientes de espaços. Compartilhe o ambiente com outras Contas da AWS ou com todas as contas da sua organização. Isso permite que vários Contas da AWS usuários visualizem informações sobre o ambiente e os aplicativos nele contidos. Para obter mais informações, consulte Compartilhar Refatorar ambientes de espaços usando o AWS RAM no Guia do usuário do AWS Migration Hub Refactor Spaces .	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Aprovação Multilateral

Você pode compartilhar os seguintes recursos de aprovação multilateral usando o AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Equipe de aprovação multilateral `mpa:ApprovalTeam`	Crie e gerencie equipes de aprovação e compartilhe-as com outras Contas da AWS ou sua organização. Isso permite que outras Contas da AWS usem uma equipe de aprovação associada a uma operação protegida. Uma operação protegida é uma lista predefinida de operações que exigem a aprovação da equipe antes de serem executadas. Para obter mais informações, consulte Termos e conceitos no Guia de usuário de aprovação multilateral.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

AWS Network Firewall

Você pode compartilhar os seguintes AWS Network Firewall recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Firewalls de rede `network-firewall:Firewall`	Crie e gerencie firewalls de rede centralmente e compartilhe-os com outras Contas da AWS para que possam criar endpoints de firewall. Isso permite que várias contas usem as proteções de um único firewall. Para obter mais informações, consulte Compartilhamento de AWS Network Firewall recursos no Guia do AWS Network Firewall desenvolvedor.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não
Políticas do firewall de rede `network-firewall:F`	Crie e gerencie políticas de firewall centralmente e compartilhe-as com outras pessoas Contas da AWS ou	 S	 S Pode compartil	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
`irewallPolicy`	com sua organização. Isso permite que várias contas em uma organização compartilhem um conjunto comum de comportamentos de monitoramento, proteção e filtragem de rede. Para obter mais informações, consulte Compartilhamento de AWS Network Firewall recursos no Guia do AWS Network Firewall desenvolvedor.		har com qualquer Conta da AWS.		

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços

Grupos de regras do firewall de rede
 	
`network-firewall:StatefulRuleGroup`
 	
`network-firewall:StatelessRuleGroup`
	Crie e gerencie grupos de regras sem estado e com estado centralmente e compartilhe-os com outras pessoas Contas da AWS ou com sua organização. Isso permite que várias contas em uma organização compartilhem AWS Organizations um conjunto de critérios para inspecionar e lidar com o tráfego de rede. Para obter mais informações, consulte Compartilhamento de AWS Network Firewall recursos no Guia do AWS Network Firewall desenvolvedor.	S	S
			
			Pode compartilhar com qualquer Conta da AWS.
				N	Não

Oracle Database@AWS

Você pode compartilhar os seguintes Oracle Database@AWS recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Oracle Database@AWS Infraestrutura Exadata `odb:CloudExadataInfrastructure`	Com Oracle Database@AWS, você pode compartilhar sua infraestrutura do Exadata e sua rede ODB entre várias Contas da AWS na mesma organização. AWS Isso permite provisionar a infraestrutura uma vez e reutilizá-la em contas confiáveis, reduzindo custos e separando responsabilidades. Para obter mais informações, consulte Compartilhamento de recursos Oracle Database@AWS no Guia Oracle Database@AWS do usuário.	N	N Pode compartilhar apenas com Contas da AWS em sua própria organização.	N	Não
Oracle Database@AWS Rede ODB	Com Oracle Database@AWS, você pode compartil	N	N	N	Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
`odb:OdbNetwork`	har sua infraestrutura do Exadata e sua rede ODB entre várias pessoas Contas da AWS na mesma organização. AWS Isso permite provisionar a infraestrutura uma vez e reutilizá-la em contas confiáveis, reduzindo custos e separando responsabilidades. Para obter mais informações, consulte Compartilhamento de recursos Oracle Database@AWS no Guia Oracle Database@AWS do usuário.		Pode compartilhar apenas com Contas da AWS em sua própria organização.		

AWS Outposts

Você pode compartilhar os seguintes AWS Outposts recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Outposts `outposts:Outpost`	Crie e gerencie Outposts de forma centralizada e compartilhe-os com outras Contas da AWS da sua organização. Isso permite que várias contas criem sub-redes e volumes do EBS em seus Outposts compartilhados e gerenciados centralmente. Para obter mais informações, consulte Trabalhando com recursos compartilhados do AWS Outposts no Guia do AWS Outposts Usuário.	N	N Pode compartilhar apenas com Contas da AWS em sua própria organização.	S	Não
Tabelas de rotas de gateway local `ec2:LocalGatewayRouteTable`	Crie e gerencie associações de VPC com um gateway local de forma centralizada e compartilhe-as com outras pessoas	N	N Pode compartilhar	N	Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	Contas da AWS em sua organização. Isso permite que várias contas criem associações de VPC com um gateway local e visualizem a tabela de rotas e a configuração da interface virtual. Para obter mais informações, consulte Compartilhar seus recursos de Outpost no Guia do usuário do AWS Outposts .		apenas com Contas da AWS em sua própria organização.		

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Sites do Outposts `outposts:Site`	Crie e gerencie sites do Outpost e compartilhe-os com outras Contas da AWS em sua organização. Isso permite que várias contas criem e gerenciem Outposts no site compartilhado e oferece suporte ao controle dividido entre os recursos do Outpost e o site. Para obter mais informações, consulte Trabalhando com recursos compartilhados do AWS Outposts no Guia do AWS Outposts Usuário.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Amazon S3 on Outposts

Você pode compartilhar o seguinte recurso do Amazon S3 nos Outposts usando o AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
S3 em Outposts `s3-outposts:Outpost`	Crie e gerencie buckets, pontos de acesso e endpoints do Amazon S3 no Outpost. Isso permite que várias contas criem e gerenciem Outposts no site compartilhado e oferece suporte ao controle dividido entre os recursos do Outpost e o site. Para obter mais informações, consulte Trabalhando com recursos compartilhados do AWS Outposts no Guia do AWS Outposts Usuário.	 N	 N Pode compartilhar apenas com Contas da AWS em sua própria organização.	 S	 Não

Autoridade de Certificação Privada da AWS

Você pode compartilhar os seguintes CA privada da AWS recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Autoridade de certificação privada (CAs) `acm-pca:CertificateAuthority`	Crie e gerencie autoridades de certificação privadas (CAs) para a infraestrutura de chave pública (PKI) interna da sua organização e compartilhe-as CAs com outras pessoas Contas da AWS ou com sua organização. Isso permite que os usuários da AWS Certificate Manager de outras contas emitam certificados X.509 assinados pela sua CA compartilhada. Para obter mais informações, consulte Controlar o acesso a uma CA privada no Guia do usuário do Autoridade de Certificação Privada da AWS .	 S	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Sim

Explorador de recursos da AWS

Você pode compartilhar os seguintes Explorador de recursos da AWS recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Visualizações do Explorador de Recursos `resource-explorer-2:View`	Crie e configure as visualizações do Resource Explorer de forma centralizada e compartilhe-as com outras pessoas Contas da AWS em sua organização. Isso permite que funções e usuários em várias áreas Contas da AWS pesquisem e descubram os recursos acessíveis por meio da visualização. Para obter mais informações, consulte Compartilhar visualizações do Explorador de Recursos no Guia do usuário do Explorador de recursos da AWS .	 N	 N Pode compartilhar apenas com Contas da AWS em sua própria organização.	 N	 Não

AWS Resource Groups

Você pode compartilhar os seguintes AWS Resource Groups recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Resource Groups (Grupos de recursos) `resource-groups:Group`	Crie e gerencie um grupo de recursos do host centralmente e compartilhe-o com outras pessoas Contas da AWS da sua organização. Isso permite que várias Contas da AWS compartilhem um grupo de hosts dedicados do Amazon EC2 criados usando a AWS License Manager. Para obter mais informações, consulte Grupos de recursos de host na AWS License Manager no Guia do usuário da AWS License Manager.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Amazon Route 53

Você pode compartilhar os seguintes recursos do Amazon Route 53 usando o AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Grupos de regras do firewall do resolvedor do Route 53 `route53resolver:FirewallRuleGroup`	Crie e gerencie grupos de regras do Route 53 Resolver DNS Firewall centralmente e compartilhe-os com outras pessoas Contas da AWS ou com sua organização. Isso permite que várias contas compartilhem um conjunto de critérios para inspecionar e lidar com consultas ao DNS de saída que passam pelo resolvedor do Route 53. Para obter mais informações, consulte Compartilhar grupos de regras do DNS Firewall do resolvedor do Route 53 entre Contas da AWS no Guia do desenvolv	S	S Pode compartilhar com qualquer Conta da AWS.	N	Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	edor do Amazon Route 53.				
Rota 53 Profiles `route53profiles:Profile`	Crie e gerencie o Route 53 Profiles centralmente e compartilhe-o com outras pessoas Contas da AWS ou com sua organização. Isso permite que várias contas apliquem as configurações de DNS especificadas no Route 53 Profiles a várias. VPCs Para obter mais informações, consulte Profiles do Amazon Route 53 no Guia de desenvolvedor do Amazon Route 53.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Regra do resolvedor `route53resolver:ResolverRule`	Crie e gerencie as regras do Resolver centralmente e compartilhe-as com outras pessoas Contas da AWS ou com sua organização. Isso permite que várias contas encaminhem consultas de DNS de suas nuvens privadas virtuais (VPCs) para os endereços IP de destino definidos nas regras do Resolver compartilhadas e gerenciadas centralmente. Para obter mais informações, consulte Compartilhando regras do Resolver com outros Contas da AWS e usando regras compartilhadas no Guia do desenvolvedor do Amazon Route 53.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Configurações de log de consultas do resolvedor `route53resolver:ResolverQueryLogConfig`	Crie e gerencie logs de consultas centralmente e compartilhe-os com outras Contas da AWS ou com sua organização. Isso permite que várias Contas da AWS consultas de DNS originadas em um registro de consultas VPCs gerenciado centralmente. Para obter mais informações, consulte Compartilhar as configurações de log de consultas do resolvedor com outras Contas da AWS no Guia do desenvolvedor do Amazon Route 53.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Amazon Simple Storage Service

Você pode compartilhar os seguintes Amazon Simple Storage Service recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Concessão de Acesso do S3 `s3:AccessGrants`	Crie e gerencie centralmente a instância S3 Access Grants e compartilhe-a com outras pessoas Contas da AWS ou com sua organização. Isso permite que várias contas visualizem e excluam recursos compartilhados. Para obter mais informações, consulte O S3 Access concede acesso entre contas no Guia do Amazon Simple Storage Service usuário.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Sim

SageMaker IA da Amazon

Você pode compartilhar os seguintes recursos de SageMaker IA da Amazon usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
SageMaker Catálogos de recursos de IA `sagemaker:SagemakerCatalog`	Para ser descoberto — permite que os proprietários de contas concedam permissões de descoberta a outras contas, para todos os recursos do grupo de recursos no catálogo de SageMaker IA. Depois de concedido o acesso, os usuários dessas contas podem visualizar os grupos de recursos que foram compartilhados com eles no catálogo. Para obter mais informações, consulte Capacidade de descoberta e acesso a grupos de recursos entre contas no Amazon SageMaker AI Developer Guide. **Note** A capacidade de descobert	N	S Pode compartilhar com qualquer Conta da AWS.	S	Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	a e o acesso são permissões separadas na SageMaker IA.				

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
SageMaker Grupos de recursos de IA `sagemaker:FeatureGroup`	Para acesso: permite que os proprietários da conta concedam permissões de acesso a outras contas, para selecionar recursos do grupo de recursos. Depois de concedido o acesso, os usuários dessas contas podem usar os grupos de recursos que foram compartilhados com eles. Para obter mais informações, consulte Capacidade de descoberta e acesso a grupos de recursos entre contas no Amazon SageMaker AI Developer Guide. **Note** A capacidade de descoberta e o acesso são permissõe	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	s separadas na SageMaker IA.				
SageMaker Hubs de IA `sagemaker:Hub`	Com o Amazon SageMaker AI JumpStart, você pode criar e gerenciar `sagemaker:Hub` centralmente e compartilhá-los com outras pessoas Contas da AWS na mesma organização. Para obter mais informações, consulte Controle o acesso ao modelo básico usando hubs privados com curadoria na Amazon SageMaker AI JumpStart no Amazon SageMaker AI Developer Guide.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
SageMaker Grupos de linhagem de IA `sagemaker:LineageGroup`	A Amazon SageMaker AI permite que você crie grupos de linhagem dos metadados do seu pipeline para obter uma compreensão mais profunda de sua história e relacionamentos. Compartilhe o grupo de linhagem com outras contas Contas da AWS ou com as contas da sua organização. Isso permite que vários Contas da AWS usuários visualizem informações sobre o grupo de linhagem e consultem as entidades de rastreamento dentro dele. Para obter mais informações, consulte Rastreamento de linhagem entre contas no Amazon SageMaker AI Developer Guide.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
SageMaker Cartões de modelo AI `sagemaker:ModelCard`	A Amazon SageMaker AI cria cartões de modelo para documentar detalhes críticos sobre seus modelos de aprendizado de máquina (ML) em um único local para simplificar a governança e a geração de relatórios. Compartilhe seus cartões-modelo com outras Contas da AWS ou com as contas de sua organização para obter uma estratégia de várias contas para suas operações de machine learning. Isso permite Contas da AWS compartilhar o acesso dos cartões-modelo para suas atividades de ML com outras contas. Para obter mais informações, consulte	 S	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	Amazon SageMaker AI Model Cards no Amazon SageMaker AI Developer Guide.				
SageMaker Grupos de pacotes do AI Model `sagemaker:model-package-group`	Com o Amazon SageMaker AI Model Registry, você pode criar e gerenciar `sagemaker:model-package-group` centralmente e compartilhá-los com outras pessoas Contas da AWS para registrar versões do modelo. Para obter mais informações, consulte Amazon SageMaker AI Model Registry no Amazon SageMaker AI Developer Guide.	 S	 S	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
SageMaker Aplicativos de parceiros de IA `sagemaker:PartnerApp`	Com os aplicativos SageMaker AI Partner AI, você pode criar e gerenciar aplicativos SageMaker AI Partner AI centralmente e compartilhar o acesso a eles com outras Contas da AWS pessoas. Para obter mais informações, consulte Configurar o compartilhamento entre contas para aplicativos de SageMaker IA parceiros da Amazon AI no Amazon SageMaker AI Developer Guide.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
SageMaker Pipelines de IA `sagemaker:Pipeline`	Com o Amazon SageMaker AI Model Building Pipelines, você pode criar, automatizar e gerenciar fluxos de trabalho de aprendizado end-to-end de máquina em grande escala. Compartilhe seus pipelines com outras contas Contas da AWS ou com as da sua organização para obter uma estratégia de várias contas para suas operações de aprendizado de máquina. Isso permite que vários Contas da AWS usuários visualizem informações sobre um pipeline e suas execuções com acesso opcional para iniciar, interromper e repetir pipelines de outras contas. Para	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	obter mais informações, consulte Cross-Account Support for SageMaker AI Pipelines no Amazon SageMaker AI Developer Guide.				

AWS Service Catalog AppRegistry

Você pode compartilhar os seguintes AWS Service Catalog AppRegistry recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
AppRegistry Aplicações `servicecatalog:Applications`	Crie um aplicativo e use-o para rastrear os recursos pertencentes a esse aplicativo em todo o seu AWS ambiente. Compartilhe	 N	 N Pode compartil	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	o aplicativo com outra pessoa Contas da AWS ou com sua organização. Isso permite que vários Contas da AWS usuários visualizem informações sobre o aplicativo e os recursos associados a ele localmente. Para obter mais informações, consulte Criar aplicações no Guia do usuário do serviço de catálogo.		har apenas com Contas da AWS em sua própria organização.		

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
AppRegistry Grupos de atributos `servicecatalog:AttributeGroups`	Crie um grupo de atributos e use-o para armazenar metadados relacionados aos seus aplicativos. Compartilhe os grupos de atributos com outras Contas da AWS ou com sua organização. Isso permite que várias Contas da AWS e usuários visualizem informações sobre os grupos de atributos . Para obter mais informações, consulte Criação de grupos de atributos no Guia do usuário do catálogo de serviços.	 N	 N Pode compartilhar apenas com Contas da AWS em sua própria organização.	 S	 Não

AWS Systems Manager Incident Manager

Você pode compartilhar os seguintes AWS Systems Manager Incident Manager recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Incident Manager Contacts `ssm-contacts:Contact`	Crie e gerencie contatos e planos de escalonamento centralmente e compartilhe os detalhes de contato com outras pessoas Contas da AWS ou com sua organização. Isso permite que muitos Contas da AWS visualizem os engajamentos que ocorrem durante um incidente. **Note** Atualmente, a capacidade de adicionar um contato compartilhado de outra conta com um plano de resposta a	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	incidentes não é permitida. Para obter mais informações, consulte Como trabalhar com contatos e planos de resposta no Guia do usuário do AWS Systems Manager Incident Manager.				

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Planos de resposta do Incident Manager `ssm-incidents:ResponsePlan`	Crie e gerencie planos de resposta centralmente e compartilhe-os com outras pessoas Contas da AWS ou com sua organização. Isso permite que eles Contas da AWS conectem CloudWatch os alarmes da Amazon e as regras de EventBridge eventos da Amazon aos planos de resposta, criando automaticamente um incidente quando ele é detectado. O incidente também tem acesso às métricas dessas outras Contas da AWS. Para obter mais informações, consulte Como trabalhar com contatos e planos de resposta no AWS Guia do usuário do Systems Manager Incident Manager.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

AWS Systems Manager

Você pode compartilhar os seguintes AWS Systems Manager recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Políticas de negação automática do SSM JITNA `ssm:Document`	Crie uma política de aprovação para acesso ao just-in-time nó com o Systems Manager. Uma política de negação de acesso impede explicitamente a aprovação automática de solicitações de acesso aos nós que você especificar. Compartilhe a política de negação de acesso com outras pessoas Contas da AWS ou com sua organização. Isso garante que sua política de negação de acesso ao just-in-time nó se aplique a todas as contas em sua organização. Para obter mais informações, consulte acesso ao	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	Just-in-time nó usando o Systems Manager no Guia AWS Systems Manager do Usuário.				

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Parâmetros avançados de armazenamento de parâmetros `ssm:Parameter`	Crie um parâmetro e use-o para armazenar dados de configuração que você poderá mencionar em seus scripts, comandos, documentos SSM e fluxos de trabalho de configuração e automação. Compartilhe o parâmetro com outra pessoa Contas da AWS ou com sua organização. Isso permite que várias Contas da AWS e usuários visualizem informações sobre a string e melhorem a segurança separando seus dados do seu código. Para obter mais informações, consulte Trabalho com parâmetros compartilhados no Guia de	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	usuário do AWS Systems Manager .				

Amazon VPC

Você pode compartilhar os seguintes recursos da Amazon Virtual Private Cloud (Amazon VPC) usando o AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Propriedade do cliente IPv4pool `ec2:CoipPool`	Durante o processo de AWS Outposts instalação, AWS cria um pool de endereços , conhecido como pool de endereços IP de propriedade do cliente, com base nas informações que você	 N	 N Pode compartilhar apenas com Contas	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	fornece sobre sua rede local. Os endereços IP de propriedade do cliente (CoIPs) fornecem conectividade local ou externa aos recursos nas sub-redes do Outpost por meio de sua rede on-premises. Você pode atribuir esses endereços a recursos em seu Outpost, como instâncias EC2, usando endereços IP elásticos ou usando a configuração de sub-rede que atribui automaticamente endereços IP de propriedade do cliente. Para obter mais informações, consulte Customer-owned IP addresses no Guia do usuário do AWS Outposts .		da AWS em sua própria organização.		

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Pools do IPAM `ec2:IpamPool`	Compartilhe os pools IPAM da Amazon VPC centralmente com outras funções ou usuários do IAM Contas da AWS, ou com uma organização ou unidade organizacional (OU) inteira em. AWS Organizations Isso permite que esses diretores aloquem AWS recursos CIDRs do pool, por exemplo VPCs, em suas respectivas contas. Para obter mais informações, consulte Compartilhar um pool IPAM usando o AWS RAM no Guia do usuário do Gerenciador de endereços IP da Amazon VPC.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Descobertas de recursos do IPAM `ec2:IpamResourceDiscovery`	Compartilhe descobertas de recursos com outros Contas da AWS. Uma descoberta de recursos é um componente IPAM da Amazon VPC que permite que o IPAM gerencie e monitore recursos que pertencem à conta proprietária. Para obter mais informações, consulte Trabalhar com descobertas de recurso no Guia do usuário da Amazon VPC IPAM.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Listas de prefixos `ec2:PrefixList`	Crie e gerencie listas de prefixos centralmente e compartilhe-as com outras pessoas Contas da AWS ou com sua organização. Isso permite várias listas de prefixos de referência de Contas da AWS em seus recursos, como grupos de segurança de VPC e tabelas de rotas de sub-rede. Para obter mais informações, consulte Trabalhar com listas de prefixos compartilhadas no Guia do usuário da Amazon VPC.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Sub-redes `ec2:Subnet`	Crie e gerencie sub-redes de forma centralizada e compartilhe-as com Contas da AWS em sua organização. Isso permite que várias Contas da AWS iniciem seus recursos de aplicativos em VPCs gerenciadas centralmente. Esses recursos incluem instâncias do Amazon EC2, bancos de dados Amazon Relational Database Service (RDS) Amazon Relational Database Service (RDS), clusters e funções do Amazon Redshift. AWS Lambda Para obter mais informações, consulte Trabalhar com VPCs compartilhadas no Guia do usuário da Amazon VPC.	 N	 N Pode compartilhar apenas com Contas da AWS em sua própria organização.	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	Note Para incluir uma sub-rede ao criar um compartilhamento de recursos, você deve ter as permissões `ec2:DescribeSubnets` e `ec2:DescribeVpcs`, além de `ram:CreateResourceShare`. As sub-redes padrão não são compartilháveis. Você só pode compartilhar sub-redes criadas por você mesmo.				

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Grupos de segurança `ec2:SecurityGroup`	Crie e gerencie grupos de segurança centralmente e compartilhe-os com outras pessoas Contas da AWS ou com sua organização. Isso permite que várias Contas da AWS associem o grupo de segurança às interfaces de rede elásticas. Para obter mais informações, consulte Compartilhar um grupo de segurança no Guia de usuário da Amazon VPC.	 S	 N Pode compartilhar apenas com Contas da AWS em sua própria organização.	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Destino de espelho de tráfego `ec2:TrafficMirrorTarget`	Crie e gerencie alvos de espelhos de tráfego centralmente e compartilhe-os com outras pessoas Contas da AWS ou com sua organização. Isso permite que várias Contas da AWS enviem tráfego de rede espelhado de fontes de espelhamento de tráfego em suas contas para um destino de espelhamento de tráfego compartilhado e gerenciado centralmente. Para obter mais informações, consulte Destinos de espelhamento de tráfego entre contas no Guia de espelhamento de tráfego.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Gateways de trânsito `ec2:TransitGateway`	Crie e gerencie gateways de trânsito centralmente e compartilhe-os com outras pessoas Contas da AWS ou com sua organização. Isso permite que várias pessoas Contas da AWS roteiem o tráfego entre suas redes VPCs e as redes locais por meio de um gateway de trânsito compartilhado e gerenciado centralmente. Para obter mais informações, consulte Compartilhar um gateway de trânsito em Gateways de trânsito da Amazon VPC. **Note** Para incluir um gateway de trânsito ao criar	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	um compartilhamento de recursos, você deve ter a permissão `ec2:DescribeTransitGateway` , além de `ram:CreateResourceShare` .				

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Domínio multicast do gateway de trânsito `ec2:TransitGatewayMulticastDomain`	Crie e gerencie domínios multicast do Transit Gateway de forma centralizada e compartilhe-os com outras pessoas Contas da AWS ou com sua organização. Isso permite que vários Contas da AWS registrem e cancelem o registro de membros do grupo ou fontes de grupos no domínio multicast. Para obter mais informações, consulte Como trabalhar com domínios multicast compartilhados no Guia de gateway de trânsito.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Acesso Verificado pela AWS grupos `ec2:VerifiedAccessGroup`	Crie e gerencie Acesso Verificado pela AWS grupos de forma centralizada e, em seguida, compartilhe-os com outras pessoas Contas da AWS ou com sua organização. Isso permite que aplicativos em várias contas usem um único conjunto compartilhado de Acesso Verificado pela AWS endpoints. Para obter mais informações, consulte Compartilhe seu Acesso Verificado pela AWS grupo AWS Resource Access Manager no Guia do Acesso Verificado pela AWS usuário.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Amazon VPC Lattice

Você pode compartilhar os seguintes recursos da Amazon VPC Lattice usando o AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Configuração de recurso do Amazon VPC Lattice `vpc-lattice:ResourceConfiguration`	Crie uma configuração de recursos no Amazon VPC Lattice para compartilhar recursos de VPC entre contas e. VPCs Na configuração de recurso, você identifica quem pode acessar esse recurso e especifica o gateway de recursos por meio do qual deseja compartilhar o recurso. Os consumidores podem acessar o recurso de VPC por meio de um endpoint da VPC de recursos criado em AWS PrivateLink. Para obter mais informações, consulte Acessar recursos da VPC por meio do AWS PrivateLink no Guia de usuário do AWS PrivateLink e Configuração de recursos da VPC no	 N	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	Guia do usuário do VPC Lattice.				
Serviços do Amazon VPC Lattice `vpc-lattice:Service`	Crie e gerencie serviços do Amazon VPC Lattice centralmente e compartilhe-os com indivíduos Contas da AWS ou com sua organização. Isso permite que os proprietários de serviços se conectem, protejam e observem a service-to-service comunicação em um ambiente com várias contas. Para obter mais informações, consulte Trabalhar com recursos compartilhados no Guia do usuário do VPC Lattice.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com usuários e perfis do IAM	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Rede de serviços da Amazon VPC Lattice `vpc-lattice:ServiceNetwork`	Crie e gerencie redes de serviços Amazon VPC Lattice centralmente e compartilhe-as com indivíduos Contas da AWS ou com sua organização. Isso permite que os proprietários da rede de serviços se conectem, protejam e observem a service-to-service comunicação em um ambiente com várias contas. Para obter mais informações, consulte Como trabalhar com recursos compartilhadas no Guia do usuário da Amazon VPC Lattice.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Gerenciando permissões em AWS RAM

Em AWS RAM, há dois tipos de permissões gerenciadas: permissõesAWS gerenciadas e permissões gerenciadas pelo cliente.

As permissões gerenciadas definem como um consumidor pode agir sobre os recursos em um compartilhamento de recursos. Ao criar um compartilhamento de recursos, você deve especificar qual permissão gerenciada usar para cada tipo de recurso incluído no compartilhamento de recursos. O modelo de política na permissão gerenciada contém tudo o que é necessário para uma política baseada em recursos, exceto a entidade principal e o recurso. O Amazon Resource Name (ARN) do recurso e o ARN dos diretores associados ao compartilhamento de recursos completam os elementos de uma política baseada em recursos.AWS RAM em seguida, cria a política baseada em recursos que ela atribui a todos os recursos desse compartilhamento de recursos.

Cada permissão gerenciada pode ter uma ou mais versões. Uma versão é designada como a versão padrão para essa permissão gerenciada. Ocasionalmente,AWS atualiza uma permissão AWS gerenciada para um tipo de recurso criando uma nova versão e designando essa nova versão como padrão. Você também pode atualizar suas permissões gerenciadas pelo cliente criando novas versões. As permissões gerenciadas que já estão anexadas a um compartilhamento de recursos não são atualizadas automaticamente. O console do AWS RAM indica quando uma nova versão padrão está disponível, e você pode revisar as alterações na nova versão padrão em comparação com a anterior.

> **Note**
>
> Recomendamos que você atualize para a nova versão da permissão AWS gerenciada assim que possível. Essas atualizações geralmente adicionam suporte para novos ou atualizados Serviços da AWS que podem compartilhar outros tipos de recursos usando AWS RAM. Uma nova versão padrão também pode abordar e corrigir vulnerabilidades de segurança.

> **Important**
>
> Você só pode anexar a versão padrão da permissão gerenciada a um novo compartilhamento de recursos.

É possível recuperar a lista das permissões gerenciadas disponíveis a qualquer momento. Para obter mais informações, consulte Visualizando permissões gerenciadas.

Tópicos

Visualizando permissões gerenciadas

Você pode ver detalhes sobre as permissões gerenciadas que estão disponíveis para atribuição a tipos de recursos em seus compartilhamentos de recursos. Você pode identificar as permissões gerenciadas atribuídas aos compartilhamentos de recursos. Para ver esses detalhes, use a Biblioteca de permissões gerenciadas no console do AWS RAM.

Console

Para ver detalhes sobre as permissões gerenciadas disponíveis em AWS RAM

1. Navegue até a página da Biblioteca de permissões gerenciadas no console do AWS RAM.
2. Como os compartilhamentos de recursos do AWS RAM existem em Regiões da AWS específicas, escolha a Região da AWS apropriada na lista suspensa no canto superior direito do console. Para ver os compartilhamentos de recursos que contêm recursos globais, defina a Região da AWS como Leste dos EUA (Norte da Virgínia), (`us-east-1`). Para obter mais informações sobre o compartilhamento de recursos globais, consulte Compartilhamento de recursos regionais em comparação com recursos globais. Embora todas as regiões compartilhem as mesmas permissões gerenciadas da AWS disponíveis, isso afeta o número de compartilhamentos de recursos associados exibidos para cada permissão gerenciada em Step 5. As permissões gerenciadas pelo cliente estão disponíveis somente na região em que foram criadas.
3. Na lista Permissões gerenciadas, escolha a permissão gerenciada da qual você deseja ver detalhes. Você pode usar a caixa de pesquisa para filtrar a lista de permissões gerenciadas

inserindo parte de um nome ou tipo de recurso, ou escolhendo um tipo de permissão gerenciada na lista suspensa.

4. (Opcional) Para alterar as preferências de exibição, escolha o ícone de engrenagem no canto superior direito do painel Permissões gerenciadas. Você pode alterar as seguintes preferências:

   - Tamanho da página: o número de recursos exibidos em cada página.
   - Quebrar linhas: se as linhas devem ser quebradas nas linhas da tabela.
   - Colunas: se deseja exibir ou ocultar informações sobre o tipo de recurso e os compartilhamentos associados.

   Depois de concluir a configuração das preferências de exibição, escolha Confirmar.

5. Para cada permissão gerenciada, a lista exibe as seguintes informações:

   - Nome da permissão gerenciada: o nome da permissão gerenciada.
   - Tipo de recurso: o tipo de recurso associado à permissão gerenciada.
   - Tipo de permissão gerenciada: se a permissão gerenciada é uma permissão gerenciada da AWS ou uma permissão gerenciada pelo cliente.
   - Compartilhamentos associados: o número de compartilhamentos de recursos associados à permissão gerenciada. Se um número aparecer, você poderá escolher o número para exibir uma tabela de compartilhamentos de recursos com as seguintes informações:
     - Nome do compartilhamento de recursos: o nome do compartilhamento de recursos associado à permissão gerenciada.
     - Versão da permissão gerenciada: a versão da permissão gerenciada que está anexada a esse compartilhamento de recursos.
     - Proprietário: o número da Conta da AWSdo proprietário do compartilhamento de recursos.
     - Permitir entidades principais externas: se esse compartilhamento de recursos permite o compartilhamento com entidades de fora da organização em AWS Organizations.
     - Status: o status atual da associação entre o compartilhamento de recursos e a permissão gerenciada.
   - Status: descreve se a permissão gerenciada é:
     - Anexável: você pode anexar a permissão gerenciada aos seus compartilhamentos de recursos.

- Não anexável: você não pode anexar a permissão gerenciada aos seus compartilhamentos de recursos.
- Excluindo: a permissão gerenciada não está mais ativa e será excluída em breve.
- Excluído: a permissão gerenciada foi excluída. Ela permanece visível por duas horas antes de desaparecer da Biblioteca de permissões gerenciadas.

Você pode escolher o nome da permissão gerenciada para exibir mais informações sobre essa permissão gerenciada. A página de detalhes de uma permissão gerenciada exibe as seguintes informações:

- Tipo de recurso: o tipo de recurso da AWS ao qual essa permissão gerenciada se aplica.
- Número de versões: você pode ter até cinco versões de uma permissão gerenciada pelo cliente.
- Versão padrão: especifica qual versão é a padrão e, portanto, atribuída automaticamente a todos os novos compartilhamentos de recursos que usam essa permissão gerenciada. Todos os compartilhamentos de recursos existentes que usam versões diferentes exibem uma solicitação para que você atualize o compartilhamento de recursos para a versão padrão.
- ARN: o nome do recurso da Amazon (ARN) da permissão gerenciada. Os ARNs para permissões gerenciadas da AWS usam o seguinte formato:

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

  A substring *[DefaultPermission]* (sem os colchetes em um ARN real) está presente no nome somente da única permissão gerenciada para esse tipo de recurso que é designada como padrão.
- Versões de permissão gerenciada: você pode escolher as informações da versão a serem exibidas nas guias abaixo dessa lista suspensa.
  - Guia de detalhes:
    - Hora da criação: a data e a hora em que essa versão da permissão gerenciada foi criada.
    - Hora da última atualização: a data e a hora em que essa versão da permissão gerenciada foi atualizada pela última vez.

- Guia do modelo de política: a lista de ações e condições de serviço, se aplicável, que essa versão da permissão gerenciada permite que as entidades principais executem no tipo de recurso associado.
- Compartilhamentos de recursos associados: a lista de compartilhamentos de recursos que usam essa versão da permissão gerenciada.

AWS CLI

Para ver detalhes sobre as permissões gerenciadas disponíveis em AWS RAM

Você pode usar o comando list-permissions para obter uma lista das permissões gerenciadas disponíveis para uso em compartilhamentos de recursos na Região da AWS atual para a conta de chamada.

```
$ 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"
        }
    ]
}
```

Você também pode encontrar o ARN de uma permissão gerenciada específica pelo nome no parâmetro `--query` do comando `list-permissions` da AWS CLI. O exemplo a seguir filtra a saída para incluir somente elementos nos resultados da matriz `permissions` que correspondam ao nome especificado. Também especificamos que queremos ver somente o campo ARN nos resultados e em formato de texto simples, em vez do JSON padrão.

```
$ aws ram list-permissions \
    --query "permissions[?name == 'My-Test-CMP'].arn \
```

```
    --output text
arn:aws:ram:us-east-1:123456789012:permission/My-Test-CMP
```

Depois de encontrar o ARN da permissão gerenciada específica na qual você está interessado, você pode recuperar seus detalhes, incluindo o texto da política JSON, executando o 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"
    }
}
```

Criação e uso de permissões gerenciadas pelo cliente no AWS RAM

AWS Resource Access Manager (AWS RAM) fornece pelo menos uma permissão AWS gerenciada para cada tipo de recurso que você pode compartilhar. No entanto, essas permissões gerenciadas podem não fornecer o privilégio mínimo de acesso para seu caso de uso de compartilhamento. Quando uma das permissões AWS gerenciadas fornecidas não funciona, você pode criar sua própria permissão gerenciada pelo cliente.

As permissões gerenciadas pelo cliente são permissões gerenciadas que você cria e mantém especificando com precisão quais ações podem ser executadas sob quais condições com recursos compartilhados usando o AWS RAM. Por exemplo, você quer limitar o acesso de leitura aos seus grupos do Gerenciador de endereços IP (IPAM) da Amazon VPC, que ajudam você a gerenciar seus endereços IP em grande escala. Você pode criar permissões gerenciadas pelo cliente para que seus desenvolvedores atribuam endereços IP, mas não visualizem o intervalo de endereços IP que outras contas de desenvolvedor atribuem. É possível seguir as práticas recomendadas de privilégio mínimo, conceda apenas as permissões necessárias para executar tarefas em recursos compartilhados.

Além disso, você pode atualizar ou excluir as permissões gerenciadas pelo cliente conforme necessário.

Tópicos

Criar uma permissão gerenciada pelo cliente

As permissões gerenciadas pelo cliente são específicas para um Região da AWS. Certifique-se de criar essa permissão gerenciada pelo cliente na região apropriada.

Console

Para criar uma permissão gerenciada pelo cliente

1. Execute um destes procedimentos:
   - Navegue até a Biblioteca de permissões gerenciadas e escolha Criar uma permissão gerenciada pelo cliente.
   - Navegue diretamente até a página Criar uma permissão gerenciada pelo cliente no console.
2. Em Detalhes da permissão gerenciada pelo cliente, insira o nome da permissão gerenciada pelo cliente.
3. Escolha o tipo de recurso ao qual essa permissão gerenciada se aplica.

4. Para Modelo de política, você define quais operações podem ser executadas nesse tipo de recurso.

   - Você pode escolher Importar permissão gerenciada para usar ações de uma permissão gerenciada existente.
   - Selecione ou desmarque as informações do nível de acesso para atender às suas necessidades no editor visual.
   - Adicione ou modifique condições usando o editor JSON.

5. (Opcional) Para anexar tags à permissão gerenciada, para Tags, insira uma chave e um valor de tag. Para adicionar mais tags, selecione Adicionar nova tag. Repita esta etapa conforme necessário.
6. Quando concluir, escolha Criar permissão gerenciada pelo cliente.

AWS CLI

Para criar uma permissão gerenciada pelo cliente

- Execute o comando create-permission e especifique um nome, o tipo de recurso ao qual a permissão gerenciada pelo cliente se aplica e o corpo do texto do modelo de política.

  O comando de exemplo a seguir cria uma permissão gerenciada para o 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
```

```
    }
}
```

Criar uma nova versão de uma permissão gerenciada pelo cliente

Se o caso de uso da permissão gerenciada pelo cliente mudar, você poderá criar uma nova versão da permissão gerenciada. Isso não afeta seus compartilhamentos de recursos existentes, somente os novos compartilhamentos de recursos futuros que usarem essa permissão gerenciada pelo cliente.

Cada permissão gerenciada pode ter até cinco versões, mas você pode associar somente a versão padrão.

Console

Para criar uma nova versão de uma permissão gerenciada pelo cliente

1. Navegue até a Biblioteca de permissões gerenciadas.
2. Filtre a lista de permissões gerenciadas por Gerenciado pelo cliente ou pesquise o nome da permissão gerenciada pelo cliente que você deseja alterar.
3. Na página de detalhes da permissão gerenciada, na seção Versões de permissões gerenciadas, escolha Criar versão.
4. Para Modelo de política, você pode adicionar ou remover ações e condições com o editor visual ou o editor JSON.

   Você também tem a opção de escolher Importar permissão gerenciada para usar um modelo de política existente.
5. Quando concluir, escolha Criar versão na parte inferior da página.

AWS CLI

Para criar uma nova versão de uma permissão gerenciada pelo cliente

1. Encontre o nome do recurso da Amazon (ARN) da permissão gerenciada para a qual você deseja criar uma nova versão. Faça isso chamando list-permissions com o parâmetro `--permission-type CUSTOMER_MANAGED` para incluir somente as permissões gerenciadas pelo 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. Depois de ter o ARN, você pode chamar a create-permission-versionoperação e fornecer o modelo de política atualizado.

```
$ 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
    }
}
```

A saída inclui o número da nova versão.

Escolha uma versão diferente para ser a padrão para uma permissão gerenciada pelo cliente

Você pode definir outra versão de permissão gerenciada pelo cliente como a nova versão padrão.

Console

Para definir uma nova versão padrão para uma permissão gerenciada pelo cliente

1. Navegue até a Biblioteca de permissões gerenciadas.
2. Filtre a lista de permissões gerenciadas por Gerenciado pelo cliente ou pesquise o nome da permissão gerenciada pelo cliente que você deseja alterar.
3. Na página Detalhes da permissão gerenciada pelo cliente, na seção Versões de permissões gerenciadas, use a lista suspensa para escolher a versão que você deseja definir como o novo padrão.
4. Escolha Definir como padrão.
5. Quando a caixa de diálogo for exibida, confirme que você deseja que essa versão seja a padrão para todos os novos compartilhamentos de recursos que usarem essa permissão gerenciada pelo cliente. Se você concordar, escolha Definir como versão padrão.

AWS CLI

Para definir uma nova versão padrão para uma permissão gerenciada pelo cliente

1. Encontre o número da versão que você deseja definir como a versão padrão ligando para list-permission-versions.

   O comando de exemplo a seguir recupera as versões atuais da permissão gerenciada especificada.

```
$ 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. Depois de definir o número da versão como padrão, você pode chamar a set-default-permission-versionoperação.

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

Este comando não retorna nenhuma saída se for bem-sucedido. Você pode executar list-permission-versionsnovamente e verificar se o `defaultVersion` campo da versão escolhida agora está definido como`true`.

Excluir uma versão de permissão gerenciada pelo cliente

Você pode ter até cinco versões de cada permissão gerenciada pelo cliente. Quando uma versão não for mais necessária e não estiver em uso, você poderá excluí-la. Você não pode excluir a versão

padrão de uma permissão gerenciada pelo cliente. As versões excluídas permanecem visíveis no console por até duas horas com um status excluído antes de serem completamente removidas.

Console

Para excluir uma versão de permissão gerenciada pelo cliente

1. Navegue até a Biblioteca de permissões gerenciadas.
2. Filtre a lista de permissões gerenciadas por Gerenciado pelo cliente ou pesquise o nome da permissão gerenciada pelo cliente com a versão que você deseja excluir.
3. Certifique-se de que a versão que você deseja excluir não seja a padrão.
4. Na seção Versões da página, escolha a guia Compartilhamentos de recursos associados para ver se algum compartilhamento usa essa versão.

   Se houver algum compartilhamento associado, você deverá alterar a versão da permissão gerenciada pelo cliente antes de excluir essa versão.
5. Escolha Excluir versão no lado direito da seção Versão.
6. Na caixa de diálogo de confirmação, selecione Excluir para confirmar que deseja excluir essa versão da sua permissão gerenciada pelo cliente.

   Escolha Cancelar se não quiser excluir essa versão da sua permissão gerenciada pelo cliente.

AWS CLI

Para excluir uma versão de uma permissão gerenciada pelo cliente

1. Ligue para a list-permission-versionsoperação para recuperar os números de versão disponíveis.
2. Depois de ter o número da versão, forneça-o como um parâmetro para delete-permission-version.

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

   Este comando não retorna nenhuma saída se for bem-sucedido. Você pode executar list-permission-versionsnovamente e verificar se a versão não está mais incluída na saída.

Excluir uma permissão gerenciada pelo cliente

Se uma permissão gerenciada pelo cliente não for mais necessária e não estiver em uso, você poderá excluí-la. Você não pode excluir um cliente que esteja associado a uma instância gerenciada pelo cliente. A permissão excluída gerenciada pelo cliente desaparece após duas horas. Até lá, ele permanece visível na Biblioteca de permissões gerenciadas com um status excluído.

Console

Para excluir uma permissão gerenciada pelo cliente

1. Navegue até a Biblioteca de permissões gerenciadas.
2. Filtre a lista de permissões gerenciadas pelo cliente ou pesquise o nome da permissão gerenciada pelo cliente que você deseja excluir.
3. Confirme se há 0 compartilhamentos associados na lista de permissões gerenciadas antes de selecionar a permissão gerenciada pelo cliente.

   Se ainda houver compartilhamentos de recursos associados à permissão gerenciada, você deverá atribuir outra permissão gerenciada a todos os compartilhamentos de recursos antes de continuar.
4. No canto superior direito da página de detalhes da permissão gerenciada pelo cliente, escolha Excluir permissão gerenciada.
5. Quando a caixa de diálogo de confirmação for exibida, escolha Excluir para excluir a permissão gerenciada.

AWS CLI

Para excluir uma permissão gerenciada pelo cliente

1. Encontre o ARN da permissão gerenciada que você deseja excluir chamando list-permissions com o `--permission-type CUSTOMER_MANAGED` parâmetro para incluir somente as permissões gerenciadas pelo 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. Depois de ter o ARN da permissão gerenciada para excluir, forneça-o como um parâmetro para a permissão de exclusão.

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

Atualização de permissões AWS gerenciadas para uma versão mais recente

Ocasionalmente, AWS atualiza as permissões AWS gerenciadas disponíveis para anexar a um compartilhamento de recursos para um tipo específico de recurso. Quando isso AWS acontece, ele cria uma nova versão da permissão AWS gerenciada. Os compartilhamentos de recursos que incluem o tipo de recurso especificado não são atualizados automaticamente para usar a versão mais recente da permissão gerenciada. Você deve atualizar explicitamente a permissão gerenciada para cada compartilhamento de recursos. Essa etapa extra é necessária para que você possa avaliar as alterações antes de aplicá-las aos seus compartilhamentos de recursos.

Console

Sempre que o console exibir uma página que lista as permissões associadas a um compartilhamento de recursos e uma ou mais dessas permissões estiverem usando uma versão diferente da padrão para a permissão, o console exibirá um banner na parte superior da página

do console. O banner indica que seu compartilhamento de recursos está usando uma versão diferente da padrão.

Além disso, as permissões individuais podem exibir um botão Atualizar para a versão padrão ao lado do número da versão atual quando essa versão não for a padrão.

A escolha desse botão inicia o assistente de Atualização de compartilhamento de recursos. Na Etapa 2 do assistente, você pode atualizar a versão de qualquer permissão não padrão para usar suas versões padrão.

As alterações não são salvas até que você conclua o assistente escolhendo Enviar na última página do assistente.

> **Note**
>
> Você pode anexar somente a versão padrão e não pode reverter para outra versão. Para permissões gerenciadas pelo cliente, depois de atualizar as permissões para a versão padrão, você não pode aplicar outra versão a um compartilhamento de recursos, a menos que primeiro defina essa outra versão como padrão. Por exemplo, se você atualizou uma permissão para a versão padrão e encontrou um erro que deseja reverter, poderá designar a versão anterior como padrão. Como alternativa, você pode criar uma nova versão diferente e depois designá-la como padrão. Depois de executar uma dessas opções, você atualizaria seus compartilhamentos de recursos para usar o que agora é a versão padrão.

AWS CLI

Para atualizar a versão de uma permissão AWS gerenciada

1. Execute o comando get-resource-shares com o parâmetro `--permission-arn` para especificar o Nome do recurso da Amazon (ARN) da permissão gerenciada que você deseja atualizar. Isso faz com que o comando retorne somente os compartilhamentos de recursos que usam essa permissão gerenciada.

   Por exemplo, o exemplo de comando a seguir retorna detalhes de cada compartilhamento de recursos que usa a permissão AWS gerenciada padrão para reservas de capacidade do Amazon EC2.

   ```
   $ aws ram get-resource-shares \
   ```

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

A saída inclui o ARN de cada compartilhamento de recursos com pelo menos um recurso cujo acesso é controlado por essa permissão gerenciada.

2. Para cada compartilhamento de recursos especificado no comando anterior, execute o comando associate-resource-share-permission. Inclua o `--resource-share-arn` para especificar o compartilhamento de recursos a ser atualizado, o `--permission-arn` para especificar qual permissão gerenciada da AWS você está atualizando e o parâmetro `--replace` para especificar que você deseja atualizar o compartilhamento para usar a versão mais recente dessa permissão gerenciada. Você não precisa especificar o número da versão; a versão padrão é usada automaticamente.

```
$ 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 o comando na etapa anterior para cada `ResourceShareArn` que você recebeu nos resultados do comando na etapa 1.

Considerações sobre o uso de permissões gerenciadas pelo cliente no AWS RAM

As permissões gerenciadas pelo cliente só estão disponíveis no Região da AWS local em que você as criou. Nem todos os tipos de recursos oferecem suporte às permissões gerenciadas pelo cliente. Para obter uma lista dos tipos de recursos compatíveis em AWS Resource Access Manager, consulteRecursos compartilháveis AWS.

Não há suporte para permissões gerenciadas pelo cliente com várias instruções. Você só pode usar operadores únicos sem negação nas permissões gerenciadas pelo cliente.

As seguintes condições não são suportadas nas permissões gerenciadas pelo cliente:

- Chaves de condição usadas para associar as propriedades da entidade principal:

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

- Chaves de condição usadas para restringir o acesso das entidades principais de serviços:
  - `aws:SourceArn`
  - `aws:SourceAccount`
  - `aws:SourceOrgPaths`
  - `aws:SourceOrgID`
- Tags do sistema:
  - `aws:PrincipalTag/aws:`
  - `aws:ResourceTag/aws:`
  - `aws:RequestTag/aws:`

> **Note**
>
> O valor `aws:SourceAccount` é preenchido automaticamente ao ser compartilhado com as entidades principais de serviços.

Como as permissões gerenciadas funcionam

Para uma visão geral rápida, assista ao vídeo a seguir que demonstra como as permissões gerenciadas permitem que você aplique a melhor prática de acesso com privilégios mínimos aos seus recursos da AWS.

Este vídeo demonstra como criar e associar permissões gerenciadas pelo cliente seguindo as práticas recomendadas de privilégio mínimo. Para obter mais informações, consulte, ???.

Ao criar um compartilhamento de recursos, você associa uma permissão AWS gerenciada a cada tipo de recurso que deseja compartilhar. Se a permissão gerenciada tiver mais de uma versão, o novo compartilhamento de recursos sempre usará a versão designada como padrão.

Depois de criar o compartilhamento de recursos,AWS RAM usa a permissão gerenciada para gerar uma política baseada em recursos que é anexada a cada recurso compartilhado.

O modelo de política em uma permissão gerenciada especifica o seguinte:

Efeito

Indica se `Allow` ou `Deny` a permissão da entidade principal para realizar uma operação em um recurso compartilhado. Para uma permissão gerenciada, o efeito é sempre `Allow`. Para obter mais informações, consulte Efeito no Guia do usuário do IAM.

Ação

A lista de operações que a entidade principal tem permissão para realizar. Isso pode ser uma ação no Console de gerenciamento da AWS ou uma operação na AWS Command Line Interface(AWS CLI) ou na AWS API. As ações são definidas pela permissão da AWS. Para obter mais informações, consulte Ações no Guia do usuário do IAM.

Condição

Quando e como uma entidade principal pode interagir com um recurso em um compartilhamento de recursos. As condições adicionam uma camada extra de segurança aos seus recursos compartilhados. Use-os para limitar o acesso de ações confidenciais aos seus recursos compartilhados. Por exemplo, você pode incluir condições que exijam que as ações tenham origem em um intervalo específico de endereços IP corporativos ou que as ações sejam executadas por usuários autenticados com autenticação multifator. Para obter mais informações sobre as chaves de condição, consulte Chaves de contexto de condição global na AWS no Guia do usuário do IAM. Para obter mais informações sobre condições específicas do serviço, consulte Ações, recursos e chaves de condição para AWS serviços na Referência de Autorização de Serviço.

> **Note**
>
> As condições estão disponíveis para permissões gerenciadas pelo cliente e tipos de recursos compatíveis para permissões gerenciadas da AWS.
> Para obter informações sobre condições que são excluídas do uso com permissões gerenciadas pelo cliente, consulte Considerações sobre o uso de permissões gerenciadas pelo cliente no AWS RAM.

Tipos de permissões gerenciadas

Ao criar um compartilhamento de recursos, você escolhe uma permissão gerenciada para associar a cada tipo de recurso incluído no compartilhamento de recursos.AWS as permissões gerenciadas são definidas pelo serviço AWS proprietário do recurso e gerenciadas por.AWS RAM Você cria e mantém suas próprias permissões gerenciadas pelo cliente.

- AWS permissão gerenciada — Há uma permissão gerenciada padrão disponível para cada tipo de recurso AWS RAM compatível. A permissão gerenciada padrão é aquela usada para um tipo de recurso, a menos que você escolha explicitamente uma das permissões gerenciadas adicionais. A permissão gerenciada padrão tem como objetivo oferecer suporte aos cenários mais comuns de clientes para compartilhar recursos do tipo especificado. A permissão gerenciada padrão permite que as entidades principais executem ações específicas que são definidas pelo serviço para o tipo do recurso. Por exemplo, para o tipo de recurso `ec2:Subnet` da Amazon VPC, a permissão gerenciada padrão permite que as entidades principais realizem as seguintes ações:
  - `ec2:RunInstances`
  - `ec2:CreateNetworkInterface`
  - `ec2:DescribeSubnets`

  Os nomes das permissões AWS gerenciadas padrão usam o seguinte formato:`AWSRAMDefaultPermission`*`ShareableResourceType`*. Por exemplo, para o tipo de `ec2:Subnet` recurso, o nome da permissão AWS gerenciada padrão é`AWSRAMDefaultPermissionSubnet`.

  > **Note**
  >
  > A permissão gerenciada padrão é separada da versão padrão de uma permissão gerenciada. Todas as permissões gerenciadas, sejam elas padrão ou uma das permissões gerenciadas adicionais suportadas por alguns tipos de recursos, são permissões separadas e completas com efeitos e ações diferentes que oferecem suporte a diferentes cenários de compartilhamento, como acesso de leitura e gravação versus acesso somente leitura. Qualquer permissão gerenciada, seja da AWS ou gerenciada pelo cliente, pode ter várias versões, uma das quais é a versão padrão dessa permissão.

  Por exemplo, quando você compartilha um tipo de recurso que oferece suporte a uma permissão gerenciada de acesso total (`Read` e `Write`) e a uma permissão gerenciada somente para

leitura, você pode criar um compartilhamento de recursos para o administrador com a permissão gerenciada de acesso total. Em seguida, você pode criar um compartilhamento de recursos separado para outros desenvolvedores usando a permissão gerenciada somente para leitura para seguir a prática de conceder privilégios mínimos.

> **Note**
>
> Todos os AWS serviços que funcionam com AWS RAM oferecem suporte a pelo menos uma permissão gerenciada padrão. Você pode ver as permissões disponíveis para cada AWS service (Serviço da AWS) na página da Biblioteca de permissões gerenciadas. Esta página fornece detalhes sobre cada permissão gerenciada disponível, incluindo quaisquer compartilhamentos de recursos atualmente associados à permissão e se o compartilhamento com entidades principais externas é permitido, se aplicável. Para obter mais informações, consulte Visualizando permissões gerenciadas.
>
> Para serviços que não oferecem suporte a permissões gerenciadas adicionais, quando você cria um compartilhamento de recursos, aplica AWS RAM automaticamente a permissão padrão definida para o tipo de recurso que você escolher. Se houver suporte, você também terá a opção de escolher Criar permissão gerenciada pelo cliente na página Associar permissões gerenciadas.

- Permissões gerenciadas pelo cliente: permissões gerenciadas pelo cliente são permissões gerenciadas que você cria e mantém especificando com precisão quais ações podem ser executadas sob quais condições com recursos compartilhados usando o AWS RAM. Por exemplo, você quer limitar o acesso de leitura aos seus grupos do Gerenciador de endereços IP (IPAM) da Amazon VPC, que ajudam você a gerenciar seus endereços IP em grande escala. Você pode criar permissões gerenciadas pelo cliente para que seus desenvolvedores atribuam endereços IP, mas não visualizem o intervalo de endereços IP que outras contas de desenvolvedor atribuem. É possível seguir as práticas recomendadas de privilégio mínimo, conceda apenas as permissões necessárias para executar tarefas em recursos compartilhados.

Segurança em AWS Resource Access Manager

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isto como segurança da nuvem e segurança na nuvem.

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao AWS Resource Access Manager (AWS RAM), consulte Serviços da AWS no escopo por programa de conformidade.
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar AWS RAM. Os tópicos a seguir mostram como configurar para atender AWS RAM aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros AWS serviços que ajudam a monitorar e proteger seus AWS RAM recursos.

Tópicos

Proteção de dados em AWS Resource Access Manager

O modelo de responsabilidade AWS compartilhada modelo se aplica à proteção de dados em AWS Resource Access Manager. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para saber mais sobre a privacidade de dados, consulte as Data Privacy FAQ. Para saber mais sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and RGPD no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com AWS os recursos. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como trabalhar com CloudTrail trilhas no Guia AWS CloudTrail do usuário.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sensíveis armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para saber mais sobre os endpoints FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sensíveis, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com AWS RAM ou Serviços da AWS usa o console, a API ou AWS SDKs. AWS CLI Quaisquer dados inseridos em tags ou em campos de texto de formato livre usados

para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

Gerenciamento de identidade e acesso para AWS Resource Access Manager

AWS Identity and Access Management (IAM) é um AWS serviço que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores no IAM controlam quem pode ser autenticado (conectado) e autorizado (com permissões) a usar AWS os recursos. Ao usar o IAM, você cria entidades principais, como funções, usuários e grupos no seu Conta da AWS. Você controla as permissões que esses diretores têm para realizar tarefas usando AWS recursos. Você pode usar o IAM sem custo adicional. Para obter mais informações sobre o gerenciamento e a criação de políticas personalizadas do IAM, consulte Gerenciamento de políticas do IAM no Guia do usuário do IAM.

Tópicos

Como AWS RAM funciona com o IAM

Por padrão, os diretores do IAM não têm permissão para criar ou modificar AWS RAM recursos. Para permitir que as entidades principais do IAM criem ou alterem recursos e realizem tarefas, você deve realizar uma das etapas a seguir. Essas ações concedem permissão para usar recursos e ações de API específicos.

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos em AWS IAM Identity Center:

Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center .

- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criando um perfil para um provedor de identidades de terceiros (federação) no Guia do Usuário do IAM.

- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

AWS RAM fornece várias políticas AWS gerenciadas que você pode usar para atender às necessidades de muitos usuários. Para saber mais sobre essas ferramentas, consulte AWS políticas gerenciadas para AWS Resource Access Manager.

Se precisar de um controle mais preciso sobre as permissões concedidas aos seus usuários, você pode criar suas próprias políticas no console do IAM. Para obter informações sobre como criar políticas e anexá-las aos usuários e perfis do IAM, consulte Políticas e permissões no IAM no Guia do usuário do AWS Identity and Access Management .

As seções a seguir fornecem os detalhes AWS RAM específicos para criar uma política de permissão do IAM.

Sumário

Estrutura da política

Uma política de permissão do IAM é um documento JSON que inclui as seguintes declarações: Efeito, Ação, Recurso e Condição. Uma política do IAM geralmente tem o seguinte formato.

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

Efeito

A declaração Efeito indica se a política permite ou nega uma permissão de entidade principal para realizar uma ação. Os valores possíveis incluem `Allow` e `Deny`.

Ação

A declaração Action especifica as ações da AWS RAM API para as quais a política está permitindo ou negando permissão. Para ver uma lista completa da ações permitidas, veja Ações definidas pelo AWS Resource Access Manager no Guia do usuário do IAM.

Recurso

A declaração de recursos especifica os AWS RAM recursos que são afetados pela política. Para especificar um recurso na declaração, você precisa usar o nome do recurso da Amazon (ARN). Para obter uma lista completa dos recursos permitidos, consulte Recursos definidos pelo AWS Resource Access Manager no Guia do usuário do IAM.

Condição

As declarações de Condição são opcionais. Eles podem ser usados para refinar ainda mais as condições sob as quais a política se aplica. AWS RAM suporta as seguintes chaves de condição:

- `aws:RequestTag/${TagKey}`: testa se a solicitação de serviço inclui uma tag com a chave de tag especificada, existe e tem o valor especificado.
- `aws:ResourceTag/${TagKey}`: testa se o recurso acionado pela solicitação de serviço tem uma tag anexada com uma chave de tag especificada na política.

  O exemplo de condição a seguir verifica se o recurso referenciado na solicitação de serviço tem uma tag anexada com o nome da chave “Proprietário” e um valor de “Equipe de desenvolvimento”.

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

- `aws:TagKeys`: especifica as chaves de tags que devem ser usadas ao criar ou marcar um compartilhamento de recursos.
- `ram:AllowsExternalPrincipals`: testa se o compartilhamento de recursos na solicitação de serviço permite o compartilhamento com entidades principais externas. Um diretor externo é uma Conta da AWS pessoa externa à sua organização em AWS Organizations. Se chegar a `False`, você poderá compartilhar esse compartilhamento de recursos com contas somente na mesma organização.
- `ram:PermissionArn`: testa se o ARN da permissão especificado na solicitação de serviço corresponde a uma string de ARN especificada na política.
- `ram:PermissionResourceType`: testa se a permissão especificada na solicitação de serviço é válida para o tipo de recurso especificado na política. Especifique os tipos de recursos usando o formato mostrado na lista de tipos de recursos compartilháveis.
- `ram:Principal`: testa se o ARN da entidade principal especificado na solicitação de serviço corresponde a uma string de ARN especificada na política.
- `ram:RequestedAllowsExternalPrincipals`: testa se a solicitação de serviço inclui o parâmetro `allowExternalPrincipals` e se seu argumento corresponde ao valor especificado na política.
- `ram:RequestedResourceType`: testa se o tipo de recurso do recurso que está sendo usado corresponde a uma string de tipo de recurso que você especifica na política. Especifique os tipos de recursos usando o formato mostrado na lista de tipos de recursos compartilháveis.
- `ram:ResourceArn`: testa se o ARN do recurso que está sendo processado pela solicitação de serviço corresponde a um ARN especificado na política.

- `ram:ResourceShareName`: testa se o nome do compartilhamento de recursos que está sendo processado pela solicitação de serviço corresponde a uma string especificada na política.
- `ram:ShareOwnerAccountId`: testa se o número de ID da conta do compartilhamento de recursos que está sendo processado pela solicitação de serviço corresponde a uma string especificada na política.

AWS políticas gerenciadas para AWS Resource Access Manager

AWS Resource Access Manager atualmente fornece várias políticas AWS RAM gerenciadas, que são descritas neste tópico.

AWS políticas gerenciadas

- AWS política gerenciada: AWSResource AccessManagerReadOnlyAccess
- AWS política gerenciada: AWSResource AccessManagerFullAccess
- AWS política gerenciada: AWSResource AccessManagerResourceShareParticipantAccess
- AWS política gerenciada: AWSResource AccessManagerServiceRolePolicy
- AWS RAM atualizações nas políticas AWS gerenciadas

Na lista anterior, você pode anexar as três primeiras políticas às suas funções, grupos e usuários do IAM para conceder permissões. A última política na lista é reservada para a função AWS RAM vinculada ao serviço.

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo as políticas gerenciadas pelo cliente que são específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) for lançada ou novas operações de API forem disponibilizadas para serviços existentes.

Para saber mais, consulte AWS Políticas gerenciadas pela no Guia do usuário do IAM.

AWS política gerenciada: AWSResource AccessManagerReadOnlyAccess

É possível anexar a política `AWSResourceAccessManagerReadOnlyAccess` às suas identidades do IAM.

Essa política fornece permissões somente de leitura para os compartilhamentos de recursos que pertencem a sua Conta da AWS.

Ele faz isso concedendo permissão para executar qualquer uma das operações `Get*` ou `List*`. Ele não fornece a capacidade de modificar nenhum compartilhamento de recursos.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `ram`: permite que as entidades principais visualizem detalhes sobre os compartilhamentos de recursos pertencentes à conta.

JSON

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

AWS política gerenciada: AWSResource AccessManagerFullAccess

É possível anexar a política `AWSResourceAccessManagerFullAccess` às suas identidades do IAM.

Essa política fornece acesso administrativo total para visualizar ou modificar os compartilhamentos de recursos que pertencem a sua Conta da AWS.

Ele faz isso concedendo permissão para executar qualquer operação `ram`.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `ram`: permite que as entidades principais visualizem ou modifiquem qualquer informação sobre os compartilhamentos de recursos que são de propriedade da Conta da AWS.

JSON

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

AWS política gerenciada: AWSResource AccessManagerResourceShareParticipantAccess

É possível anexar a política `AWSResourceAccessManagerResourceShareParticipantAccess` às suas identidades do IAM.

Essa política fornece aos diretores a capacidade de aceitar ou rejeitar compartilhamentos de recursos que são compartilhados com ela e de exibir detalhes sobre esses compartilhamentos de recursos. Conta da AWS Ele não fornece nenhuma capacidade de modificar esses compartilhamentos de recursos.

Ele faz isso concedendo permissão para executar algumas operações `ram`.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `ram`: permite que as entidades principais aceitem ou rejeitem convites de compartilhamento de recursos e visualizem detalhes sobre os compartilhamentos de recursos que são compartilhados com a conta.

JSON

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

AWS política gerenciada: AWSResource AccessManagerServiceRolePolicy

A política AWS gerenciada só `AWSResourceAccessManagerServiceRolePolicy` pode ser usada com a função vinculada ao serviço para. AWS RAM Você não pode anexar, desanexar, modificar ou excluir essa política.

Essa política AWS RAM fornece acesso somente para leitura à estrutura da sua organização. Quando você ativa a integração entre AWS RAM e AWS Organizations, cria AWS RAM automaticamente uma função vinculada ao serviço chamada

AWSServiceRoleForResourceAccessManagerque o serviço assume quando precisa pesquisar informações sobre sua organização e suas contas, por exemplo, quando você visualiza a estrutura da organização no console. AWS RAM

Ele faz isso concedendo permissão somente de leitura para executar as operações `organizations:Describe` e `organizations:List` que fornecem detalhes da estrutura e das contas da organização.

Detalhes das permissões

Esta política inclui as seguintes permissões.

- `organizations`: permite que as entidades principais visualizem informações sobre a estrutura da organização, incluindo as unidades organizacionais e as Contas da AWS que elas contêm.

JSON

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

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

AWS RAM atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas AWS RAM desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o feed RSS na página Histórico do AWS RAM documento.

Alteração	Descrição	Data
AWS Resource Access Manager começou a rastrear alterações	AWS RAM documentou suas políticas gerenciadas existentes e começou a monitorar as mudanças.	16 de setembro de 2021

Usando funções vinculadas a serviços para AWS RAM

AWS Resource Access Manager usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente ao AWS RAM serviço. As funções vinculadas ao serviço são predefinidas AWS e incluem todas as permissões AWS RAM necessárias para chamar outros AWS serviços em seu nome.

Uma função vinculada ao serviço AWS RAM facilita a configuração porque você não precisa adicionar manualmente as permissões necessárias. AWS RAM define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, só AWS RAM pode assumir suas funções vinculadas ao serviço. As permissões definidas incluem a política de confiança e a política de permissões, e essa política não pode ser anexada a nenhuma outra entidade do IAM.

Para obter informações sobre outros serviços compatíveis com perfis vinculados a serviços, consulte Serviços da AWS compatíveis com o IAM e procure os serviços que contenham Sim na coluna Service-Linked Role. Escolha um Sim com um link para visualizar a documentação do perfil vinculado para esse serviço.

Permissões de função vinculadas ao serviço para AWS RAM

AWS RAM usa a função vinculada ao serviço nomeada `AWSServiceRoleForResourceAccessManager` quando você ativa o compartilhamento com. AWS Organizations Essa função concede permissões ao AWS RAM serviço para visualizar os detalhes da organização, como a lista de contas dos membros e em quais unidades organizacionais cada conta está.

Essa função vinculada ao serviço confia no seguinte serviço para assumir a função:

- `ram.amazonaws.com`

A política de permissões de função nomeada AWSResource AccessManagerServiceRolePolicy é anexada a essa função vinculada ao serviço e permite AWS RAM concluir as seguintes ações nos recursos especificados:

- Ações: ações somente para leitura que recuperam detalhes sobre a estrutura da sua organização. Para ver a lista completa de ações, você pode ver a política no console do IAM: AWSResourceAccessManagerServiceRolePolicy.

Para que um diretor ative o AWS RAM compartilhamento em sua organização, esse diretor (uma entidade do IAM, como um usuário, grupo ou função) precisa ter permissão para criar um papel vinculado ao serviço. Para saber mais, consulte Permissões de Função Vinculadas ao Serviço no Guia do Usuário do IAM.

Criando uma função vinculada ao serviço para AWS RAM

Não é necessário criar manualmente um perfil vinculado ao serviço. Quando você ativa o AWS RAM compartilhamento em sua organização ou executa o Console de gerenciamento da AWSEnableSharingWithAwsOrganizationem sua conta usando o AWS CLI ou uma AWS API, AWS RAM cria a função vinculada ao serviço para você.

Chame `enable-sharing-with-aws-organizations` para criar a função vinculada a serviço na sua conta.

Se você excluir essa função vinculada ao serviço, AWS RAM não terá mais permissões para visualizar os detalhes da estrutura da sua organização.

Editando uma função vinculada ao serviço para AWS RAM

AWS RAM não permite que você edite a função AWSResource AccessManagerServiceRolePolicy vinculada ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para saber mais, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluindo uma função vinculada ao serviço para AWS RAM

Você pode usar o console do IAM AWS CLI ou a AWS API para excluir manualmente a função vinculada ao serviço.

Como excluir manualmente o perfil vinculado ao serviço usando o IAM

Use o console do IAM AWS CLI, o ou a AWS API para excluir a função `AWSResourceAccessManagerServiceRolePolicy` vinculada ao serviço. Para saber mais, consulte Excluir um perfil vinculado ao serviço no Guia do usuário do IAM.

Regiões suportadas para funções vinculadas a AWS RAM serviços

AWS RAM suporta o uso de funções vinculadas ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte Regiões e endpoints do AWS no Referência geral da Amazon Web Services.

Exemplo de políticas do IAM para AWS RAM

Este tópico inclui exemplos de políticas do IAM AWS RAM que demonstram o compartilhamento de recursos e tipos de recursos específicos e a restrição do compartilhamento.

Exemplos de política de IAM

- Exemplo 1: Permitir o compartilhamento de recursos específicos
- Exemplo 2: permitir o compartilhamento de tipos de recursos específicos
- Exemplo 3: Restringir o compartilhamento com pessoas externas Contas da AWS

Exemplo 1: Permitir o compartilhamento de recursos específicos

Você pode usar uma política de permissão do IAM para restringir as entidades principais a associarem apenas recursos específicos a compartilhamentos de recursos.

Por exemplo, a política a seguir limita as entidades principais a compartilhar somente a regra do resolvedor com o nome do recurso da Amazon (ARN) especificado. O operador `StringEqualsIfExists` permite uma solicitação se a solicitação não incluir um parâmetro `ResourceArn` ou se incluir esse parâmetro, que seu valor corresponda exatamente ao ARN especificado.

Para obter mais informações sobre quando e por que usar `...IfExists` operadores, consulte... IfExists operadores de condição no Guia do usuário do IAM.

JSON

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

Exemplo 2: permitir o compartilhamento de tipos de recursos específicos

É possível usar uma política do IAM para limitar as entidades principais a associar somente tipos de recursos específicos ao compartilhamento de recursos.

As ações, `AssociateResourceShare` e `CreateResourceShare`, podem aceitar entidades principais e `resourceArns` como parâmetros de entrada independentes. Portanto, AWS RAM autoriza cada principal e recurso de forma independente, para que possa haver vários contextos de solicitação. Isso significa que, quando uma entidade principal está sendo associada a um compartilhamento de recursos do AWS RAM , a chave de condição `ram:RequestedResourceType` não está presente no contexto da solicitação. Da mesma maneira, quando um recurso está sendo associado a um compartilhamento de recursos do AWS RAM , a chave de condição `ram:Principal` não está presente no contexto da solicitação. Portanto, para

permitir `AssociateResourceShare` e `CreateResourceShare` ao associar os principais ao compartilhamento de AWS RAM recursos, você pode usar o operador de `Null`condição.

Por exemplo, a política a seguir limita as entidades principais a compartilhar somente regras do resolvedor do Amazon Route 53 e permite que elas associem qualquer entidade principal a esse compartilhamento.

JSON

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

Exemplo 3: Restringir o compartilhamento com pessoas externas Contas da AWS

Você pode usar uma política do IAM para impedir que os diretores compartilhem recursos com pessoas Contas da AWS que estão fora da AWS organização.

Por exemplo, a política do IAM a seguir impede que os principais adicionem compartilhamentos externos Contas da AWS aos recursos.

JSON

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

Exemplos de políticas de controle de serviços para AWS Organizations e AWS RAM

AWS RAM suporta políticas de controle de serviço (SCPs). SCPs são políticas que você anexa a elementos em uma organização para gerenciar permissões dentro dessa organização. Um SCP se aplica a tudo Contas da AWS sob o elemento ao qual você anexa o SCP. SCPs ofereça controle central sobre o máximo de permissões disponíveis para todas as contas em sua organização. Eles podem ajudar você a garantir sua Contas da AWS permanência dentro das diretrizes de controle de acesso da sua organização. Para obter mais informações, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations .

Pré-requisitos

Para usar SCPs, você deve primeiro fazer o seguinte:

- Ativar todos os recursos em sua organização. Para obter mais informações, consulte Habilitar todos os recursos na sua organização no Guia do usuário do AWS Organizations .
- Habilite SCPs para uso em sua organização. Para obter mais informações, consulte Habilitar e desabilitar tipos de política no Guia do usuário do AWS Organizations .

- Crie o SCPs que você precisa. Para obter mais informações sobre criação SCPs, consulte Criação e atualização SCPs no Guia AWS Organizations do usuário.

Políticas de controle de serviço de exemplo

Sumário

Os exemplos a seguir mostram como você pode controlar vários aspectos do compartilhamento de recursos em uma organização.

Exemplo 1: impedir compartilhamento externo

O exemplo a seguir, a SCP impede que os usuários criem compartilhamentos de recursos que permitem o compartilhamento com entidades principais que não fazem parte da organização.

AWS RAM autoriza APIs separadamente para cada diretor e recurso listados na chamada.

JSON

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

```
                "Bool": {
                    "ram:RequestedAllowsExternalPrincipals": "true"
                }
            }
        }
    ]
}
```

Exemplo 2: impedir que os usuários aceitem convites de compartilhamento de recursos de contas externas fora da sua organização

O SCP a seguir impede que qualquer entidade principal em uma conta afetada aceite um convite para usar um compartilhamento de recursos. Os compartilhamentos de recursos que são compartilhados com outras contas na mesma organização da conta de compartilhamento não geram convites e, portanto, não são afetados por esse SCP.

JSON

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

Exemplo 3: permitir que contas específicas compartilhem apenas tipos de recursos especificados

O SCP a seguir permite que apenas contas `111111111111` e a `222222222222` criem novos compartilhamentos de recursos que compartilham listas de prefixos do Amazon EC2 ou associa listas de prefixos a compartilhamentos de recursos existentes.

AWS RAM autoriza APIs separadamente para cada diretor e recurso listados na chamada.

O operador `StringEqualsIfExists` permitirá uma solicitação se a solicitação não incluir um parâmetro de tipo de recurso ou se incluir esse parâmetro, que seu valor corresponda exatamente

ao tipo de recurso especificado. Se estiver incluindo uma entidade principal, você deverá ter `...IfExists`.

Para obter mais informações sobre quando e por que usar `...IfExists` operadores, consulte... IfExists operadores de condição no Guia do usuário do IAM.

JSON

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

Exemplo 4: evitar o compartilhamento com toda a organização ou com unidades organizacionais

A SCP a seguir impede que os usuários criem compartilhamentos de recursos que compartilhem recursos com uma organização inteira ou com qualquer unidade organizacional. Os usuários podem compartilhar com indivíduos Contas da AWS na organização ou com funções ou usuários do IAM.

AWS RAM autoriza APIs separadamente para cada diretor e recurso listados na chamada.

JSON

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

Exemplo 5: permitir o compartilhamento somente com entidades principais

O exemplo a seguir, a SCP permite que os usuários compartilhem recursos apenas com a unidade organizacional `o-12345abcdef`, da organização `ou-98765fedcba`, e Conta da AWS `111111111111`.

Se você estiver usando um elemento `"Effect": "Deny"` com um operador de condição negada como `StringNotEqualsIfExists`, a solicitação ainda será negada mesmo se a chave de condição estiver ausente. Use um operador de condição `Null` para verificar se uma chave de condição não está presente no momento da autorização.

AWS RAM autoriza APIs separadamente para cada diretor e recurso listados na chamada.

JSON

```
{
```

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

Exemplo 6: Evitar compartilhamentos de recursos com RetainSharingOnAccountLeaveOrganization ativado

O SCP a seguir impede que os usuários criem ou modifiquem compartilhamentos de recursos quando a chave de `ram:RetainSharingOnAccountLeaveOrganization` condição está definida como. `true`

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

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

Desativando o compartilhamento de recursos com AWS Organizations

Se você ativou anteriormente o compartilhamento com AWS Organizations e não precisa mais compartilhar recursos com toda a sua organização ou unidades organizacionais (OUs), você pode desativar o compartilhamento. Quando você desativa o compartilhamento com AWS Organizations, todas as organizações ou OUs são removidas dos compartilhamentos de recursos que você criou e elas perdem o acesso aos recursos compartilhados. As contas externas (contas adicionadas ao compartilhamento de recursos por meio de convite) não serão afetadas e continuarão associadas ao compartilhamento de recursos.

Para desativar o compartilhamento com AWS Organizations

1. Desative o acesso confiável ao AWS Organizations uso do AWS Organizations [disable-aws-service-access](#) AWS CLI comando.

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

   > **Important**
   >
   > Quando você desativa o acesso confiável a AWS Organizations, os diretores de suas organizações são removidos de todos os compartilhamentos de recursos e perdem o acesso a esses recursos compartilhados.

2. Use o console do IAM AWS CLI, o ou as operações da API do IAM para excluir a função AWSServiceRoleForResourceAccessManagervinculada ao serviço. Para saber mais, consulte [Excluir um perfil vinculado ao serviço](#) no Guia do usuário do IAM.

Registrar em log e monitorar no AWS RAM

O monitoramento é uma parte importante da manutenção da confiabilidade, da disponibilidade e do desempenho do AWS RAM e de soluções da AWS. Você deve coletar dados de monitoramento de todas as partes de sua solução da AWS para depurar uma falha em vários pontos com facilidade, caso ocorra. A AWS fornece várias ferramentas para monitorar seus recursos do AWS RAM e responder a incidentes em potencial:

Amazon EventBridge

Fornece um fluxo quase em tempo real de eventos do sistema que descrevem alterações nos recursos da AWS. O EventBridge habilita a computação orientada a eventos automatizada, já que é possível escrever regras que monitoram determinados eventos e acionam ações automatizadas em outros serviços da AWS quando esses eventos ocorrem. Para obter mais informações, consulte Monitoramento AWS RAM usando EventBridge.

AWS CloudTrail

Captura chamadas de API e eventos relacionados feitos por você ou em sua Conta da AWS e entrega os arquivos de log a um bucket do Amazon S3 especificado por você. É possível identificar quais usuários e contas chamaram a AWS, o endereço IP de origem do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte Registrando chamadas de AWS RAM API com AWS CloudTrail.

Monitoramento AWS RAM usando EventBridge

Usando a Amazon EventBridge, você pode configurar notificações automáticas para eventos específicos em AWS RAM. Os eventos de AWS RAM são entregues quase EventBridge em tempo real. Você pode configurar EventBridge para monitorar eventos e invocar alvos em resposta a eventos que indicam alterações em seus compartilhamentos de recursos. As alterações em um compartilhamento de recursos acionam eventos tanto para o proprietário do compartilhamento de recursos quanto para as entidades principais que receberam acesso ao compartilhamento de recursos.

Quando você cria um padrão de eventos, a origem é `aws.ram`.

> **Note**
>
> Tome cuidado ao escrever códigos que dependam desses eventos. Esses eventos não são garantidos, mas são emitidos com base no melhor esforço. Se ocorrer um erro ao AWS RAM tentar emitir um evento, o serviço tentará várias vezes mais. No entanto, isso pode expirar e resultar na perda desse evento específico.

Para obter mais informações, consulte o Guia EventBridge do usuário da Amazon.

Exemplo: alertas sobre falhas no compartilhamento de recursos

Considere o cenário em que você deseja compartilhar as reservas de capacidade do Amazon EC2 com outras contas em sua organização. Fazer isso é uma boa maneira de reduzir seus custos.

No entanto, se você não atender a todos os pré-requisitos para compartilhar uma reserva de capacidade, ela poderá falhar silenciosamente na execução das tarefas assíncronas envolvidas no compartilhamento de recursos. Se a operação de compartilhamento falhar e seus usuários em outras contas tentarem iniciar instâncias com uma dessas reservas de capacidade, o Amazon EC2 agirá como se a reserva de capacidade estivesse cheia e, em vez disso, iniciará a instância como uma instância sob demanda. Isso pode resultar em custos maiores do que o esperado.

Para monitorar falhas no compartilhamento de recursos, configure uma EventBridge regra da Amazon que alerte você sempre que um compartilhamento AWS RAM de recursos falhar. O procedimento tutorial a seguir usa um tópico do Amazon Simple Notification Service (SNS) para notificar todos os assinantes do tópico sempre que EventBridge descobrir uma falha no compartilhamento de recursos. Para obter mais informações sobre tópicos do Amazon SNS, consulte o Guia do desenvolvedor do Amazon Simple Notification Service.

Para criar uma regra que notifique você quando o compartilhamento de recursos falhar

1. Abra o EventBridge console da Amazon.
2. No painel de navegação, escolha Regras e, na lista Regras, escolha Criar regra.
3. Insira um nome e uma descrição opcional para a sua regra, e escolha Próximo.
4. Role para baixo até a caixa Padrão de evento e escolha Padrões personalizados (editor JSON).
5. Veja a seguir um exemplo de padrão de evento para copiar e colar:

```
{
```

```
  "source": ["aws.ram"],
  "detail-type": ["Resource Sharing State Change"],
  "detail": {
    "event": ["Resource Share Association"],
    "status": ["failed"]
  }
}
```

6. Escolha Próximo.
7. Para Alvo 1, em Tipo de alvo, escolha AWS service (Serviço da AWS).
8. Em Selecionar um destino, escolha Tópico do SNS.
9. Em Tópico, selecione o tópico do SNS no qual você deseja publicar a notificação. O tópico já deve existir.
10. Escolha Próximo e, em seguida, escolha Próximo novamente para verificar sua configuração.
11. Quando estiver satisfeito com suas opções, selecione Criar regra.
12. De volta à página Regras, verifique se sua nova regra está marcada como Ativada. Se necessário, selecione o botão de opção ao lado do nome de sua regra e selecione Habilitar.

Desde que essa regra esteja habilitada, qualquer compartilhamento de AWS RAM recursos que falhe gera um alerta de SNS para os destinatários do tópico no qual você publicou.

Você também pode confirmar que as reservas de capacidade compartilhada estão acessíveis às contas com as quais você as compartilhou, tentando visualizá-las no console do Amazon EC2 a partir dessas contas.

Registrando chamadas de AWS RAM API com AWS CloudTrail

AWS RAM é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço em AWS RAM. CloudTrail captura todas as chamadas de API AWS RAM como eventos. As chamadas capturadas incluem chamadas do AWS RAM console e chamadas de código para as operações AWS RAM da API. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3 que você especificar, incluindo eventos para. AWS RAM Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Use as informações coletadas por CloudTrail para determinar a solicitação que foi feita AWS RAM, o endereço IP solicitante, o solicitante, quando ela foi feita e detalhes adicionais.

Para obter mais informações sobre CloudTrail, consulte o Guia AWS CloudTrail do usuário.

AWS RAM informações em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre em AWS RAM, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS de serviço no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para obter um registro contínuo de eventos na sua Conta da AWS, incluindo eventos para o AWS RAM, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, a trilha se aplica a todas as AWS regiões. A trilha registra eventos de todas as regiões na partição da AWS e entrega os arquivos de log no bucket do Amazon S3 que você especifica. Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para saber mais, consulte:

- Criando uma trilha para o seu Conta da AWS
- AWS service (Serviço da AWS) integrações com registros CloudTrail
- Configurando notificações do Amazon SNS para CloudTrail
- Recebendo arquivos de CloudTrail log de várias regiões e Recebendo arquivos de CloudTrail log de várias contas

Todas AWS RAM as ações são registradas CloudTrail e documentadas na Referência da AWS RAM API. Por exemplo, as chamadas para as ações `CreateResourceShare`, `AssociateResourceShare` e `EnableSharingWithAwsOrganization` geram entradas nos arquivos de log do CloudTrail.

Cada evento ou entrada de log contém informações que ajudam a determinar quem realizou a solicitação.

- Conta da AWS credenciais raiz
- Credenciais de segurança temporárias de uma função AWS Identity and Access Management (IAM) ou usuário federado.
- Credenciais de segurança de longo prazo de um usuário do IAM.
- Outro AWS serviço.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

Entendendo as entradas do arquivo de AWS RAM log

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

O exemplo a seguir mostra uma entrada de CloudTrail registro para a `CreateResourceShare` ação.

```
{
    "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"
}
```

Validação de conformidade para AWS Resource Access Manager

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. Para obter mais informações sobre sua responsabilidade de conformidade ao usar Serviços da AWS, consulte a documentação AWS de segurança.

Resiliência em AWS Resource Access Manager

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que executam o failover automaticamente entre as zonas de disponibilidade sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura AWS global.

Segurança da infraestrutura em AWS Resource Access Manager

Como serviço gerenciado, AWS Resource Access Manager é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a

infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar AWS RAM pela rede. Os clientes devem oferecer compatibilidade com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Acesso AWS Resource Access Manager usando um endpoint de interface ()AWS PrivateLink

Você pode usar AWS PrivateLink para criar uma conexão privada entre sua VPC e. AWS Resource Access Manager Você pode acessar AWS RAM como se estivesse em sua VPC, sem o uso de um gateway de internet, dispositivo NAT, conexão VPN ou conexão. Direct Connect As instâncias na sua VPC não precisam de endereços IP públicos para acessar o AWS RAM.

Estabeleça essa conectividade privada criando um endpoint de interface, habilitado pelo AWS PrivateLink. Criaremos um endpoint de interface de rede em cada sub-rede que você habilitar para o endpoint de interface. Estas são interfaces de rede gerenciadas pelo solicitante que servem como ponto de entrada para o tráfego destinado ao AWS RAM.

Para saber mais, consulte Acessar os Serviços da AWS pelo AWS PrivateLink no Guia do AWS PrivateLink .

Considerações para AWS RAM

Antes de configurar um endpoint de interface para AWS RAM, consulte Considerações no AWS PrivateLink Guia.

AWS RAM suporta fazer chamadas para todas as suas ações de API por meio do endpoint da interface.

Há suporte para políticas de endpoint de VPC. AWS RAM Por padrão, o acesso total a AWS RAM é permitido por meio do endpoint da interface.

Crie um endpoint de interface para AWS RAM

Você pode criar um endpoint de interface para AWS RAM usar o console Amazon VPC ou AWS Command Line Interface o AWS CLI(). Para obter mais informações, consulte Criar um endpoint de interface no Guia do usuário do AWS PrivateLink .

Crie um endpoint de interface para AWS RAM usar o seguinte nome de serviço:

```
com.amazonaws.region.ram
```

Se você habilitar o DNS privado para o endpoint da interface, poderá fazer solicitações de API a AWS RAM usando seu nome DNS regional padrão. Por exemplo, `.ram.us-east-1.amazonaws.com`

Crie uma política de endpoint para seu endpoint de interface.

Uma política de endpoint é um recurso do IAM que pode ser anexado ao endpoint de interface. A política de endpoint padrão permite acesso total AWS RAM por meio do endpoint da interface. Para controlar o acesso AWS RAM permitido pela sua VPC, anexe uma política de endpoint personalizada ao endpoint da interface.

Uma política de endpoint especifica as seguintes informações:

- As entidades principais que podem realizar ações (Contas da AWS, usuários do IAM e perfis do IAM).
- As ações que podem ser realizadas.
- Os recursos nos quais as ações podem ser executadas.

Para obter mais informações, consulte Controlar o acesso aos serviços usando políticas de endpoint no Guia do AWS PrivateLink .

Exemplo: política de VPC endpoint para ações AWS RAM

Veja a seguir um exemplo de uma política de endpoint personalizado. Quando você anexa essa política ao seu endpoint de interface, ela concede acesso às AWS RAM ações listadas para todos os diretores em todos os recursos.

JSON

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

Solução de problemas com AWS RAM

Use as informações desta seção do guia para ajudá-lo a diagnosticar e corrigir problemas comuns ao trabalhar com AWS Resource Access Manager (AWS RAM).

Tópicos

Erro: “O ID da sua conta não existe em uma AWS organização”

Cenário

Você recebe o erro "Seu ID de conta não existe em uma AWS organização" ao tentar compartilhar um recurso com contas ou unidades organizacionais (OUs) em sua organização.

Causa

Esse erro pode ocorrer se a função vinculada ao serviço AWSServiceRoleForResourceAccessManagernão for criada com êxito quando você ativar a integração entre e. AWS Resource Access Manager AWS Organizations

Solução

Para recriar o perfil vinculado ao serviço necessário, execute as etapas a seguir para desativar a integração e ativá-la novamente.

> **Important**
>
> Quando você desativa o acesso confiável a AWS Organizations, os diretores da sua organização são removidos de todos os compartilhamentos de recursos e perdem o acesso a esses recursos compartilhados.

1. Faça login na conta de gerenciamento da sua organização usando um perfil do IAM ou um usuário com permissões administrativas.
2. Navegue até a página Serviços no AWS Organizations console.
3. Escolha IAM.
4. Escolha Desabilitar acesso confiável.
5. Navegue até a página Configurações no AWS RAM console.
6. Selecione a caixa Habilitar compartilhamento com e AWS Organizations, em seguida, escolha Salvar configurações.

Agora você deve poder usar AWS RAM para compartilhar seus recursos com contas e OUs na organização.

Erro: "AccessDeniedException”

Cenário

Você recebe uma exceção de Acesso Negado ao tentar compartilhar um recurso ou visualizar um compartilhamento de recursos.

Causa

Você pode receber esse erro se tentar criar um compartilhamento de recursos sem ter as permissões necessárias. Isso pode ser causado por permissões insuficientes nas políticas anexadas ao seu diretor AWS Identity and Access Management (IAM). Isso também pode acontecer devido às restrições impostas por uma política de controle de AWS Organizations serviço (SCP) que afeta você Conta da AWS.

Solução

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos em AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center .
- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criando um perfil para um provedor de identidades de terceiros (federação) no Guia do Usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Para resolver o erro, você precisa garantir que as permissões sejam concedidas por declarações `Allow` na política de permissão usada pela entidade principal que faz a solicitação. Além disso, as permissões não devem ser bloqueadas pelas da sua organização SCPs.

Para criar um compartilhamento de recursos, você precisa das duas permissões a seguir:

- `ram:CreateResourceShare`
- `ram:AssociateResourceShare`

Para visualizar um compartilhamento de recursos, você precisa das permissões a seguir:

- `ram:GetResourceShares`

Para anexar permissões a um compartilhamento de recursos, você precisa das permissões a seguir:

- *`resourceOwningService`*`:`*`PutPolicyAction`*

  Isso é um espaço reservado. Você deve substituí-la pela permissão PutPolicy "" (ou equivalente) para o serviço que possui o recurso que você deseja compartilhar. Por exemplo, se você estiver compartilhando uma regra de resolução do Route 53, então a permissão necessária seria: `route53resolver:PutResolverRulePolicy`. Se você quiser permitir a criação de um

compartilhamento de recursos que contenha vários tipos de recursos, deverá incluir a permissão relevante para cada tipo de recurso que você deseja permitir.

O exemplo a seguir mostra a possível aparência dessa política de permissão do IAM.

JSON

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

Erro: "UnknownResourceException”

Cenário

Você recebe um dos erros a seguir:

- “CannotCreateResourceShare: UnknownResourceException: OrganizationalUnit ou *xxxx* - não foi encontrado”
- “CannotUpdateResourceShare: UnknownResourceException: OrganizationalUnit ou *xxxx* - não foi encontrado”.

Causa

Esses erros podem ocorrer se você habilitar a integração entre AWS RAM e AWS Organizations usando o console Organizations ou a API Organizations Enable AWSService Access em vez de usar

o AWS RAM console. Quando você ativa a integração usando o console ou a API do Organizations, o serviço não cria a função `AWSServiceRoleForResourceAccessManager` na sua conta. Essa função é necessária para acessar informações sobre sua organização. Como a função não foi criada, não é AWS RAM possível acessar detalhes sobre as contas ou unidades organizacionais (OUs) em sua organização.

Solução

Para resolver o problema, desative a integração entre AWS RAM AWS Organizations e. Em seguida, ative-o novamente chamando a operação da AWS RAM EnableSharingWithAwsOrganizationAPI ou usando o Console de gerenciamento da AWS para realizar as etapas a seguir.

> **Important**
>
> Quando você desativa o acesso confiável a AWS Organizations, os diretores da sua organização são removidos de todos os compartilhamentos de recursos e perdem o acesso a esses recursos compartilhados.

1. Faça login na conta de gerenciamento da sua organização usando um perfil do IAM ou um usuário com permissões administrativas.
2. Navegue até a página Serviços no AWS Organizations console.
3. Escolha IAM.
4. Escolha Desabilitar acesso confiável.
5. Navegue até a página Configurações no AWS RAM console.
6. Selecione a caixa Habilitar compartilhamento com e AWS Organizations, em seguida, escolha Salvar configurações.

Agora você deve poder usar AWS RAM para compartilhar seus recursos com contas e OUs na organização.

Erros ao tentar compartilhar com contas fora da minha organização

Cenário

Você recebe um dos seguintes erros ao tentar compartilhar recursos com contas que estão fora da sua organização:

- “Você não pode compartilhar o recurso fora da sua organização.”
- “O recurso que você está tentando compartilhar só pode ser compartilhado dentro da sua AWS organização. “
- “InvalidParameterException: O ID da conta principal não está em sua AWS organização. Você não tem permissão para adicionar Contas da AWS externas a um compartilhamento de recursos.“
- “OperationNotPermittedException: O recurso que você está tentando compartilhar só pode ser compartilhado dentro da sua AWS organização. “

Possíveis causas e soluções

Alguns tipos de recursos só podem ser compartilhados com contas na mesma organização

Alguns tipos de recursos não podem ser compartilhados com nenhuma conta que não seja membro dessa organização. Um exemplo do tipo de recurso com essa restrição são as conexões privadas virtuais (VPCs) que fazem parte do Amazon Elastic Compute Cloud (Amazon EC2).

Para verificar se você pode compartilhar um determinado tipo de recurso com contas e entidades principais fora da sua organização, consulte Recursos da AWS compartilháveis.

A função vinculada ao serviço não foi criada com sucesso

Esse problema pode ocorrer se a função vinculada ao serviço `AWSServiceRoleForResourceAccessManager` não tiver sido criada com êxito quando você ativou a integração entre e. AWS RAM AWS Organizations

Se você receber um desses erros ao tentar compartilhar um recurso com uma conta que faz parte da sua organização, execute as etapas a seguir para excluir e recriar a função vinculada ao serviço.

> **Important**
>
> Quando você desativa o acesso confiável a AWS Organizations, os diretores da sua organização são removidos de todos os compartilhamentos de recursos e perdem o acesso a esses recursos compartilhados.

1. Faça login na conta de gerenciamento da sua organização usando um perfil do IAM ou um usuário com permissões administrativas.

2. Navegue até a página Serviços no AWS Organizations console.
3. Escolha IAM.
4. Escolha Desabilitar acesso confiável.
5. Navegue até a página Configurações no AWS RAM console.
6. Selecione a caixa Habilitar compartilhamento com e AWS Organizations, em seguida, escolha Salvar configurações.

Não consigo ver recursos compartilhados na conta de destino

Cenário

Os usuários não conseguem ver os recursos que acreditam serem compartilhados com eles por outras Contas da AWS.

Possíveis causas e soluções

O compartilhamento com AWS Organizations foi ativado usando Organizations em vez de AWS RAM

Se AWS Organizations foi ativado usando Organizations em vez de AWS RAM, o compartilhamento dentro da organização falhará. Para verificar se essa é a causa do problema, navegue até a página Configurações no console do AWS RAM e verifique se a caixa de seleção Habilitar compartilhamento com AWS Organizations está marcada.

- Se a caixa de seleção estiver marcada, essa não é a causa.
- Se a caixa de seleção não estiver marcada, essa pode ser a causa. Não marque a caixa de seleção ainda. Execute as etapas a seguir para corrigir a situação.

> **Important**
>
> Quando você desativa o acesso confiável a AWS Organizations, os diretores da sua organização são removidos de todos os compartilhamentos de recursos e perdem o acesso a esses recursos compartilhados.

1. Faça login na conta de gerenciamento da sua organização usando um perfil do IAM ou um usuário com permissões administrativas.
2. Navegue até a página Serviços no AWS Organizations console.
3. Escolha IAM.
4. Escolha Desabilitar acesso confiável.
5. Navegue até a página Configurações no AWS RAM console.
6. Selecione a caixa Habilitar compartilhamento com e AWS Organizations, em seguida, escolha Salvar configurações.

Talvez seja necessário atualizar o compartilhamento e especificar as contas ou unidades organizacionais dentro da organização com as quais compartilhar.

O compartilhamento de recursos não especifica essa conta como uma entidade principal

Na seção Conta da AWS que criou o compartilhamento de recursos, visualize o compartilhamento de recursos no AWS RAM console. Verifique se a conta que não consegue acessar os recursos está listada como Entidade principal. Se não estiver, atualize o compartilhamento para adicionar a conta como entidade principal.

O perfil ou o usuário na conta não tem as permissões mínimas exigidas

Quando você compartilha um recurso na conta A com outra conta B, os usuários e perfis na conta B não têm acesso automático aos recursos no compartilhamento. O administrador da conta B deve primeiro conceder permissão aos usuários e perfis do IAM na conta B que precisam acessar o recurso. Como exemplo, a política a seguir mostra como você pode conceder acesso somente de leitura a usuários e perfis na conta B para um recurso da conta A. A política especifica o recurso pelo nome do recurso da Amazon (ARN).

JSON

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

```
                "ram:List*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:<service>:us-east-1:<Account-A-ID>:<resource-
id>"
        }
    ]
}
```

O recurso está em uma configuração Região da AWS diferente da configuração atual do console

AWS RAM é um serviço regional. Os recursos existem em uma região específica e Região da AWS, para vê-los, eles Console de gerenciamento da AWS devem ser configurados para visualizar os recursos nessa região.

O Região da AWS que o console está acessando no momento é exibido no canto superior direito do console. Para alterá-lo, escolha o nome da região atual e, no menu suspenso, escolha a região cujos recursos você deseja ver.

Erro: limite excedido

Cenário

Você recebe "Você atingiu o limite do número de recursos que você pode compartilhar" ou ResourceShareLimitExceededException"" ao tentar compartilhar recursos.

Causa

Esses erros ocorrem quando você atinge o número máximo de recursos que você pode compartilhar usando o AWS RAM serviço ou AWS service (Serviço da AWS) aquele que criou o recurso que você está tentando compartilhar. Essa cota (anteriormente conhecida como limite) pode afetar a conta de compartilhamento ou a conta com a qual você está compartilhando o recurso.

Solução

1. Para ver suas cotas, no local em Conta da AWS que você está vendo o erro, navegue até uma das páginas a seguir, dependendo do tipo de cota que você está alcançando:

- A página do AWS RAM do serviço de cotas no console
- A página do AWS service (Serviço da AWS) cujos recursos são afetados pela cota

2. Role para baixo e escolha a cota relevante.
3. Se estiver disponível para essa cota, escolha Solicitar aumento de cota.
4. Insira o novo valor da cota e escolha Solicitar.
5. A solicitação aparece na página Histórico da solicitação de cota, onde você pode verificar o status da solicitação até que ela seja finalizada.

A outra conta na minha organização nunca recebe um convite

Cenário

Quando você compartilha recursos com outra conta na mesma organização gerenciada pelo AWS Organizations, eles não recebem convites.

Causa

Esse será o comportamento esperado se sua conta estiver com o compartilhamento dentro da organização da AWS ativado.

Quando essa opção está ativada e você compartilha com outra conta em sua organização, nenhum convite é enviado e nenhuma aceitação é necessária. Todas as contas da organização que você menciona como entidades principais no compartilhamento de recursos podem começar imediatamente a acessar os recursos no compartilhamento.

Se sua conta não ativou o compartilhamento dentro da AWS organização, quando você compartilha com outras contas, mesmo que elas estejam na mesma AWS organização, elas são tratadas como contas autônomas. Os convites são enviados e devem ser aceitos antes que os usuários possam acessar os recursos nos compartilhamentos.

Você não pode compartilhar uma sub-rede VPC

Cenário

Quando você tenta usar AWS RAM para compartilhar uma sub-rede VPC com outra conta, a operação de compartilhamento é bem-sucedida. No entanto, a conta consumidora aparece `LIMIT EXCEEDED` para esse recurso no AWS RAM console.

Causa

Alguns tipos de recursos individuais têm restrições específicas de serviço separadas das restrições impostas por. AWS RAM Algumas dessas restrições podem impedir efetivamente o compartilhamento, mesmo que você não tenha atingido uma das restrições no AWS RAM. Os limites são um exemplo dessas restrições. A Amazon Virtual Private Cloud (Amazon VPC) limita o número de sub-redes que você pode compartilhar com outra conta individual. Se você tentar compartilhar uma sub-rede com uma conta consumidora que já contém o número máximo de sub-redes, essas contas consumidoras serão exibidas `LIMIT EXCEEDED` no console desse recurso. Para obter mais informações sobre os limites de compartilhamento de VPC, consulte Cotas da Amazon VPC – Compartilhamento de VPC no Guia do usuário do Amazon Virtual Private Cloud.

Para resolver isso, primeiro verifique se há outros compartilhamentos de recursos que possam estar compartilhando o recurso especificado com a conta afetada e remova os compartilhamentos que você talvez não precise mais. Também é possível solicitar um aumento para um limite compatível com ajustes. Use o console do Serviço de Cotas para solicitar um aumento de limite.

> **Note**
>
> AWS RAM não detecta automaticamente alterações no aumento do limite. Você deve associar novamente o recurso ou a entidade principal ao compartilhamento de recursos para que a RAM detecte a alteração.

Cotas de serviço para AWS RAM

Sua Conta da AWS tem os limites a seguir, relativos ao AWS Resource Access Manager (AWS RAM). É possível solicitar o aumento de alguns desses limites. Para solicitar um aumento de limite, entre em contato com o Suporte.

> **Note**
>
> As seguintes definições se aplicam à descrição nas cotas abaixo:
>
> - Recurso: um elemento individual criado por um AWS service (Serviço da AWS) que você deseja compartilhar, como um bucket do Amazon S3 ou uma instância do Amazon EC2. Cada recurso referenciado em um compartilhamento de recursos conta como um em relação a essa cota. Se você compartilhar o mesmo recurso em três compartilhamentos de recursos diferentes, isso aumentará sua contagem dessa cota em três.
> - Compartilhamento de recursos: um contêiner criado pelo AWS RAM que você pode usar para compartilhar recursos. Cada compartilhamento de recursos, independentemente de quantos recursos ele contenha, conta como um em relação à sua cota.
> - Entidade principal compartilhada: um identificador que você associou a um compartilhamento de recursos. Pode ser um usuário ou perfil do AWS Identity and Access Management (IAM), um identificador de Conta da AWS, uma unidade organizacional ou uma organização inteira. Cada entidade principal compartilhada que você faz referência em um compartilhamento de recursos adiciona um ao seu uso de cota. Se você compartilhar com uma organização inteira referenciando seu ID, ela contará como apenas uma nessa cota.
> - Permissão gerenciada pelo cliente: permissões gerenciadas que você cria para lidar com casos de uso específicos usando acesso com privilégios mínimos para gerenciar como seus recursos compartilhados são usados.

Recurso	Limite-padrão
Número máximo de compartilhamentos de recursos por Região da AWS	25.000

Recurso	Limite-padrão
Número máximo de associações de recursos por compartilhamento de recursos	5.000
Número máximo de associações de entidades principais por compartilhamento de recursos	5.000
O número máximo de permissões personali zadas.	1.500
O número máximo de permissões personali zadas.	10
Número máximo de versões por permissão gerenciada pelo cliente	5
Número máximo de associações de recursos em todos os compartilhamentos de recursos em uma Região da AWS **Note** Cada recurso incluído em um compartil hamento de recursos é contabilizado nesse limite. Se um recurso estiver incluído em 10 compartilhamentos de recursos diferentes, isso conta 10 contra o limite.	25.000

Recurso	Limite-padrão
Número máximo de associações de entidades principais em todos os compartilhamentos de recursos em uma Região da AWS **Note** Cada entidade principal incluída em um compartilhamento de recursos é contabilizada nesse limite. Se uma entidade principal for incluída em 10 compartilhamentos de recursos diferentes, isso conta 10 contra o limite.	25.000
Número máximo de convites pendentes por conta compartilhada • Essa cota se aplica somente ao envio de contas que estão compartilhando com contas que não fazem parte do mesmo AWS Organizations. • Não há cota para limitar quantos convites pendentes uma conta de recebimento pode ter. • Os convites não são usados ao compartil har entre contas que fazem parte do mesmo AWS Organizations e você ativou o compartil hamento de recursos no AWS Organizations.	250

Usar o AWS RAM com um SDK da AWS

Os kits de desenvolvimento de software (software development kits, ou SDKs) AWS estão disponíveis em muitas linguagens de programação populares. Cada SDK fornece uma API, exemplos de código e documentação que ajudam os desenvolvedores a construir aplicações em sua linguagem preferida.

Documentação do SDK	Exemplos de código
AWS SDK para C++	Exemplos de código do AWS SDK para C++
AWS SDK para Go	Exemplos de código do AWS SDK para Go
AWS SDK para Java	Exemplos de código do AWS SDK para Java
AWS SDK para JavaScript	Exemplos de código do AWS SDK para JavaScript
AWS SDK para .NET	AWS SDK para .NET Exemplos de código da
AWS SDK para PHP	AWS SDK para PHP Exemplos de código da
AWS SDK para Python (Boto3)	AWS SDK para Python (Boto3) Exemplos de código da
AWS SDK para Ruby	AWS SDK para Ruby Exemplos de código do

Exemplo de disponibilidade

Você não pode encontrar o que precisa? Solicite um exemplo de código com o link de feedback.

Histórico de documentos do Guia AWS RAM do usuário

A tabela a seguir descreve adições importantes à AWS Resource Access Manager documentação. Também atualizamos a documentação com frequência para abordar os comentários enviados por você.

Para receber notificações sobre essas atualizações, você pode assinar o feed AWS RAM RSS.

Alteração	Descrição	Data
Suporte adicional para compartilhar CloudFront recursos da Amazon	Agora você pode compartilhar Amazon CloudFront VPC Origins com outras pessoas Contas da AWS da sua organização.	6 de outubro de 2025
Adição de suporte para compartilhar recursos do Billing and Cost Management	Agora você pode compartilhar painéis do Billing and Cost Management com Contas da AWS outras pessoas ou com sua organização. AWS RAM	19 de agosto de 2025
Suporte adicional para compartilhar AWS Cloud Map recursos	Agora você pode compartilhar AWS Cloud Map namespaces com outras pessoas Contas da AWS da sua organização.	14 de agosto de 2025
Adição de suporte para compartilhar recursos do Amazon Application Recovery Controller (ARC	Agora você pode compartilhar os planos do Amazon Application Recovery Controller (ARC) com outros Contas da AWS ou com sua organização AWS RAM.	31 de julho de 2025
Suporte adicional para compartilhar Oracle Database@AWS recursos	Agora você pode compartilhar a infraestrutura do Oracle Database@AWS Exadata e as redes ODB com outras	30 de junho de 2025

	pessoas Contas da AWS da sua organização.	
Adição de suporte para compartilhamento de recursos de aprovação multilateral	Agora você pode compartilhar equipes de aprovação de várias partes com outras pessoas Contas da AWS ou dentro da sua organização.	17 de junho de 2025
Suporte adicional para compartilhar recursos de SageMaker IA da Amazon	Agora você pode usar AWS RAM para compartilhar aplicativos Amazon SageMaker AI Partner com outras Contas da AWS pessoas e com sua organização.	6 de junho de 2025
Suporte adicional para compartilhar AWS Network Firewall recursos	Agora você pode usar AWS RAM para compartilhar AWS Network Firewall firewalls com outras pessoas Contas da AWS e com sua organização.	28 de maio de 2025
Suporte adicional para compartilhar AWS Systems Manager recursos	Você pode compartilhar uma política de AWS Systems Manager negação de acesso com outras pessoas Contas da AWS ou com suas organizações. AWS RAM	30 de abril de 2025
Suporte adicional para compartilhar Conexões de código da AWS recursos	Agora você pode compartilhar conexões Conexões de código da AWS de código com outras Contas da AWS pessoas ou dentro da sua organização.	05 de março de 2025

Suporte adicional para compartilhar AWS Billing recursos	Agora você pode compartilhar AWS Billing visualizações com outras pessoas Contas da AWS em sua organização.	20 de dezembro de 2024
Adição de suporte para compartilhar configurações de recursos do Amazon VPC Lattice	Agora você pode compartilhar configurações de recursos do Amazon VPC Lattice com outras Contas da AWS.	1.º de dezembro de 2024
Adição de suporte para compartilhar recursos do Amazon API Gateway	Agora você pode compartilhar nomes de domínio do API Gateway com outras Contas da AWS pessoas ou dentro da sua organização.	21 de novembro de 2024
Adição de suporte para compartilhar recursos da Amazon VPC	Agora você pode compartilhar grupos de segurança da Amazon VPC com outras pessoas Contas da AWS ou dentro da sua organização.	30 de outubro de 2024
Suporte adicional para compartilhar AWS End User Messaging SMS recursos	Você pode compartilhar AWS End User Messaging SMS recursos com outras pessoas Contas da AWS ou com suas organizações AWS RAM.	24 de setembro de 2024
AWS PrivateLink	Com AWS PrivateLink o for AWS RAM, você pode se conectar diretamente à RAM usando um endpoint de interface em sua nuvem privada virtual (VPC).	9 de setembro de 2024

Suporte adicional para compartilhamento AWS Backup	Você pode compartilhar cofres logicamente isolados em sua organização ou dentro dela. Contas da AWS	7 de agosto de 2024
Adição do suporte para compartilhamento de recursos do Elastic Load Balancing	Você pode compartilhar os repositórios fiduciários do Elastic Load Balancing em sua Contas da AWS organização ou dentro dela.	5 de agosto de 2024
Adição de suporte para compartilhar modelos personalizados do Amazon Bedrock	Agora você pode usar AWS RAM para compartilhar modelos personalizados do Amazon Bedrock com outras pessoas Contas da AWS e com sua organização.	1.º de agosto de 2024
Suporte adicional para compartilhar AWS CloudHSM backups	Você pode compartilhar AWS CloudHSM backups com outras pessoas Contas da AWS ou com suas organizaç ões AWS RAM.	28 de junho de 2024
Foi adicionado suporte para compartilhar Model Registry recursos de SageMaker IA da Amazon.	Agora você pode compartil har parâmetros avançados de forma segura e eficiente em Contas da AWS ou na sua organização.	27 de junho de 2024
Suporte adicionado para compartilhar Amazon SageMaker AI JumpStart	Agora você pode compartil har Amazon SageMaker AI JumpStart Hubs com Contas da AWS ou dentro da sua organização.	27 de junho de 2024

Suporte adicional para compartilhamento Amazon Route 53 ResolverProfiles	Agora você pode usar AWS RAM para compartilhar Amazon Route 53 Resolver Profiles com outras pessoas Contas da AWS da sua organização.	22 de abril de 2024
Suporte adicionado para compartilhar recursos do AWS Systems Manager Parameter Store	Agora você pode compartil har parâmetros avançados de forma segura e eficiente em Contas da AWS ou na sua organização.	21 de fevereiro de 2024
Suporte adicionado para compartilhar Amazon FSx for OpenZFS Snapshots	Agora você pode compartil har Amazon FSx for OpenZFS Snapshots com outras pessoas da sua Contas da AWS organização.	19 de dezembro de 2023
Suporte adicionado para compartilhar Amazon Simple Storage Service recursos	Agora você pode compartilhar a instância do Amazon Simple Storage Service Access Grants com outras Contas da AWS pessoas ou com sua organização AWS RAM.	27 de novembro de 2023
Suporte adicionado para compartilhar Explorador de recursos da AWS visualiza ções	Agora você pode compartil har Explorador de recursos da AWS visualizações com outras pessoas Contas da AWS da sua organização.	14 de novembro de 2023

Adição de suporte para compartilhar recursos do Amazon Application Recovery Controller (ARC	Agora você pode compartilhar clusters do Amazon Application Recovery Controller (ARC) com outros Contas da AWS ou com sua organização AWS RAM.	18 de outubro de 2023
Suporte adicional para compartilhar DataZone recursos da Amazon	Agora você pode compartilhar DataZone recursos da Amazon com outras pessoas Contas da AWS ou com sua organização.	4 de outubro de 2023
Suporte adicional para compartilhamento principal de serviços	Agora você pode associar entidades principais de serviço a compartilhamentos de recursos. Isso permite que serviços específicos gerenciem as ações necessárias para os recursos do cliente em seu nome.	29 de agosto de 2023
Suporte adicionado para compartilhar recursos SageMaker do Model Card	Agora você pode compartilhar recursos SageMaker do Model Card com outras pessoas Contas da AWS ou com sua organização.	18 de agosto de 2023
Foi adicionado suporte para grupos de recursos da Amazon SageMaker AI Feature Store e SageMaker AI Catalog como recursos compartilháveis	Agora você pode compartilhar grupos de recursos da Amazon SageMaker AI Feature Store e recursos do SageMaker AI Catalog com outras pessoas Contas da AWS ou com sua organização.	20 de julho de 2023

Aumento do limite da cota de serviço para convites pendentes	O número máximo de convites pendentes por conta de compartilhamento aumentou de 20 para 250.	8 de junho de 2023
Adicionado suporte para AWS AppSync GraphQL APIs como recursos compartilháveis	Agora você pode compartilhar o AWS AppSync GraphQL APIs com outras Contas da AWS pessoas com. AWS RAM	24 de maio de 2023
Foi adicionado suporte para Acesso Verificado pela AWS grupos como recursos compartilháveis	Agora você pode criar e gerenciar Acesso Verificado pela AWS grupos centralmente e depois compartilhá-los com outras pessoas Contas da AWS ou com sua organização.	27 de abril de 2023
Foi adicionado suporte para permissão gerenciada pelo cliente no AWS RAM console	Agora você pode criar e manter com segurança controles de acesso a recursos detalhados para tipos de recursos suportados.	19 de abril de 2023
Suporte adicional para o serviço Amazon VPC Lattice e recursos compartilháveis de rede de serviços	Agora você pode compartilhar o serviço Amazon VPC Lattice e os recursos de rede de serviços com outros. Contas da AWS	31 de março de 2023
Foi adicionado suporte para entidades do AWS Marketplace Catálogo como recursos compartilháveis	Agora você pode compartilhar suas entidades com outras pessoas Contas da AWS no Marketplace.	27 de março de 2023

Foi adicionado suporte para gerenciar versões de permissão no AWS RAM console	Agora você pode usar o AWS RAM console para ver os detalhes da versão e atualizar as permissões para qualquer versão designada como padrão.	16 de janeiro de 2023
Atualização de práticas recomendadas do IAM	Guia atualizado para alinhamento com as práticas recomendadas do IAM. Para saber mais, consulte Práticas recomendadas de segurança no IAM.	3 de janeiro de 2023
Suporte adicionado para grupos de posicionamento do Amazon EC2 como recursos compartilháveis	Agora você pode compartil har grupos de posicionamento do Amazon EC2 com outras pessoas Contas da AWS para iniciar suas instâncias.	8 de novembro de 2022
Links adicionados para dois vídeos introdutórios sobre AWS RAM	Foram adicionados vídeos de visão geral que descrevem AWS RAM e fornecem um passo a passo sobre como compartilhar um recurso com outras pessoas. Contas da AWS	29 de agosto de 2022
Suporte adicional para pipelines de SageMaker IA da Amazon	Agora você pode compartilhar pipelines de SageMaker IA com outros Contas da AWS.	2 de agosto de 2022
Foi adicionado suporte para AWS Service Catalog AppRegistry aplicativos e grupos de atributos como tipos de recursos compartilháveis	Agora você pode compartil har AppRegistry aplicativos e grupos de atributos com outros Contas da AWS.	17 de junho de 2022

AWS Resource Access Manager recebe a certificação SOC e ISO	AWS RAM foi validado como compatível com os padrões Service Organization Control (SOC) e International Organization for Standardization (ISO) ISO 9001, ISO 27001, ISO 27017, ISO 27018 e ISO 27701.	31 de maio de 2022
AWS Resource Access Manager recebe a certificação FedRAMP	AWS RAM foi validado como compatível com o Programa Federal de Gerenciamento de Riscos e Autorizações (FedRAMP).	8 de abril de 2022
AWS Resource Access Manager recebe a certificação PCI DSS	AWS RAM foi validado como compatível com o Padrão de Segurança de Dados (DSS) do Setor de Cartões de Pagamento (PCI).	27 de fevereiro de 2022
Adicionado suporte para descobertas de recursos IPAM da Amazon VPC como recursos compartilháveis. Além disso, agora você pode compartilhar IPAM Pools com contas fora de uma organização	Agora você pode compartilhar descobertas de recursos do IPAM com outras Contas da AWS.	25 de janeiro de 2022
Adicionado suporte para compartilhamento de recursos globais	Agora você pode compartilhar recursos globais com outros Contas da AWS.	2 de dezembro de 2021

Suporte adicional para redes centrais de WAN em AWS nuvem como recursos globais compartilháveis	Agora você pode compartilhar as principais redes do Cloud WAN com outras Contas da AWS.	2 de dezembro de 2021
Suporte para compartil hamento de grupos do Gerenciador de endereços IP (IPAM) da Amazon VPC	Você pode usar AWS RAM para compartilhar os pools IPAM da Amazon VPC. Para obter mais informaçõ es, consulte AWS Recursos compartilháveis no Guia do AWS RAM usuário.	1º de dezembro de 2021
Support para compartilhar recursos de SageMaker IA da Amazon	Você pode usar AWS RAM para compartilhar grupos de linhagem de SageMaker IA. Para obter mais informações, consulte Recursos da AWS compartilháveis no Guia do usuário do AWS RAM .	30 de novembro de 2021
Support para compartilhar recursos do AWS Migration Hub Refactor Spaces	Você pode usar AWS RAM para compartilhar ambientes do Migration Hub. Para obter mais informações, consulte Recursos da AWS compa rtilháveis no Guia do usuário do AWS RAM .	29 de novembro de 2021
Informações adicionad as sobre políticas AWS RAMAWS de permissão do IAM gerenciadas	Detalhes publicados sobre as políticas AWS de permissão gerenciadas disponíveis que você pode acessar no console do IAM e anexar aos diretores do IAM no seu. Conta da AWS	16 de setembro de 2021

Adicionado suporte para compartilhamento de recursos do S3 no Outposts	Agora você pode usar AWS RAM para compartilhar o S3 no Outposts com outros. Contas da AWS	5 de agosto de 2021
Adicionado suporte para permissões gerenciadas adicionais e compartilhamento de recursos com entidades principais do IAM	Para tipos de recursos compatíveis, você pode escolher entre permissõe s AWS RAM gerenciadas adicionais e compartilhar recursos com funções e usuários individuais do IAM.	10 de junho de 2021
Suporte adicional para compartilhar recursos do AWS Systems Manager Incident Manager	Agora você pode usar AWS RAM para compartilhar contatos e planos de resposta do AWS Systems Manager Incident Manager com outros Contas da AWS.	10 de maio de 2021
Adicionado suporte para compartilhar recursos do Amazon Route 53	Agora você pode usar AWS RAM para compartilhar grupos de regras do Amazon Route 53 Resolver DNS Firewall com outros Contas da AWS.	31 de março de 2021
Suporte adicional para compartilhar AWS Transit Gateway recursos	Agora você pode usar AWS RAM para compartilhar domínios multicast do Transit Gateway com outros. Contas da AWS	10 de dezembro de 2020

Suporte adicional para compartilhar AWS Network Firewall recursos	Agora você pode usar AWS RAM para compartilhar políticas de AWS Network Firewall firewall e grupos de regras com outros Contas da AWS.	17 de novembro de 2020
Adicionado suporte para compartilhamento de Outposts e tabelas de rotas de gateway local	Agora você pode usar AWS RAM para compartilhar Outposts e tabelas de rotas de gateway local com outros. Contas da AWS	15 de outubro de 2020
Adicionado suporte para compartilhar logs de consulta do Route 53	Agora você pode usar AWS RAM para compartilhar registros de consulta do Route 53 com outros Contas da AWS.	7 de setembro de 2020
Suporte adicional para compartilhar Autoridade de Certificação Privada da AWS recursos	Agora você pode usar AWS RAM para compartilhar autoridades de certificação CA privada da AWS privadas (CAs) com outras Contas da AWS.	17 de agosto de 2020
Foi adicionado suporte para compartilhar catálogos de dados, bancos de dados e tabelas do AWS Glue	Agora você pode usar AWS RAM para compartilhar catálogos de dados, bancos de dados e tabelas do AWS Glue com outros Contas da AWS.	7 de julho de 2020
Foi adicionado suporte para compartilhar listas de prefixos da Amazon VPC	Agora você pode usar AWS RAM para compartilhar listas de prefixos.	29 de junho de 2020

Suporte adicional para compartilhar endereços de AWS Outposts propriedade do cliente IPv4	Agora você pode usar AWS RAM para compartilhar IPv4 endereços de AWS Outposts propriedade do cliente com outros. Contas da AWS	22 de abril de 2020
Suporte adicionado para compartilhar AWS App Mesh malhas	Agora você pode usar AWS RAM para compartilhar malhas com outros Contas da AWS.	17 de janeiro de 2020
Foi adicionado suporte para compartilhar AWS CodeBuild projetos e grupos de relatórios	Agora você pode usar AWS RAM para compartilhar AWS CodeBuild projetos e grupos de relatórios com outros Contas da AWS.	13 de dezembro de 2019
Adicionado suporte para compartilhamento de recursos adicionais	Agora você pode usar AWS RAM para compartilhar hosts dedicados do Amazon EC2, grupos de AWS Resource Groups recursos e component es, imagens e receitas de imagens do Amazon EC2 Image Builder com outros. Contas da AWS	2 de dezembro de 2019
Adicionado suporte para compartilhamento de reservas de capacidade sob demanda	Agora você pode usar AWS RAM para compartilhar reservas de capacidade sob demanda com outros Contas da AWS.	29 de julho de 2019

Adicionado suporte para compartilhar clusters de banco de dados Aurora	Agora você pode usar AWS RAM para compartilhar clusters de banco de dados Aurora com outros. Contas da AWS	2 de julho de 2019
Adicionado suporte para compartilhar alvos de espelhamento de tráfego	Agora você pode usar AWS RAM para compartilhar alvos de espelhamento de tráfego com outros Contas da AWS.	25 de junho de 2019
Adicionado suporte para compartilhamento de configurações de licença	Agora você pode usar AWS RAM para compartilhar as configurações AWS de licença do License Manager com outros Contas da AWS.	5 de dezembro de 2018
Adicionado suporte para compartilhar sub-redes	Agora você pode usar AWS RAM para compartilhar sub-redes da Amazon VPC com outras. Contas da AWS	27 de novembro de 2018
Adicionado suporte para compartilhar gateways de trânsito	Agora você pode usar AWS RAM para compartilhar gateways de trânsito da Amazon VPC com outros. Contas da AWS	26 de novembro de 2018
Adicionado suporte para compartilhar regras do Resolver	Agora você pode usar AWS RAM para compartilhar as regras do Route 53 Resolver com outros Contas da AWS.	20 de novembro de 2018

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.