Guia do usuário

AWS Resource Access Manager

AWS Resource Access Manager: Guia do usuário

Table of Contents

O que é o AWS Resource Access Manager?

AWS Resource Access Manager (AWS RAM) ajuda você a compartilhar com segurança seus recursos Contas da AWS dentro de sua organização ou unidades organizacionais (OUs) e com AWS Identity and Access Management funções e usuários (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 torná-lo 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 (OUs) especificadas. 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 funções e usuários especificados do IAM.

Índice

Visões gerais do vídeo

O vídeo a seguir fornece uma breve introdução AWS RAM e descreve como criar um compartilhamento de recurso. 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 o 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 detalhes de uso para recursos compartilhados por meio da integração ao AWS RAM com o Amazon CloudWatch e AWS CloudTrail AWS RAM fornece visibilidade abrangente de contas e recursos 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 entidades principais (IAM) (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 uma unidade organizacional (UO) sem precisar enumerar cada uma das Conta da AWS IDs.
- Os usuários podem ver os recursos compartilhados com eles diretamente no AWS service (Serviço da AWS) console 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 de 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 PromoteResourceShareCreatedFromPolicy operação de API.
- Use o equivalente da operação da API, que é o comando AWS Command Line Interface (AWS CLI) promote-resource-share-created-from-policy.

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 às entidades principais da conta consumidora ao recurso compartilhado. Quaisquer políticas e permissões aplicáveis a funções e usuários 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

Com o AWS RAM, você compartilha recursos que possui 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 recurso. 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 no mesmo que Região da AWS 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. As entidades principais podem ser individuais Contas da AWS, as contas em uma organização ou unidade organizacional (OU) em AWS Organizations ou AWS Identity and Access Management funções (IAM) ou usuários individuais.

  > **Note**
  >
  > Nem todos os tipos de recursos podem ser compartilhados com perfis e usuários do IAM. Para obter inform ações 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 funções e usuários 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 pela 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 do local Região da AWS em que ele existe na conta proprietária.
- Se o recurso for global, você poderá acessá-lo de qualquer um Região da AWS que o console de serviço e as ferramentas do recurso suportem. Você pode visualizar esses compartilhamentos 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`.

Como acessar o AWS RAM

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

Console do AWS RAM

O AWS RAM fornece uma interface de usuário na web, o console do AWS RAM. Após se cadastrar em uma conta da Conta da AWS, você poderá acessar o console do AWS RAM fazendo login no AWS Management Console e selecionando o AWS RAM na página inicial do console.

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

AWS CLI e ferramentas para o Windows PowerShell

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

AWS SDKs

A AWS fornece comandos de API para um amplo conjunto de linguagens de programação. Para obter informações sobre os SDKs , consulte o AWS Guia de referência de 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. A API do AWS RAM permite emitir solicitações HTTPS diretamente para o serviço. Quando você usa a API do AWS RAM, deve incluir código para assinar digitalmente solicitações usando suas credenciais. Para obter mais informações, consulte a Referência da API do AWS RAM.

Definição de preços do AWS RAM

Não há encargos adicionais para a criação de AWS RAM e o compartilhamento de 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 de propriedade 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 Payment Card Industry (PCI) Data Security Standard (DSS).

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

FedRAMP

AWS RAM está autorizado como FedRAMP Moderate nas seguintes Regiões da AWS: 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 seguintes Regiões da AWS: AWS GovCloud (EUA-Leste) e AWS GovCloud (Leste dos EUA).

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 AWS ISO e CSA STAR em AWS Artifact.

Para obter mais informações sobre a conformidade do SOC SOC.

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

Conceitos básicos do 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 pessoas 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, ainda será possível compartilhar recursos com contas individuais Contas da AWS na organização. Para tipos de recursos compatíveis, você também pode compartilhar recursos com funções individuais AWS Identity and Access Management (IAM) ou usuários em sua organização. Nesse caso, esses diretores são tratados 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.

Índice

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 com AWS Organizations e os diretores com 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 IAM diretor 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 IAM funções 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 IAM baseadas em identidade anexadas a funções ou usuários individuais pelo IAM administrador na conta consumidora. Essas políticas devem conceder `Allow` acesso às ações especificadas e ao Amazon Resource Name (ARN) de um recurso na conta de compartilhamento.

AWS RAM suporta os seguintes tipos IAM principais 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.
- IAMFunções ou usuários individuais em outra conta — Alguns tipos de recursos oferecem suporte ao compartilhamento direto com IAM funções ou usuários individuais. Especifique esse tipo principal por meio de seuARN.
  - IAMpapel — `arn:aws:iam::123456789012:role/rolename`
  - IAMusuário — `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 pela ARN organização ou pela OU.
  - Todas as contas em uma organização — Veja a seguir um exemplo ARN de uma organização em AWS Organizations:

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

  - Todas as contas em uma unidade organizacional — Veja a seguir um exemplo ARN de 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 "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 recurso

Políticas baseadas em recursos são documentos de JSON texto que implementam a linguagem da IAM política. Ao contrário das políticas baseadas em identidade que você anexa ao principal, como uma IAM função ou usuário, 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 políticas baseadas em recursos no Guia do usuário. IAM

As políticas baseadas em recursos geradas por AWS RAM são avaliadas junto com todos os outros tipos de IAM políticas. Isso inclui todas as políticas IAM baseadas em identidade vinculadas 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 por AWS RAM participam da mesma lógica de avaliação de políticas de todas as outras IAM políticas. Para obter detalhes completos sobre a avaliação de políticas e como determinar as permissões resultantes, consulte Lógica de avaliação de políticas no Guia IAM do usuário.

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 o 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 e nas API operações do serviço proprietário do recurso, 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 CodeBuild API operações 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 deleARN.
- 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 para recursos individuais no console de serviço relevante ou. API
- 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 IAM política JSON baseada. 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. Isso inclui os seguintes tipos de recursos:

- Amazon Aurora: clusters de banco de dados
- Amazon EC2 — reservas de capacidade e anfitriões 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 EC2 recurso de imagem do 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.

```
{
    "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 EC2 recurso de imagem do Image Builder com uma IAMfunção ou usuário em outra Conta da AWS, AWS RAM gera uma política semelhante ao exemplo a seguir e a anexa a qualquer recurso de imagem incluído no compartilhamento de recursos.

```
{
  "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 EC2 recurso de imagem do 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 "Principal": "*" em uma política baseada em recursos.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "imagebuilder:GetImage",
                "imagebuilder:ListImages",
            ],
            "Resource": "arn:aws:imagebuilder:us-east-1:123456789012:image/
testimage/1.0.0/44"
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-123456789"
                }
            }
        }
    ]
}
```

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

Quando você inclui `"Principal": "*"` em uma política baseada em recursos, a política concede acesso a todos os IAM diretores na conta que contém o recurso, sujeita a quaisquer restrições impostas por um `Condition` elemento, 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 um `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 deseja limitar o acesso de leitura aos seus pools do Amazon VPC IP Address Manager (IPAM), 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:

- Habilitar o compartilhamento de recursos no 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 Regiões da AWS local em que foram criados.
- Alguns recursos têm considerações e pré-requisitos especiais para compartilhamento. Para obter mais informações, consulte Recursos compartilháveis AWS.

Habilitar o compartilhamento de recursos no 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.

Se você não precisar mais compartilhar recursos com toda a organização ou OUs desativar 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 você precisar excluir posteriormente 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 de membro ou com IAM funções ou usuários na conta de membro e depois remover essa conta da organização, todos os diretores 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 "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 IAM funções e usuários individuais Contas da AWS ou, para serviços suportados, de fora da sua organização como diretores em um compartilhamento de recursos.

> **Note**
>
> Nem todos os tipos de recursos podem ser compartilhados com IAM funções e usuários. 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 anfitriões 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 de 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 AWS recursos.

   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 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 ter mais informações, consulte Criar uma política 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 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 VPC sub-redes da Amazon. Você também pode compartilhar alguns tipos de recursos compatíveis com IAM funções e usuários.

      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 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 "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 IAM função ou usuário Conta da AWS externo à sua organização. Em vez disso, você deve desativar Exibir estrutura organizacional e usar a lista suspensa e a caixa de texto para inserir a ID ouARN.

- Para especificar um principal por ID ouARN, incluindo diretores que estão fora da organização, selecione o tipo principal para cada diretor. Em seguida, insira a ID (para uma Conta da AWS organização ou OU) ou ARN (para uma IAM função ou usuário) e escolha Adicionar. Os principais tipos, IDs e ARN formatos 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
    ```

  - IAMfunção — Para adicionar uma IAM função, insira ARN a função. Use a seguinte sintaxe:

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

    Por exemplo:

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

> **Note**
>
> Para obter a exclusividade ARN de uma IAM função, visualize a lista de funções no IAM console, use o AWS CLI comando get-role ou a GetRoleAPIação.

- IAMusuário — Para adicionar um IAM usuário, 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 exclusivo ARN para um IAM usuário, visualize a lista de usuários no IAM console, use o get-user AWS CLI comando, ou o GetUserAPIação.

- 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 Compartilhamento AWS de recursos pertencentes a você.

AWS CLI

Criar o compartilhamento de um recurso

Usar a create-resource-sharecomando. 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 a permissão gerenciada ARN para o cliente e, em seguida, crie o compartilhamento de recursos. Para obter mais informações, consulte Criar uma política 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"
    }
}
```

Uso dos recursos AWS 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 no AWS Organizations e o compartilhamento na organização está habilitado, as entidades da organização obtêm acesso automaticamente aos recursos compartilhados e não recebem esses convites.
- Se você compartilhar com o Conta da AWS proprietário do recurso, as entidades 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 página do AWS RAM console.

   > **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 `Pending` status 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 o compartilhamento de recursos para recusar o convite. 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 na `us-west-2` região e mostra que um compartilhamento de recursos está disponível no `PENDING` estado.

```
$ 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 Amazon Resource Name (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 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 operações de API/CLI de cada recurso. Se o recurso for regional, você deverá usar o correto Região da AWS no console de serviço ou 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 AWS

Você pode usar AWS Resource Access Manager (AWS RAM) para compartilhar AWS recursos de sua propriedade e acessar AWS recursos 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 Amazon Resource Name (ARN) para identificar se um recurso é regional ou global. Os recursos regionais mostram o Região da AWS. 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 o AWS Management Console, você escolhe Região da AWS onde deseja criar a instância. Se você usar o AWS Command Line Interface (AWS CLI) para criar a instância, inclua o `--region` parâmetro. Os AWS SDKs 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 especificar uma Região da AWS diferente no console ou em um comando da AWS CLI, você 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 têm ARNs semelhantes ao exemplo a seguir para uma VPC que existe na `us-east-1` região.

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

Recursos globais

Alguns AWS suportam recursos que você pode acessar globalmente, o que significa que você pode usar o recurso de qualquer lugar. Você não especifica uma Região da AWS no console de um serviço global. Para acessar um recurso global, você não especifica um parâmetro de `--region` ao usar as operações do serviço da 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 da 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 Lestedos 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 ambos `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 `us-east-1` Região.

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, use a região que contém os recursos que 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 AWS RAM AWS CLI e 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`.

Compartilhamento AWS de recursos pertencentes a você

Você pode usar AWS Resource Access Manager (AWS RAM) para compartilhar os recursos que você especifica com os 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 você não precisa mais.

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

Visualizar seus compartilhamentos de recursos

1. Abra a página Compartilhado por mim: compartilhamentos de recursos na página do AWS RAM console.
2. Como existem AWS RAM compartilhamentos de recursos específicos Regiões da AWS, escolha o apropriado Região da AWS na lista suspensa no canto superior direito do console. Para ver compartilhamentos de recursos que contêm recursos globais, defina 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 Lista o nome do compartilhamento de recursos, ID, proprietário, Nome de Recurso da Amazon (ARN), data de criação, se ele permite o compartilhamento com contas externas e seu status atual.
   - Permissões gerenciadas Lista 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 Lista 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 Lista as entidades com as quais os recursos são compartilhados.
   - Tags Lista 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 no seu. Conta da AWS

O exemplo a seguir mostra os compartilhamentos de recursos que são compartilhados na chamada Região da AWS (`us-east-1`) atual Conta da AWS. Para criar os compartilhamentos de recursos em uma região diferente, use o `--region` *<region-code>* parâmetro. 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"
        }
    ]
}
```

Criando 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 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 de membro ou com IAM funções ou usuários na conta de membro e depois remover essa conta da organização, todos os diretores 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 "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 IAM funções e usuários individuais Contas da AWS ou, para serviços suportados, de fora da sua organização como diretores em um compartilhamento de recursos.

  Note

  Nem todos os tipos de recursos podem ser compartilhados com IAM funções e usuários. 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 anfitriões 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 de 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 AWS recursos.

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 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 ter mais informações, consulte Criar uma política 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 VPC sub-redes da Amazon. Você também pode compartilhar alguns tipos de recursos compatíveis com IAM funções e usuários.

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 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 "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 comou-), 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 IAM função ou usuário Conta da AWS externo à sua organização. Em vez disso, você deve desativar Exibir estrutura organizacional e usar a lista suspensa e a caixa de texto para inserir a ID ouARN.

- Para especificar um diretor por ID ouARN, incluindo diretores que estão fora da organização, selecione o tipo principal para cada diretor. Em seguida, insira a ID (para uma Conta da AWS organização ou OU) ou ARN (para uma IAM função ou usuário) e escolha Adicionar. Os principais tipos, IDs e ARN formatos 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
    ```

  - IAMfunção — Para adicionar uma IAM função, insira ARN a função. Use a seguinte sintaxe:

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

Por exemplo:

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

> **Note**
>
> Para obter a exclusividade ARN de uma IAM função, visualize a lista de funções no IAM console, use o AWS CLI comando get-role ou a GetRoleAPIação.

- IAMusuário — Para adicionar um IAM usuário, 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 exclusivo ARN para um IAM usuário, visualize a lista de usuários no IAM console, use o get-user AWS CLI comando, ou o GetUserAPIação.

- 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 Compartilhamento AWS de recursos pertencentes a você.

AWS CLI

Criar o compartilhamento de um recurso

Usar a create-resource-sharecomando. 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 a permissão gerenciada ARN para o cliente e, em seguida, crie o compartilhamento de recursos. Para obter mais informações, consulte Criar uma política 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 um compartilhamento de recursos no AWS RAM

Você pode atualizar um compartilhamento de recursos 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 AWS gerenciada 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 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 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 AWS Management Console.

   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 por 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 política 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 AWS gerenciadas, 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 IAM funções Contas da AWS ou usuários individuais que estão fora da sua organização, escolha Permitir compartilhamento com diretores externos.
- Para restringir o compartilhamento de recursos somente aos diretores da sua organização em AWS Organizations, escolha Permitir compartilhamento somente com os diretores da sua organização.

b. Para entidades principais, faça o seguinte:

- (Opcional) Para adicionar uma organização, unidade organizacional (OU) ou membro Conta da AWS 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 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 "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.

> **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 IAM função ou usuário Conta da AWS externo à sua organização. 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 principal na lista suspensa e, em seguida, insira o ID ou ARN para o principal. Por fim, escolha Adicionar.

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

  - Outro Conta da AWS (que não seja o proprietário 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.
  - Isso Conta da AWS (proprietário do recurso) — Todas as funções e usuários 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 ou sua organização repetindo essa etapa. OUs
- (Opcional) Para remover um principal, localize-o em Principais selecionados, marque sua caixa de seleção e escolha Desmarcar.

10. Escolha Próximo.

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 AWS CLI comandos para modificar um compartilhamento de recursos:

- Para renomear um compartilhamento de recursos ou alterar se entidades 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 diretores 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 por 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 as ARNs permissões gerenciadas disponíveis para uma sub-rede Amazon Elastic Compute Cloud (AmazonEC2) e, em seguida, usa uma delas ARNs para substituir a permissão AWS gerenciada 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 EC2 sub-rede da Amazon com o especificado ARN 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.

Visualizar os recursos compartilhados em 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 na página de AWS RAM console.
2. Como os compartilhamentos de AWS RAM recursos existem em um local específico Regiões da AWS, escolha o apropriado Região da AWS na lista suspensa no canto superior direito do console. Para ver compartilhamentos de recursos que contêm recursos globais, Região da AWS defina 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 lista de recursos 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 no 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 `--region` *<region-code>* parâmetro.

```
$ 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"
        }
    ]
}
```

Visualizar as entidades principais com as 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 página do AWS RAM console.
2. Como os compartilhamentos de AWS RAM recursos existem de forma específica Regiões da AWS, escolha o apropriado Região da AWS na lista suspensa no canto superior direito do console. Para ver os compartilhamentos de recursos que contêm recursos globais, Região da AWS defina 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 das entidades 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, as entidades são a organização da conta de chamada 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
        }
```

```
    ]
}
```

Excluir um compartilhamento de recursos em 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

Excluir o compartilhamento de um recurso

1. Abra a página Compartilhado por mim: compartilhamentos de recursos na página do AWS RAM console.
2. Como AWS RAM existem compartilhamentos de recursos específicos Regiões da AWS, escolha o apropriado na lista suspensa Região da AWS no canto superior direito do console. Para ver os compartilhamentos de recursos que contêm recursos globais, defina Região da AWS como Leste dos EUA (Norte da Virgínia), (`us-east-1`). Para obter mais informações sobre o compartilhamento global de recursos, 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 comando delete-resource-share para excluir um compartilhamento de recursos que você não precisa mais.

O exemplo a seguir usa primeiro o comando get-resource-shares para obter o nome do recurso da Amazon (ARN) do compartilhamento de recurso que deseja excluir. Em seguida, ele usa delete-resource-share para 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
}
```

Acesse AWS recursos compartilhados com você

Com AWS Resource Access Manager (AWS RAM), você pode visualizar os compartilhamentos de recursos aos quais você foi adicionado, os recursos compartilhados que você pode acessar e os Contas da AWS que têm recursos compartilhados 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 (UO) que contém a conta
- Sua conta individual
- Para tipos de recursos compatíveis, sua função ou usuário 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 Os diretores 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 de entidade principal no compartilhamento de recursos é desassociado. O convite não pode mais ser aceito pelos usuários finais.

- Clusters de banco de dados do Amazon Aurora
- 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

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 `Pending` status 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 o compartilhamento de recursos para recusar o convite. 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 na conta especificada 123456789012 Região da AWS.

```
$ 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 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 na página do AWS RAM console.

2. Como os compartilhamentos de AWS RAM recursos existem de forma específica 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, Região da AWS defina 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 console AWS RAM exibe informações semelhantes às seguintes:

   - 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 pessoa 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 comando get-resource-shares 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 AWS RAM console.
2. Como os compartilhamentos de AWS RAM recursos existem Região da AWS de forma específicaRegiões da AWS, escolha o apropriado na lista suspensa no canto superior direito do console. Para ver os compartilhamentos de recursos que contêm recursos globais, Região da AWS defina 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 recursos compartilhados específicos. É possível aplicar vários filtros para restringir a pesquisa.
4. As seguintes informações estão disponíveis:
   - Resource ID (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 no especificado Região da AWS de outro 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 console do AWS RAM em https://console.aws.amazon.com/ram.
2. Como os compartilhamentos de AWS RAM recursos existem Regiões da AWS de forma específica Região da AWS escolha a na lista suspensa no canto superior direito do console. Para visualizar os compartilhamentos de recursos que contêm recursos globais, defina 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. No painel de navegação, selecione Shared with me (Compartilhados comigo), Principals (Principais).
4. (Opcional) É possível aplicar um filtro para encontrar diretores específicos. 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 entidades principais que estão compartilhando recursos com você Conta da AWS.

O exemplo de comando 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 indivíduo Conta da AWS e não no contexto de uma organização. Não é possível sair de um Conta da AWS se você foi adicionado a ele por uma conta dentro da organização e o compartilhamento com o AWS Organizations está habilitado. 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 recurso
Amazon Aurora	`rds:Cluster`
Amazon EC2	`ec2:CapacityReservation` `ec2:DedicatedHost`
AWS License Manager	`license-manager:LicenseConfiguration`

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

Amazon Route 53	`route53resolver:ResolverRule`

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

Serviço	Tipo de recurso
	`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 AWS RAM console.
2. Como os compartilhamentos de AWS RAM recursos existem Regiões da AWS de forma específica Região da AWS, escolha a na lista suspensa no canto superior direito do console. Para ver os compartilhamentos de recursos que contêm recursos globais, Região da AWS defina 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 comando disassociate-resource-share para deixar um compartilhamento de recursos.

Os comandos de exemplo a seguir fazem com que Conta da AWS o 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 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"
        }
    ]
}
```

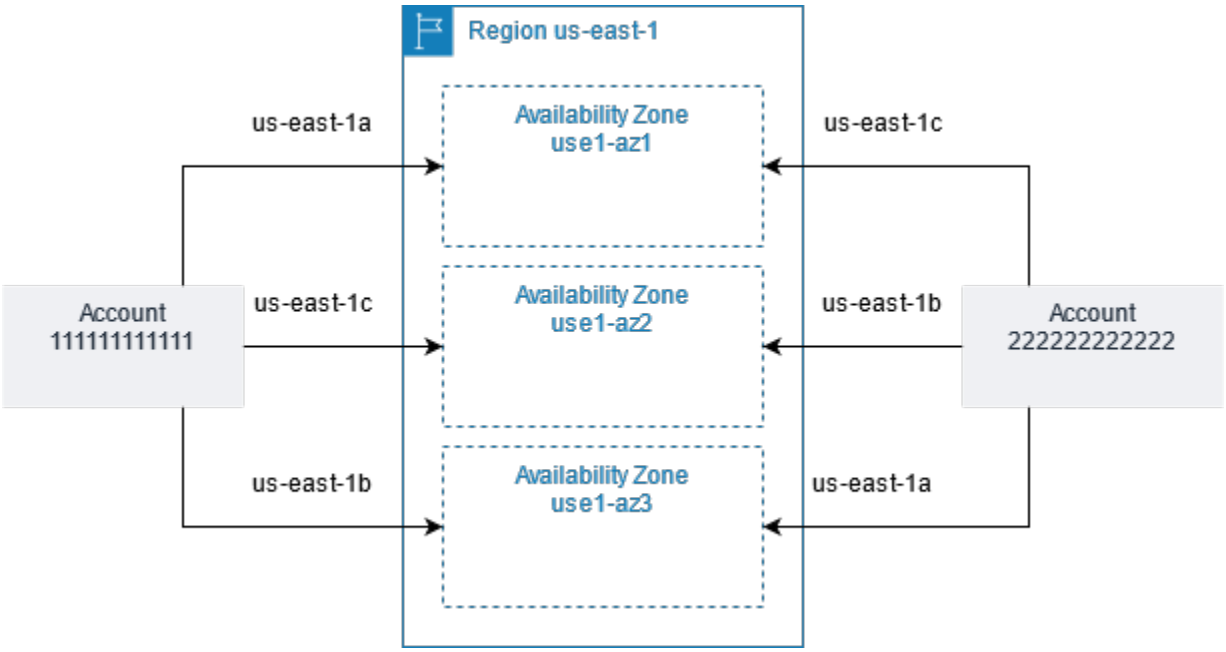
2. Em seguida, você pode executar o comando para deixar o compartilhamento de recursos. Observe que você também deve especificar o ID da sua conta, 123456789012, como principal para se desassociar do compartilhamento de recursos especificado, que é compartilhado por conta 111111111111.

```
$ 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 AWS recursos

AWS mapeia as zonas de disponibilidade físicas aleatoriamente com os nomes das zonas de disponibilidade de cada uma 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 AWS conta pode não representar a mesma localização física `us-east-1a` de uma AWS conta diferente. 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 zona de disponibilidade 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 costuma AWS RAM compartilhar esse recurso com outras pessoas 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 AZ. O AZ ID é um identificador exclusivo e consistente de uma Zona de Disponibilidade em todas as contas da Contas da AWS. Por exemplo,

`use1-az1` é um ID de Zona de Disponibilidade da `us-east-1` região e representa a mesma localização física em todas as AWS contas.

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 da AZ de cada VPC e sub-rede é exibido no console da Amazon VPC e pode ser consultado usando o AWS CLI.

Console

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

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

AWS CLI

Para visualizar os IDs de AZs 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 IAM usuários e funções	 — 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 gerenciad as pelo cliente também são suportadas para esse tipo de recurso.	
	 : recursos desse tipo oferecem suporte ao uso de permissõe s gerenciadas pelo cliente.	Sim
	 : recursos desse tipo não oferecem suporte ao uso de permissões gerenciadas pelo cliente.	Não
Pode compartil har 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

Amazon API Gateway

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

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

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 IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Mesh `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 GraphQL API

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

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
GraphyQL API `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 AWS AppSync mesclagem unificada API que pode acessar dados de vários subesquemas APIs em contas diferentes 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 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 IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Clusters do banco de dados `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 com o Amazon Aurora AWS RAM e 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 IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
BackupVault `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 do (s) cofre (s). Para obter mais informações, consulte Visão geral dos cofres com abertura lógica no Guia do desenvolvedor.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 AWS RAM.

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

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 IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Visualização de faturamento `billing:billingview`	Crie e gerencie visualizações de faturamento personalizadas de forma centralizada e compartilhe-as com outras pessoas Contas da AWS ou com sua organização. Isso permite que proprietários de aplicativos e unidades de negócios acessem os AWS gastos em nível de unidade de negócios a partir de uma conta de membro. Para obter mais informações, consulte Controle do acesso aos dados de gerenciamento de custos com o Billing View no Guia do AWS Cost Management usuário.	 N	 N Pode compartilhar apenas com Contas da AWS em sua própria organização.	 S	 Não

AWS Private Certificate Authority

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

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Private Certificate Authority (CA) `acm-pca:CertificateAuthority`	Crie e gerencie autoridades de certificação privadas (CAs) para a infraestrutura de chave pública interna da sua organização (PKI) 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	 S	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Sim

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	AWS Private Certificate Authority .				

Amazon DataZone

Você pode compartilhar os seguintes DataZone recursos usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
DataZone Domínio `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	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	Amazon DataZone no Guia DataZone do usuário da Amazon.				

AWS CloudHSM

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

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
AWS CloudHSM Backup `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	 S	 S	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	informações sobre o Backup e as usem para restaurar um AWS CloudHSM cluster. Para obter mais informações, consulte Gerenciamento de AWS CloudHSM backups no Guia AWS CloudHSM do usuário.				

AWS CodeBuild

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

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Projeto	Crie um projeto e use-o para executar compilações. Compartil	S	S	S	Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
`codebuild:Project`	he 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 .		Pode compartilhar com qualquer Conta da AWS.		

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Grupo 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 organização. 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 .	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Amazon EC2

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

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	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 EC2 instâncias da Amazon Contas da AWS iniciem sua capacidade reservada gerenciada centralmente. Para obter mais informações, consulte Como trabalhar com reservas de capacidade compartilhada no Guia EC2 do usuário da Amazon.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	Important Se você não atender a todos os pré-requisitos para compartilhar uma reserva de capacidade, a operação de compartilhamento poderá falhar. Se isso acontecer e um usuário tentar iniciar uma EC2 instância da Amazon nessa reserva de capacidade, ela será iniciada como uma instância sob demanda que pode gerar custos mais altos.				

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	Recomendamos que você verifique se pode acessar a reserva de capacidade e compartilhada tentando visualizá-la no EC2 console da Amazon. 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				

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	Exemplo: alertas sobre falhas no compartilhamento de recursos.				

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

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	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 EC2 instâncias da Amazon de qualquer uma das contas com as quais você compartilha em um grupo de posicionamento compartilhado. Para obter mais informações, consulte Compartilhar um grupo de posicionamento no Guia EC2 do usuário da Amazon.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

EC2Image Builder

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

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Componentes `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 os recursos do Share EC2 Image Builder no Guia do usuário do EC2 Image Builder.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não
Fórmulas de contêiner `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 você gerencie quem	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	pode usar documentos predefinidos para duplicar a criação de imagens de contêiner. Para obter mais informações, consulte os recursos do Share EC2 Image Builder no Guia do usuário do EC2 Image Builder.				

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Imagens `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 EC2 Image Builder em toda a sua organização. Para obter mais informações, consulte os recursos do Share EC2 Image Builder no Guia do usuário do EC2 Image Builder.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Fórmulas de imagens `imagebuilder:ImageRecipe`	Crie e gerencie suas receitas de imagens de forma centralizada 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 compilações. AMI Para obter mais informações, consulte os recursos do Share EC2 Image Builder no Guia do usuário do EC2 Image Builder.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 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 IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
OptOutList `sms-voice:opt-out-list`	Crie um OptOutList e compartilhe-o com outras Contas da AWS pessoas em sua organização. Você pode compartilhá-los OptOutList para que os outros aplicativos possam excluir os números de telefone do usuário de diferentes Contas da AWS ou verificar 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
PhoneNumber `sms-voice:phone-number`	Crie e gerencie números de telefone para compartilhá-los com outras pessoas Contas da AWS ou	 N	 S Pode compartil	 S	 Sim

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	com sua organização. Isso permite que várias mensagens sejam Contas da AWS enviadas usando o número de telefone compartilhado. Para obter mais informações, consulte Trabalhando com recursos compartilhados no Guia AWS End User Messaging SMS do usuário.		har com qualquer Conta da AWS.		

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Grupo `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 IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
SenderId `sms-voice:sender-id`	Crie, SenderId gerencie e compartilhe-os com outras pessoas Contas da AWS ou com sua organização. Isso permite que várias mensagens sejam Contas da AWS enviadas usando o compartilhado SenderId. 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 Open ZFS

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

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Volume do FSx `fsx:Volume`	Crie e gerencie ZFS volumes abertos FSx de forma centralizada 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 Amazon FSx for Open ZFS User Guide.	 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 IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Catálogo de dados `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
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 IAM usuários e funções	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 extraiam, transformem e carreguem (ETL) trabalhos 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 IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
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 S3JDBC, fontes de dados, Amazon Redshift, fontes de streaming e outros armazenamentos de dados. Isso permite que os usuários executem consultas e ETL trabalhos 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	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	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 IAM usuários e funções	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 gerenciadas centralme	N	S Pode compartilhar com qualquer Conta da AWS.	N	Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	nte, 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 IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Entidade principal de	Crie, gerencie e compartilhe entidades em Contas da AWS	 S	 S	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
catálogo do Marketplace `aws-marketplace:Entity`	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 .		Pode compartilhar com qualquer Conta da AWS.		

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 IAM usuários e funções	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

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 IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Políticas de firewall `network-firewall:FirewallPolicy`	Crie e gerencie políticas de firewall centralmente e compartilhe-as com outras pessoas Contas da AWS ou 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 políticas de firewall e grupos de regras no Guia do desenvolvedor do AWS Network Firewall .	 S	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

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

Grupos de regras
 	
`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 políticas de firewall e grupos de regras no Guia do desenvolvedor do AWS Network Firewall .	 S	 S
			
			Pode compartilhar com qualquer Conta da AWS.
				 N	 Não

AWS Outposts

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

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	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 EBS volumes 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
Tabela de rotas do gateway local `ec2:LocalGatewayRouteTable`	Crie e gerencie VPC associações com um gateway local de forma centralizada e compartilhe-as com outras pessoas Contas da	 N	 N Pode compartilhar	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	AWS em sua organização. Isso permite que várias contas criem VPC associações 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 IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Sites `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 IAM usuários e funções	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

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 IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Visões `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 IAM usuários e funções	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 vários Contas da AWS compartilhem um grupo de hosts EC2 dedicados da Amazon criados usando 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 IAM usuários e funções	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 Route 53 Resolver DNS Firewall `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 DNS consultas externas que passam pelo Resolvedor do Route 53. Para obter mais informações, consulte Compartilhando grupos de regras do Route 53 Resolver DNS Firewall Contas da AWS no Amazon Route 53 Developer Guide.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não
route 53 Profiles	Crie e gerencie o Route 53 Profiles centralmente e compartilhe-os	 S	 S	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
`route53profiles:Profile`	com outras pessoas Contas da AWS ou com sua organização. Isso permite que várias contas apliquem as DNS configurações especificadas no Route 53. Profiles para váriosVPCs. Para obter mais informações, consulte Amazon Route 53 Profilesno Guia do desenvolvedor do Amazon Route 53.		Pode compartilhar com qualquer Conta da AWS.		

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	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 DNS consultas 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 IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Logs de consulta `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 DNS consultas que se originam VPCs em um registro de consultas 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

Controlador de recuperação de aplicativos Amazon (ARC)

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

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
ARCCluster do `route53-recovery-control:Cluster`	Crie e gerencie ARC clusters 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 Application Recovery Controller (ARC).	 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 IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Access Grants `s3:AccessGrants`	Crie e gerencie centralmente as Instâncias do S3 Access Grants e compartilhe-as 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 IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
SageMaker Catálogo AI `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 IAM usuários e funções	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 IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
SageMaker Grupo 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 permissões	S	S Pode compartilhar com qualquer Conta da AWS.	S	Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	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 AI JumpStart `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 IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Grupo de linhagem `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 IAM usuários e funções	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 IAM usuários e funções	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 Grupo de pacotes de modelos de registro de modelos AI `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 IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
SageMaker Pipeline 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 IAM usuários e funções	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 IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Aplicativo `servicecatalog:Application`	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 IAM usuários e funções	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 IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Grupo de atributos `servicecatalog:AttributeGroup`	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 IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Contatos `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. Para obter mais informações, consulte Como trabalhar com contatos e planos de resposta no Guia do usuário do AWS Systems Manager Incident Manager.	 Sim	 Sim Pode compartilhar com qualquer Conta da AWS.	 Sim	 Não
Plano de resposta	Crie e gerencie planos de resposta centralmente e compartilhe-os com outras pessoas	 Sim	 Sim	 Sim	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
`ssm-incidents:ResponsePlan`	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.		Pode compartilhar com qualquer Conta da AWS.		

AWS Systems Manager Armazenamento de parâmetros

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

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Parameter `ssm:Parameter`	Crie um parâmetro e use-o para armazenar dados de configuração que você pode referenciar em seus scripts, comandos, SSM documentos e fluxos de trabalho de configuração e automação. Compartilhe o parâmetro com outra pessoa Contas da AWS ou com sua organização. Isso permite que vários Contas da AWS usuários visualizem informações sobre a string e melhorem a segurança separando seus dados do seu código. Para obter mais informações, consulte	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	Como trabalhar com parâmetros compartilhados no Guia AWS Systems Manager do usuário.				

Amazon VPC

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

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Endereços de propriedade do cliente IPv4 `ec2:CoipPool`	Durante o processo de AWS Outposts instalação, AWS cria um pool de endereços, conhecido como pool de endereços IP de propriedade do	 N	 N Pode compartilhar	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	cliente, com base nas informações que você 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 EC2 instâncias, 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		apenas com Contas da AWS em sua própria organização.		

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	do usuário do AWS Outposts .				
Pools do Gerenciador de Endereços IP (IPAM) `ec2:IpamPool`	Compartilhe os VPC IPAM pools da Amazon centralmente com outras Contas da AWS IAM funções ou usuários, ou com uma organização ou unidade organizacional (OU) inteira em AWS Organizations. Isso permite que esses diretores aloquem AWS recursos CIDRs do pool, por exemploVPCs, em suas respectivas contas. Para obter mais informações, consulte Compartilhar um IPAM pool usando AWS RAM o Guia do usuário do Amazon VPC IP Address Manager.	 S	 S Pode compartilhar com qualquer Conta da AWS.	 S	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	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 IP Address Manager (IPAM) `ec2:IpamResourceDiscovery`	Compartilhe descobertas de recursos com outros Contas da AWS. A descoberta de recursos é um VPC IPAM componente da Amazon que IPAM permite gerenciar e monitorar recursos que pertencem à conta proprietária. Para obter mais informações, consulte Trabalhe com descobertas de recursos no Guia do VPC IPAM usuário da Amazon.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	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 Contas da AWS referência em seus recursos, como grupos de VPC segurança e tabelas de rotas de sub-rede. Para obter mais informações, consulte Como trabalhar com listas de prefixos compartilhadas no Guia do VPC usuário da Amazon.	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	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 vários Contas da AWS iniciem seus recursos de aplicativos em um gerenciamento VPCs centralizado. Esses recursos incluem EC2 instâncias da Amazon, bancos de dados Amazon Relational Database Service RDS (), clusters AWS Lambda e funções do Amazon Redshift. Para obter mais informações, consulte Como [trabalhar com o VPC compartilhamento](#) no Guia VPC do usuário da Amazon.	 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 IAM usuários e funções	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 IAM usuários e funções	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 vários Contas da AWS associem o grupo de segurança às suas interfaces de rede elástica. Para obter mais informações, consulte Compartilhar um grupo de segurança no Guia VPC do usuário da Amazon.	 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 IAM usuários e funções	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 IAM usuários e funções	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 Compartilhamento de um gateway de trânsito nos Amazon VPC Transit Gateways. **Note** Para incluir um gateway de trânsito ao criar um compartil	 N	 S Pode compartilhar com qualquer Conta da AWS.	 N	 Não

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

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	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 IAM usuários e funções	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 grupo `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 do Amazon VPC Lattice usando AWS RAM.

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
Serviço Amazon VPC Lattice `vpc-lattice:Service`	Crie e gerencie serviços Amazon VPC Lattice de forma centralizada 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 Trabalhando com recursos compartilhados no Guia do usuário do VPC Lattice.	N	S Pode compartilhar com qualquer Conta da AWS.	S	Não
Rede de serviços Amazon VPC Lattice `vpc-lattice:ServiceNetwork`	Crie e gerencie redes de serviços Amazon VPC Lattice de forma centralizada e compartilhe-as com indivíduos Contas da AWS ou	N	S Pode compartilhar com	S	Não

Tipo de recurso e código	Caso de uso	Pode compartilhar com IAM usuários e funções	Pode compartilhar com contas fora da organização	Pode usar permissões gerenciadas pelo cliente	Pode compartilhar com as entidades principais de serviços
	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 compartilhados no Guia do usuário do Amazon VPC Lattice.		qualquer Conta da AWS.		

AWS Nuvem WAN

Você pode compartilhar os seguintes WAN recursos de AWS nuvem usando AWS RAM.

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

Gerenciando permissões em AWS RAM

Em AWS RAM, há dois tipos de permissões gerenciadas: permissões, AWS 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 das entidades principais associadas 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 AWS RAM console 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 o mais rápido 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 AWS RAM console.

Console

Para ver detalhes sobre as permissões gerenciadas disponíveis em AWS RAM

1. Navegue até a página da biblioteca de permissões gerenciadas na página do AWS RAM console.
2. Como os AWS RAM compartilhamentos de recursos existem de forma específica Regiões da AWS, escolha o apropriado Região da AWS na lista suspensa no canto superior direito do console. Para ver os compartilhamentos de recursos que contêm recursos globais, Região da AWS defina o como Leste dos EUA (Norte da Virgínia), (`us-east-1`). Para obter mais informações sobre o compartilhamento de recursos de compartilhamento global, consulte Compartilhamento de recursos regionais em comparação com recursos globais. Embora todas as regiões compartilhem as mesmas permissões AWS gerenciadas 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 AWS gerenciada 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 Conta da AWS número do 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 AWS recurso 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 de recurso da Amazon (ARN) da permissão gerenciada. Os ARNs para permissões AWS gerenciadas 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 list-permissions comando para obter uma lista das permissões gerenciadas disponíveis para uso em compartilhamentos de recursos na conta atual Região da AWS para a 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 `--query` parâmetro do `list-permissions` AWS CLI comando. O exemplo a seguir filtra a saída para incluir somente elementos nos resultados da `permissions` matriz 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 menor privilégio 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 o uso compartilhado de recursos AWS RAM. Por exemplo, você quer limitar o acesso de leitura aos seus pools do Amazon VPC IP Address Manager (IPAM), 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. Você pode seguir a prática recomendada de privilégio mínimo, concedendo 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 política 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 política gerenciada pelo cliente

1. Faça um dos seguintes 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 na págin a do 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 o 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 conforme necessário.
6. Quando concluir, escolha Criar permissão gerenciada pelo cliente.

AWS CLI

Para criar uma política 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 `imagebuilder:Component` tipo de recurso.

```
$ 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 usam 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 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 permissão gerenciadas, escolha Criar versão.
4. Para o 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 de recurso da Amazon (ARN) da permissão gerenciada para a qual você deseja criar uma nova versão. Faça isso 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, você pode chamar a operação create-permission-version 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 versão 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 pelo cliente ou pesquise o nome da permissão gerenciada pelo cliente que você deseja alterar.
3. Na página de detalhes da permissão gerenciada pelo cliente, na seção Versões de permissão 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 usam 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 versão padrão chamando list-permission-versions.

   O comando de exemplo a seguir está associado a uma instância de banco de dados gerenciada pelo cliente.

```
$ 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 operação set-default-permission-version.

```
$ 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-versions novamente 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 instância 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 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 esta versão da sua permissão gerenciada pelo cliente.

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

AWS CLI

Para excluir uma versão de uma permissão gerenciada pelo cliente

1. Chame a operação list-permission-versions 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-versions novamente 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 atualize 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 AWS permissão gerenciada

1. Execute o comando get-resource-shares com o `--permission-arn` parâmetro para especificar o Amazon Resource Name (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 AWS gerenciada você está atualizando e o `--replace` parâmetro 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 um `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 combinar as propriedades do principal:
  - `aws:PrincipalOrgId`
  - `aws:PrincipalOrgPaths`
  - `aws:PrincipalAccount`

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

> **Note**
>
> O `aws:SourceAccount` valor é preenchido automaticamente ao ser compartilhado com os diretores do serviço.

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 AWS recursos.

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 deve `Allow` ou não `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. Pode ser uma ação no AWS Management Console, ou uma operação na AWS Command Line Interface (AWS CLI) ou na API da AWS. As ações são definidas pela AWS permissão. Para obter mais informações, consulte Ações no Guia do usuário do usuário 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 AWS chaves de contexto de condição global no Manual do usuário do IAM. Para obter mais informações sobre condições específicas do serviço, consulte Ações, recursos e chaves de condição AWS do serviço na Referência de autorização do serviço.

> **Note**
>
> As condições estão disponíveis para permissões gerenciadas pelo cliente e tipos de recursos compatíveis para permissões AWS gerenciadas.

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 de recurso. Por exemplo, para o tipo de recurso Amazon VPC `ec2:Subnet`, 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, AWS seja ela 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 uma 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.

- As 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 AWS RAM. Por exemplo, você quer limitar o acesso de leitura aos seus grupos da Amazon VPC IP Address Manager (IPAM), 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 RAM

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 RAM

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 seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre privacidade de dados, consulte Privacidade de dados FAQ. Para obter informações sobre proteção de dados na Europa, consulte o Modelo de Responsabilidade AWS Compartilhada e GDPR a postagem no blog AWS de segurança.

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 a autenticação multifator (MFA) com cada conta.
- UseSSL/TLSpara se comunicar com AWS os recursos. Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Configure API e registre as 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 sigilosos armazenados no Amazon S3.
- Se você precisar de FIPS 140-3 módulos criptográficos validados ao acessar AWS por meio de uma interface de linha de comando ou umaAPI, use um endpoint. FIPS Para obter mais informações sobre os FIPS endpoints disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com AWS RAM ou Serviços da AWS usa o console,API, AWS CLI, ou AWS SDKs. Quaisquer dados inseridos em tags ou 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 altamente recomendável que você não inclua informações de credenciais no URL para validar sua solicitação para esse servidor.

Gerenciamento de identidade e acesso para AWS RAM

AWS Identity and Access Management (IAM) é um AWS serviço que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Administradores que IAM controlam quem pode ser autenticado (conectado) e autorizado (com permissões) a usar AWS recursos. Ao usarIAM, 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 IAM sem custo adicional. Para obter mais informações sobre como gerenciar e criar IAM políticas personalizadas, consulte Gerenciamento de IAM políticas no Guia IAM do usuário.

Tópicos

Como AWS RAM funciona com IAM

Por padrão, IAM os diretores não têm permissão para criar ou modificar AWS RAM recursos. Para permitir que IAM os diretores criem ou modifiquem recursos e executem tarefas, execute uma das etapas a seguir. Essas ações concedem permissão para usar recursos e API ações 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 IAM por meio de um provedor de identidade:

Crie um perfil para a federação de identidades. Siga as instruções em Criar uma função para um provedor de identidade terceirizado (federação) no Guia IAM do usuário.

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

AWS RAM fornece várias políticas AWS gerenciadas que você pode usar para atender às necessidades de muitos usuários. Para obter mais informações sobre essas ferramentas, consulte Políticas gerenciadas pela AWS para o AWS RAM.

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

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

Sumário

Estrutura da política

Uma política de IAM permissão é um JSON documento que inclui as seguintes declarações: Efeito, Ação, Recurso e Condição. Uma IAM política geralmente assume 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 de ação especifica as AWS RAM API ações para as quais a política está permitindo ou negando permissão. Para obter uma lista completa das ações permitidas, consulte Ações definidas por AWS Resource Access Manager no Guia IAM do usuário.

Recurso

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

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 a permissão ARN especificada na solicitação de serviço corresponde a uma ARN string 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 principal especificado na solicitação de serviço corresponde a uma ARN string 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 recurso que está sendo processado pela solicitação de serviço corresponde ao ARN que você especificou 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.

Políticas gerenciadas pela AWS para o AWS RAM

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

Políticas gerenciadas pela AWS

- AWS política gerenciada: AWSResourceAccessManagerReadOnlyAccess
- AWS política gerenciada: AWSResourceAccessManagerFullAccess
- AWS política gerenciada: AWSResourceAccessManagerResourceShareParticipantAccess
- AWS política gerenciada: AWSResourceAccessManagerServiceRolePolicy
- Atualizações do AWS RAM para políticas gerenciadas pela AWS

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 vinculada à AWS RAM função de serviço do service-linked.

Uma política gerenciada pela AWS é uma política independente criada e administrada pela AWS. As políticas gerenciadas pela AWS são criadas para fornecer permissões a vários casos de uso comuns a fim de que você possa começar a atribuir permissões a usuários, grupos e perfis.

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

Você não pode alterar as permissões definidas em políticas gerenciadas pela AWS. Se a AWS atualiza as permissões definidas em um política gerenciada pela AWS, a atualização afeta todas as identidades de entidades principais (usuários, grupos e perfis) às quais a política está vinculada. É mais provável que a AWS atualize uma política gerenciada pela AWS quando um novo AWS service (Serviço da AWS) é lançado ou novas operações de API são disponibilizadas para os serviços existentes.

Para obter mais informações, consulte Políticas gerenciadas pela AWS no Manual do usuário do IAM.

AWS política gerenciada: AWSResourceAccessManagerReadOnlyAccess

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

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

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

Detalhes da permissão

Esta política inclui as seguintes permissões.

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

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

AWS política gerenciada: AWSResourceAccessManagerFullAccess

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

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

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

Detalhes da permissão

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.

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

AWS política gerenciada: AWSResourceAccessManagerResourceShareParticipantAccess

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

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

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

Detalhes da permissão

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.

```
{
    "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: AWSResourceAccessManagerServiceRolePolicy

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

Esta política AWS RAM fornece acesso somente 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 AWSServiceRoleForResourceAccessManager que 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 `organizations:Describe` operações `organizations:List` e que fornecem detalhes da estrutura e das contas da organização.

Detalhes da permissão

Esta política inclui as seguintes permissões.

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

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

Atualizações do AWS RAM para políticas gerenciadas pela AWS

Visualizar detalhes sobre atualizações em políticas gerenciadas pela AWS para o AWS RAM desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações feitas nesta página, inscreva-se no feed RSS na página de histórico de documentos do AWS RAM.

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

Usar funções vinculadas ao serviço do AWS RAM

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

Uma função vinculada ao serviço facilita a configuração do AWS RAM porque você não precisa adicionar as permissões necessárias manualmente. AWS RAM define as permissões de suas funções vinculadas ao serviço e, a menos que definido em contrário, somente AWS RAM pode assumir suas funções. 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 funções vinculadas a serviços, consulte Serviços da AWS compatíveis com o IAM e procure os serviços que contenham Yes (Sim) na coluna Service-Linked Role (Função vinculada a serviço). Escolha um Sim com um link para visualizar a documentação da função vinculada a esse serviço.

Permissões da função vinculada ao serviço para o 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.

Esta função vinculada ao service-linked confia no seguinte serviço para assumir a função:

- `ram.amazonaws.com`

A política de permissões para essa função vinculada ao serviço chama-se AWSCloud9ServiceRolePolicy, e ela permite que o AWS RAM conclua 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 uma entidade principal ative o AWS RAM compartilhamento em sua organização, essa entidade principal (uma entidade do IAM, por exemplo, um usuário, grupo ou função) deve ter permissão para criar uma função vinculada a serviço. Para obter mais informações, consulte Permissões de função vinculada ao serviço no Guia do usuário do IAM.

Criação de uma função vinculada a um serviço do AWS RAM

Não é necessário criar manualmente uma função vinculada ao serviço. Quando você ativa o AWS RAM compartilhamento dentro da sua organização no AWS Management Console, ou executa o EnableSharingWithAWSOrganization em sua conta usando o AWS CLI ou uma AWS API, AWS RAM cria a função vinculada ao serviço para você.

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

Editar uma função vinculada ao serviço para o AWS RAM

O AWS RAM não permite que você edite a função vinculada ao serviço AWSResourceAccessManagerServiceRolePolicy. Depois que criar uma função vinculada ao serviço, você não poderá alterar o nome da função, pois várias entidades podem fazer referência a ela. No entanto, será possível editar a descrição da função usando o IAM. Para obter mais informações, consulte Editar uma função vinculada ao serviço no Guia do usuário do IAM.

Exclusão de uma função vinculada ao serviço do AWS RAM

Também é possível usar o console do IAM, a AWS CLI ou a API da AWS para excluir manualmente a função vinculada ao serviço.

Como excluir manualmente a função vinculada ao serviço usando o IAM

Use o console do IAM, a AWS CLI ou a API da AWS para excluir a função vinculada ao serviço `AWSResourceAccessManagerServiceRolePolicy`. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Regiões com suporte a funções vinculadas a serviço do AWS RAM

O AWS RAM oferece suporte a funções vinculadas a serviços 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.

Exemplos 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 entidades principais 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 a associarem apenas recursos específicos a compartilhamentos de recursos.

Por exemplo, a política a seguir limita as entidades a compartilhar somente a regra do resolvedor com o nome de recurso da Amazon (ARN) especificado. O operador `StringEqualsIfExists` permite uma solicitação se a solicitação não incluir um `ResourceArn` parâmetro 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 Operadores de condição ...IfExists no Guia do usuário do IAM.

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

```
        "Condition": {
            "StringEqualsIfExists": {
                "ram:ResourceArn": "arn:aws:route53resolver:us-
west-2:123456789012:resolver-rule/rslvr-rr-5328a0899aexample"
            }
        }
    }]
}
```

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.

Por exemplo, a política a seguir limita as entidades principais a compartilhar somente regras do resolvedor.

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

Exemplo 3: restringir o compartilhamento com entidades principais externas Contas da AWS

É possível usar uma política do IAM para impedir que as entidades compartilhem recursos com Contas da AWS contas da AWS fora da organização.

Por exemplo, a seguinte política do IAM impede que entidades principais adicionem compartilhamentos externos Contas da AWS aos recursos compartilhados.

```
{
```

```
    "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). SCPssão políticas que você anexa a elementos em uma organização para gerenciar permissões dentro dessa organização. E SCP se aplica a tudo o que Contas da AWS está abaixo do elemento ao qual você anexa SCP o. SCPsofereça 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 usarSCPs, 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 criaçãoSCPs, 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 seguinte SCP impede que os usuários criem compartilhamentos de recursos que permitam o compartilhamento com entidades que estão fora da organização do usuário de compartilhamento.

```
{
    "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 seguinte SCP impede que qualquer 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 isso. SCP

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

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

O seguinte SCP permite somente contas 111111111111 e 222222222222 a criação de novos compartilhamentos de recursos que compartilhem listas de EC2 prefixos da Amazon ou associem listas de prefixos a compartilhamentos de recursos existentes.

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

```
}
```

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

O seguinte SCP 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 IAM funções ou usuários.

```
{
    "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 SCP permite que os usuários compartilhem recursos somente com a unidade `o-12345abcdef`, organizacional da `ou-98765fedcba` organização Conta da AWS `111111111111` e.

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

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.

Para habilitar o compartilhamento com o AWS Organizations

1. Desative o acesso confiável ao AWS Organizations usando o comando AWS Organizations disable-aws-service-access AWS CLI.

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

> **Important**
>
> Quando você desabilita o acesso confiável ao AWS Organizations, os principais das organizações são removidos de todos os compartilhamentos de recursos e perdem o acesso a esses recursos compartilhados.

2. Use o console do IAM, a AWS CLI ou a API do IAM para excluir a função vinculada ao serviço AWSServiceRoleForEC2CapacityReservationFleet. Para obter mais informações, consulte Excluir uma função vinculada ao serviço no Guia do usuário do IAM.

Registro e monitoramento em AWS RAM

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

Amazon EventBridge

Fornece um near-real-time fluxo de eventos do sistema que descrevem as mudanças nos AWS recursos. EventBridge permite a computação automatizada baseada em eventos, pois você pode escrever regras que observam determinados eventos e acionam ações automatizadas em outros AWS serviços quando esses eventos acontecem. Para obter mais informações, consulte Monitoramento AWS RAM usando EventBridge.

AWS CloudTrail

Captura API chamadas e eventos relacionados feitos por você ou em seu nome Conta da AWS e entrega os arquivos de log em um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte Registrar em log chamadas de API do AWS RAM com o 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 EC2 de capacidade da Amazon 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, a 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 a AmazonSNS, 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 do evento e escolha Padrões personalizados (JSONeditor).
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 alvo, escolha o SNStópico.
9. Em Tópico, escolha o SNS tópico 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 SNS alerta 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 EC2 console da Amazon a partir dessas contas.

Registrar em log chamadas de API do AWS RAM com o AWS CloudTrail

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

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

Informações do AWS RAM no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando ocorre uma atividade no AWS RAM, ela é registrada em um evento do CloudTrail junto com outros eventos de serviços da AWS em Event history (Histórico de eventos). Você pode visualizar, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Visualizar eventos com o histórico de eventos do CloudTrail.

Para obter um registro contínuo de eventos na sua Conta da AWS, incluindo eventos para o AWS RAM, crie uma trilha. Uma trilha permite que o CloudTrail entregue arquivos de log a um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as regiões da AWS. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, é possível configurar outros serviços da AWS para analisar mais ainda mais e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- Criar uma trilha para a sua Conta da AWS
- Integrações de AWS service (Serviço da AWS) com logs do CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões e Receber arquivos de log do CloudTrail de várias contas

Todas as ações do AWS RAM são registradas pelo CloudTrail e são documentadas na Referência de API do AWS RAM. Por exemplo, as chamadas para as APIs `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 de raiz
- Credenciais de segurança temporárias de um perfil do AWS Identity and Access Management (IAM) ou de um usuário federado.
- Credenciais de segurança de longo prazo de um usuário do IAM.
- Outro serviço da AWS.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail.

Noções básicas sobre entradas de arquivos de log do AWS RAM

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Os arquivos de log do CloudTrail 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 de solicitação e assim por diante. Os arquivos de log do CloudTrail não são um rastreamento de pilha ordenada de chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

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

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "NOPIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:user/admin",
        "accountId": "111122223333",
        "accessKeyId": "BCDIOSFODNN7EXAMPLE",
        "userName": "admin"
    },
    "eventTime": "2018-11-03T04:23:19Z",
    "eventSource": "ram.amazonaws.com",
    "eventName": "CreateResourceShare",
```

```
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.1.0",
    "userAgent": "aws-cli/1.16.2 Python/2.7.10 Darwin/16.7.0 botocore/1.11.2",
    "requestParameters": {
        "name": "foo"
    },
    "responseElements": {
        "resourceShare": {
            "allowExternalPrincipals": true,
            "name": "foo",
            "owningAccountId": "111122223333",
            "resourceShareArn": "arn:aws:ram:us-east-1:111122223333:resource-share/
EXAMPLE0-1234-abcd-1212-987656789098",
            "status": "ACTIVE"
        }
    },
    "requestID": "EXAMPLE0-abcd-1234-mnop-987654567876",
    "eventID": "EXAMPLE0-1234-abcd-hijk-543234565434",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
```

Resiliência no AWS RAM

A infraestrutura global da AWS se baseia em Regiões da AWS e zonas de disponibilidade. A Regiões da AWS oferece várias zonas de disponibilidade separadas e isoladas fisicamente que são conectadas com baixa latência, altas taxas de throughput e em redes altamente redundantes. Com as zonas de disponibilidade, você pode 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 Regiões da AWS e zonas de disponibilidade, consulte Infraestrutura global da AWS.

Segurança da infraestrutura em AWS RAM

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 API chamadas AWS publicadas para acessar AWS RAM pela rede. Os clientes devem oferecer suporte para:

- Segurança da camada de transporte (TLS). Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Suítes de criptografia com sigilo direto perfeito (), como (Ephemeral PFS Diffie-Hellman) ou DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando uma ID de chave de acesso e uma chave de acesso secreta associada a um IAM principal. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

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

Você pode usar: AWS PrivateLink para criar uma conexão privada entre seu VPC e AWS Resource Access Manager. Você pode acessar AWS RAM como se estivesse no seuVPC, sem o uso de um gateway de internet, NAT dispositivo, VPN conexão ou AWS Direct Connect conexão. As instâncias em seu VPC não precisam de endereços IP públicos para acessar AWS RAM.

Você estabelece essa conexão privada criando um endpoint de interface, alimentado por AWS PrivateLink. Criamos uma interface de rede de endpoint em cada sub-rede que você habilita para o endpoint da interface. Essas são interfaces de rede gerenciadas pelo solicitante que servem como ponto de entrada para o tráfego destinado a AWS RAM.

Para obter mais informações, consulte Access Serviços da AWS através AWS PrivateLink no AWS PrivateLink Guia.

Considerações para AWS RAM

Antes de configurar um endpoint de interface para AWS RAM, revise as considerações no AWS PrivateLink Guia.

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

VPCas políticas de endpoint são suportadas para AWS RAM. Por padrão, acesso total ao 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 usando o VPC console da Amazon ou o AWS Command Line Interface (AWS CLI). Para obter mais informações, consulte Criar um endpoint de interface no AWS PrivateLink Guia.

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

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

Se você habilitar private DNS para o endpoint da interface, poderá fazer API solicitações para AWS RAM usando seu DNS nome 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 IAM recurso que você pode anexar a um endpoint de interface. A política de endpoint padrão permite acesso total a AWS RAM por meio do endpoint da interface. Para controlar o acesso permitido ao AWS RAM do seuVPC, anexe uma política de endpoint personalizada ao endpoint da interface.

Uma política de endpoint especifica as seguintes informações:

- Os diretores que podem realizar ações (Contas da AWS, IAM usuários e IAM funções).
- As ações que podem ser executadas.
- Os recursos nos quais as ações podem ser executadas.

Para obter mais informações, consulte Controlar o acesso aos serviços usando políticas de endpoint no AWS PrivateLink Guia.

Exemplo: política VPC de endpoint para AWS RAM actions

O exemplo a seguir refere-se a uma política de endpoint personalizada. Quando você anexa essa política ao seu endpoint de interface, ela concede acesso às informações listadas AWS RAM ações para todos os diretores em todos os recursos.

```
{
```

```
    "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 organização da AWS ”

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. Entre na conta de gerenciamento da sua organização usando uma IAM função ou usuário com permissões administrativas.
2. Navegue até a página Serviços no AWS Organizations console.
3. Selecione RAM.
4. Escolha Disable trusted access (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 AWS Identity and Access Management (IAM) principal. Isso também pode acontecer devido às restrições impostas por uma política de controle de AWS Organizations serviço (SCP) que afeta sua 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 IAM por meio de um provedor de identidade:

  Crie um perfil para a federação de identidades. Siga as instruções em Criar uma função para um provedor de identidade terceirizado (federação) no Guia IAM do usuário.
- IAMusuários:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criar uma função para um IAM usuário no Guia do IAM usuário.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adicionar permissões a um usuário (console) no Guia do IAM usuário.

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 pela sua organizaçãoSCPs.

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 como seria essa política de IAM permissão.

```
{
    "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 possível encontrar”
- “CannotUpdateResourceShare: UnknownResourceException: OrganizationalUnit ou-*xxxx* não foi possível encontrar”.

Causa

Esses erros podem ocorrer se você habilitar a integração entre AWS RAM e AWS Organizations usando o console Organizations ou o Organizations E nableAWSService Access API em vez de usar o AWS RAM console. Quando você ativa a integração usando o console Organizations ouAPI, o serviço não cria a `AWSServiceRoleForResourceAccessManager` função 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, ligue-o novamente chamando a AWS RAM EnableSharingWithAwsOrganizationAPIoperação ou usando o AWS Management Console para executar 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. Entre na conta de gerenciamento da sua organização usando uma IAM função ou usuário com permissões administrativas.
2. Navegue até a página Serviços no AWS Organizations console.
3. Selecione RAM.
4. Escolha Disable trusted access (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 de tipo de recurso com essa restrição são as conexões privadas virtuais (VPCs) que fazem parte do Amazon Elastic Compute Cloud (AmazonEC2).

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. Entre na conta de gerenciamento da sua organização usando uma IAM função ou usuário com permissões administrativas.
2. Navegue até a página Serviços no AWS Organizations console.

3. Selecione RAM.
4. Escolha Disable trusted access (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 AWS RAM console e verifique se a AWS Organizations caixa de seleção Habilitar compartilhamento com 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. Entre na conta de gerenciamento da sua organização usando uma IAM função ou usuário com permissões administrativas.

2. Navegue até a página Serviços no AWS Organizations console.
3. Selecione RAM.
4. Escolha Disable trusted access (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 às IAM funções e aos usuários da conta B que precisam acessar o recurso. Como exemplo, a política a seguir mostra como você pode conceder acesso somente de leitura a funções e usuários na conta B para um recurso da conta A. A política especifica o recurso por seu Amazon Resource Name (). ARN

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ram:Get*",
                "ram:List*"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:<service>:<Region-code>:<Account-A-ID>:<resource-id>"
        }
    ]
```

```
}
```

O recurso está em uma 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 AWS Management Console 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 VPC sub-rede

Cenário

Quando você tenta usar AWS RAM para compartilhar uma VPC sub-rede 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 (AmazonVPC) 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 esse limite, consulte VPCCotas da Amazon — VPC compartilhamento no Guia do usuário da 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 principal ao compartilhamento de recursos RAM para detectar a alteração.

Cotas de serviço para AWS RAM

Sua conta da 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 Support.

Note

As seguintes definições se aplicam à descrição nas cotas abaixo:

- Recurso - Um elemento AWS service (Serviço da AWS) criado por um indivíduo 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 AWS RAM criado 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. Isso pode ser uma função ou usuário AWS Identity and Access Management (IAM), um Conta da AWS identificador, uma unidade organizacional ou uma organização inteira. Cada entidade 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
Número máximo de associações de recursos por compartilhamento de recursos	5.000

Recurso	Limite padrão
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 um 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 prinde entidades principais em todos os compartil hamentos de recursos em um 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 da mesma 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 da mesma 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 (SDKs) da AWS estão disponíveis para muitas linguagens de programação populares. Cada SDK fornece uma API, exemplos de código e documentação que facilitam a criação de aplicações em seu idioma preferido pelos desenvolvedores.

Documentação do SDK	Exemplos de código
AWS SDK for C++	Exemplos de código do AWS SDK for C++
AWS SDK for Go	Exemplos de código do AWS SDK for Go
AWS SDK for Java	Exemplos de código do AWS SDK for Java
AWS SDK for JavaScript	Exemplos de código do AWS SDK for JavaScript
AWS SDK for .NET	Exemplos de código do AWS SDK for .NET
AWS SDK for PHP	Exemplos de código do AWS SDK for PHP
AWS SDK for Python (Boto3)	Exemplos de código do AWS SDK for Python (Boto3)
AWS SDK for Ruby	Exemplos de código do AWS SDK for Ruby

Exemplo de disponibilidade

Você não pode encontrar o que precisa? Solicite um exemplo de código com o link de feedback.

Histórico de documentos para o 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 se inscrever no AWS RAM RSS feed.

Alteração	Descrição	Data
Foi adicionado suporte 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
Foi adicionado 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
Foi adicionado suporte para compartilhar VPC recursos da Amazon.	Agora você pode compartilhar grupos de VPC segurança da Amazon com outras pessoas Contas da AWS ou dentro da sua organização.	30 de outubro de 2024
Foi adicionado suporte 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 for AWS RAM, você pode se conectar diretamente RAM usando um endpoint de	9 de setembro de 2024

	interface em sua nuvem privada virtual (VPC).	
Foi adicionado suporte para compartilhamento AWS Backup.	Você pode compartilhar cofres logicamente isolados em sua organização ou dentro dela. Contas da AWS	7 de agosto de 2024
Suporte adicionado 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
Foi adicionado suporte 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
Suporte adicionado para compartilhar Amazon SageMaker AI Model Registry recursos.	Agora você pode compartil har parâmetros avançados de forma segura e eficiente em sua organização Contas da AWS ou dentro dela.	27 de junho de 2024
Foi adicionado suporte para compartilhar o 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 Contas da AWS pessoas da sua organização.	22 de abril de 2024
Foi adicionado suporte para compartilhar recursos AWS Systems Manager do Parameter Store.	Agora você pode compartil har parâmetros avançados de forma segura e eficiente em sua organização Contas da AWS ou dentro dela.	21 de fevereiro de 2024
Foi adicionado suporte para compartilhar Amazon FSx for Open ZFS Snapshots.	Agora você pode compartil har o Amazon FSx for Open ZFS Snapshots com outras pessoas Contas da AWS da sua organização.	19 de dezembro de 2023
Foi adicionado suporte 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
Foi adicionado suporte 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

Foi adicionado 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
Foi adicionado suporte 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
Adicionado suporte para compartilhamento de entidade principal de serviço.	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
Foi adicionado suporte 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
Foi adicionado suporte ao 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 permissões gerenciadas 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
Foi adicionado suporte ao serviço Amazon VPC Lattice e aos recursos compartilháveis da rede de serviços.	Agora você pode compartilhar o serviço Amazon VPC Lattice e os recursos da 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
IAMatualização das melhores práticas.	Guia atualizado para se alinhar às IAM melhores práticas. Para obter mais informações, consulte Melhores práticas de segurança em IAM.	3 de janeiro de 2023
Foi adicionado suporte para grupos de EC2 posiciona mento da Amazon como recursos compartilháveis.	Agora você pode compartil har grupos de EC2 posiciona mento da Amazon com outras Contas da AWS pessoas 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
Foi adicionado suporte 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 SOC uma ISO certificação.	AWS RAM foi validado como compatível com os padrões Service Organization Control (SOC) e International Organization for Standardi zation (ISO) ISO 9001, ISO 27001, 27017, 27018 e ISO 27701. ISO ISO	31 de maio de 2022
AWS Resource Access Manager recebe a RAMP certificação do Fed.	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 PCI DSS certificação.	AWS RAM foi validado como compatível com o Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCIDSS).	27 de fevereiro de 2022
Foi adicionado suporte para descobertas VPC IPAM de recursos da Amazon como recursos compartilháveis. Além disso, agora você pode compartilhar IPAM grupos com contas fora de uma organizaç ão.	Agora você pode compartilhar descobertas IPAM de recursos com outras Contas da AWS pessoas.	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

Foi adicionado suporte para redes WAN centrais AWS em nuvem como recursos globais compartilháveis.	Agora você pode compartilhar redes WAN principais do Cloud com outras Contas da AWS.	2 de dezembro de 2021
Support para compartilhar pools do Amazon VPC IP Address Manager (IPAM)	Você pode usar AWS RAM para compartilhar VPC IPAM pools da Amazon. Para obter mais informações, 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 compartilháveis no Guia do usuário do AWS RAM .	29 de novembro de 2021
Foram adicionadas informações sobre políticas AWS RAMAWS de IAM permissões gerenciadas.	Detalhes publicados sobre as políticas AWS de permissão gerenciada disponíveis que você pode acessar no IAM console e anexar aos IAM diretores em 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
Suporte adicional para permissões gerenciadas adicionais e compartilhamento de recursos com IAM diretores	Para tipos de recursos compatíveis, você pode escolher entre permissõe s AWS RAM gerenciadas adicionais e compartilhar recursos com IAM funções e usuários individuais.	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 outras pessoas 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
Foi adicionado suporte para compartilhar AWS Private Certificate Authority 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 VPC prefixos da Amazon.	Agora você pode usar AWS RAM para compartilhar listas de prefixos.	29 de junho de 2020

Foi adicionado suporte para compartilhar endereços de AWS Outposts propriedade do clienteIPv4.	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
Foi adicionado suporte 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 Amazon EC2 Dedicated Hosts, grupos de AWS Resource Groups recursos e componentes, 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 VPC sub-redes da Amazon 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 os gateways de VPC trânsito da Amazon 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.