Manual do usuário

# Explorador de recursos da AWS

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

# Explorador de recursos da AWS: Manual do usuário

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

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestigie a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

# Table of Contents

# O que Explorador de recursos da AWSé

Explorador de recursos da AWS é um serviço de pesquisa e descoberta de recursos. Com o Explorador de Recursos, você pode explorar os recursos, como instâncias do Amazon Elastic Compute Cloud, fluxos do Amazon Kinesis ou tabelas do Amazon DynamoDB usando uma experiência semelhante à do mecanismo de pesquisa na Internet. Você pode pesquisar seus recursos usando metadados de recursos, como nomes, tags e. IDs O Resource Explorer funciona Regiões da AWS em toda a sua conta para simplificar suas cargas de trabalho entre regiões.

O Resource Explorer fornece respostas rápidas às suas consultas de pesquisa usando índices criados e mantidos pelo Explorador de recursos da AWS serviço. O Explorador de Recursos usa várias fontes de dados para coletar informações sobre os recursos na sua Conta da AWS. O Explorador de Recursos armazena essas informações nos índices para o Explorador de Recursos pesquisar.

> **Queremos seu feedback sobre esta documentação**
>
> Nosso objetivo é ajudar você fazer o melhor uso possível do Explorador de Recursos. Se este guia ajudar você a fazer isso, nos informe. Se o guia não estiver ajudando, queremos que nos diga para podermos resolver o problema. Use o link de feedback que está no canto superior direito de cada página. Isso envia seus comentários diretamente aos redatores deste guia. Nós analisamos cada envio, procurando oportunidades para melhorar a documentação. Agradecemos antecipadamente por sua ajuda!

Tópicos



## Você está usando o Explorador de Recursos pela primeira vez?

Se você estiver usando o Explorador de Recursos pela primeira vez, recomendamos que comece lendo os seguintes tópicos na seção Conceitos básicos:

- Termos e conceitos do Explorador de Recursos
- Configurar o Explorador de Recursos usando a Configuração rápida

# Recursos do Explorador de Recursos

O Explorador de Recursos fornece os seguintes recursos:

- Os usuários podem pesquisar recursos em suas regiões Região da AWS ou em todas as suas Conta da AWS.
- Os usuários podem usar palavras-chave, operadores de pesquisa e atributos, como tags, para filtrar os resultados de pesquisa apenas para os recursos correspondentes.
- Quando os usuários encontram um recurso nos resultados da pesquisa, eles podem ir imediatamente para o console nativo do recurso para trabalhar com esse recurso.
- Os administradores podem criar visualizações que definem quais recursos estão disponíveis nos resultados de pesquisa. Os administradores podem criar diferentes visualizações para diferentes grupos de usuários com base em suas tarefas e conceder permissões para as visualizações apenas aos usuários que precisam delas.
- O Resource Explorer, como muitos outros Serviços da AWS, acaba sendo consistente. O Explorador de Recursos atinge alta disponibilidade replicando dados em vários servidores em datacenters da Amazon em todo o mundo. Se uma solicitação para alterar alguns dados for bem-sucedida, a alteração estará comprometida e armazenada com segurança. Porém, depois, a alteração deve ser replicada em todo o Explorador de Recursos, o que pode levar algum tempo. Por exemplo, isso acontece quando o Explorador de Recursos encontra um recurso em uma região e o replica na região que contém o índice agregador da conta.

# Regiões suportadas pelo Resource Explorer

| Nome da região | Região | Endpoint | Protocolo | |
|---|---|---|---|---|
| Leste dos EUA (Ohio) | us-east-2 | resource-explorer-2.us-east-2.amazonaws.com<br>resource-explorer-2-fips.us-east-2.amazonaws.com | HTTPS<br>HTTPS<br>HTTPS | |

| Nome da região | Região | Endpoint | Protocolo |
|---|---|---|---|
| | | resource-explorer-2-fips.us-east-2.api.aws | |
| Leste dos EUA (Norte da Virgínia) | us-east-1 | resource-explorer-2.us-east-1.amazonaws.com<br>resource-explorer-2-fips.us-east-1.amazonaws.com<br>resource-explorer-2-fips.us-east-1.api.aws | HTTPS<br>HTTPS<br>HTTPS |
| Oeste dos EUA (Norte da Califórnia) | us-west-1 | resource-explorer-2.us-west-1.amazonaws.com<br>resource-explorer-2-fips.us-west-1.amazonaws.com<br>resource-explorer-2-fips.us-west-1.api.aws | HTTPS<br>HTTPS<br>HTTPS |
| Oeste dos EUA (Oregon) | us-west-2 | resource-explorer-2.us-west-2.amazonaws.com<br>resource-explorer-2-fips.us-west-2.amazonaws.com<br>resource-explorer-2-fips.us-west-2.api.aws | HTTPS<br>HTTPS<br>HTTPS |
| África (Cidade do Cabo) | af-south-1 | resource-explorer-2.af-south-1.amazonaws.com | HTTPS |
| Ásia-Pacífico (Hong Kong) | ap-east-1 | resource-explorer-2.ap-east-1.amazonaws.com | HTTPS |
| Ásia-Pacífico (Hyderabad) | ap-south-2 | resource-explorer-2.ap-south-2.amazonaws.com | HTTPS |

| Nome da região | Região | Endpoint | Protocolo | |
|---|---|---|---|---|
| Ásia-Pacífico (Jacarta) | ap-southeast-3 | resource-explorer-2.ap-southeast-3.amazonaws.com | HTTPS | |
| Ásia-Pacífico (Melbourne) | ap-southeast-4 | resource-explorer-2.ap-southeast-4.amazonaws.com | HTTPS | |
| Ásia-Pacífico (Mumbai) | ap-south-1 | resource-explorer-2.ap-south-1.amazonaws.com | HTTPS | |
| Ásia-Pacífico (Osaka) | ap-northeast-3 | resource-explorer-2.ap-northeast-3.amazonaws.com | HTTPS | |
| Ásia-Pacífico (Seul) | ap-northeast-2 | resource-explorer-2.ap-northeast-2.amazonaws.com | HTTPS | |
| Ásia-Pacífico (Singapura) | ap-southeast-1 | resource-explorer-2.ap-southeast-1.amazonaws.com | HTTPS | |
| Ásia-Pacífico (Sydney) | ap-southeast-2 | resource-explorer-2.ap-southeast-2.amazonaws.com | HTTPS | |
| Ásia-Pacífico (Tóquio) | ap-northeast-1 | resource-explorer-2.ap-northeast-1.amazonaws.com | HTTPS | |

| Nome da região | Região | Endpoint | Protocolo |
|---|---|---|---|
| Canadá (Central) | ca-central-1 | resource-explorer-2.ca-central-1.amazonaws.com<br>resource-explorer-2-fips.ca-central-1.amazonaws.com<br>resource-explorer-2-fips.ca-central-1.api.aws | HTTPS<br>HTTPS<br>HTTPS |
| Oeste do Canadá (Calgary) | ca-west-1 | resource-explorer-2.ca-west-1.amazonaws.com<br>resource-explorer-2-fips.ca-west-1.amazonaws.com<br>resource-explorer-2-fips.ca-west-1.api.aws | HTTPS<br>HTTPS<br>HTTPS |
| Europa (Frankfurt) | eu-central-1 | resource-explorer-2.eu-central-1.amazonaws.com | HTTPS |
| Europa (Irlanda) | eu-west-1 | resource-explorer-2.eu-west-1.amazonaws.com | HTTPS |
| Europa (Londres) | eu-west-2 | resource-explorer-2.eu-west-2.amazonaws.com | HTTPS |
| Europa (Milão) | eu-south-1 | resource-explorer-2.eu-south-1.amazonaws.com | HTTPS |
| Europa (Paris) | eu-west-3 | resource-explorer-2.eu-west-3.amazonaws.com | HTTPS |
| Europa (Espanha) | eu-south-2 | resource-explorer-2.eu-south-2.amazonaws.com | HTTPS |
| Europa (Estocolmo) | eu-north-1 | resource-explorer-2.eu-north-1.amazonaws.com | HTTPS |

| Nome da região | Região | Endpoint | Protocolo |
|---|---|---|---|
| Europa (Zurique) | eu-central-2 | resource-explorer-2.eu-central-2.amazonaws.com | HTTPS |
| Israel (Tel Aviv) | il-central-1 | resource-explorer-2.il-central-1.amazonaws.com | HTTPS |
| Oriente Médio (Barém) | me-south-1 | resource-explorer-2.me-south-1.amazonaws.com | HTTPS |
| Oriente Médio (UAE) | me-central-1 | resource-explorer-2.me-central-1.amazonaws.com | HTTPS |
| América do Sul (São Paulo) | sa-east-1 | resource-explorer-2.sa-east-1.amazonaws.com | HTTPS |

# Relacionado Serviços da AWS

A seguir estão os outros Serviços da AWS cujo objetivo principal é ajudá-lo a gerenciar seus AWS recursos:

AWS Resource Access Manager (AWS RAM)

Compartilhe os recursos em um Conta da AWS com o outro Contas da AWS. Se sua conta for gerenciada por AWS Organizations, você poderá usar AWS RAM para compartilhar recursos com as contas em uma unidade organizacional ou com todas as contas da organização. Os recursos compartilhados funcionam para os usuários dessas contas da mesma forma que funcionariam se tivessem sido criados na conta local.

AWS Resource Groups

Crie grupos para seus AWS recursos. Depois, você pode usar e gerenciar cada grupo como uma unidade, em vez de ter que referenciar cada recurso individualmente. Seus grupos podem

consistir em recursos que fazem parte da mesma pilha do AWS CloudFormation ou que estão marcados com as mesmas tags. Alguns tipos de recursos também são compatíveis com a aplicação de uma configuração a um grupo de recursos para afetar todos os recursos relevantes do grupo.

Editor de tags e o AWS Resource Groups Tagging API

Tags são metadados definidos pelo cliente que você pode anexar aos recursos. Você pode categorizar os recursos para finalidades como alocação de custos e controle de acesso baseado em atributo.

# Definição de preço

Não há cobrança para pesquisar recursos usando Explorador de recursos da AWS, incluindo criar visualizações, ativar regiões ou pesquisar recursos. No processo de criação de seu inventário de recursos, o Resource Explorer liga APIs em seu nome, o que pode resultar em cobranças. A interação com os recursos encontrados nos resultados da pesquisa pode resultar em cobranças de uso que variam de acordo com o tipo de recurso e seu AWS service (Serviço da AWS). Para obter mais informações sobre AWS como as cobranças pelo uso normal de um tipo de recurso específico, consulte a documentação do serviço proprietário desse tipo de recurso.

# Conceitos básicos do Explorador de Recursos

Use os tópicos desta seção para obter uma compreensão básica dos conceitos e termos usados por Explorador de recursos da AWS. Saiba quais são os pré-requisitos que você deve atender para usar o Explorador de Recursos com sucesso e como ativar o Explorador de Recursos na sua Conta da AWS.

## Acessar o Explorador de Recursos

Você pode interagir com o Explorador de Recursos das seguintes maneiras:

Console do Explorador de Recursos

O Explorador de Recursos fornece uma interface de usuário na Web, o console do Explorador de Recursos. Se você se inscreveu em um Conta da AWS, você pode acessar o console do Resource Explorer entrando AWS Management Consolee escolhendo Resource Explorer na página inicial do console.

Você também pode usar o navegador para ir diretamente para a página Painel do Explorador de Recursos ou para a página Pesquisa de recursos. Se você ainda não fez login, será pedido que faça isso antes que o console seja exibido.

> **Note**
>
> O console Resource Explorer é um console global, o que significa que você não precisa selecionar um Região da AWS para trabalhar. Porém, quando você usa o Explorador de Recursos para criar um índice ou uma visualização, precisa especificar uma região para armazenar o índice ou a visualização. Ao usar o Explorador de Recursos para pesquisar, você pode escolher qualquer visualização a que tenha acesso. Os resultados vêm automaticamente da região associada à visualização selecionada. Se a visualização for da região que contém o índice agregador, os resultados incluirão recursos de todas as regiões nas quais você criou índices do Explorador de Recursos.

AWS Management Console pesquisa unificada

Na parte superior de cada página do AWS Management Console, há uma barra de pesquisa. Você pode configurar o Explorador de Recursos para participar da pesquisa unificada. Assim,

seus usuários podem usar a sintaxe de consulta de pesquisa do Explorador de Recursos na caixa de texto da pesquisa unificada e ver os recursos correspondentes nos resultados de pesquisa. Ao ativar esse recurso, os usuários podem pesquisar recursos no console de qualquer um AWS service (Serviço da AWS) sem precisar primeiro alternar para o console do Resource Explorer.

> **Important**
>
> A pesquisa unificada sempre pesquisa usando a visualização padrão na Região da AWS que contém o índice agregador.

Comandos do Resource Explorer no AWS CLI e Ferramentas para Windows PowerShell

As ferramentas AWS CLI e para PowerShell fornecer acesso direto às API operações públicas do Resource Explorer. Essas ferramentas funcionam no Windows, no macOS e no Linux. Para obter mais informações sobre os conceitos básicos, consulte o Guia do usuário da AWS Command Line Interface ou o Guia do usuário do AWS Tools for Windows PowerShell. Para obter mais informações sobre os comandos para o Explorador de Recursos, consulte a AWS CLI Command Reference ou a AWS Tools for Windows PowerShell Cmdlet Reference.

Operações do Resource Explorer no AWS SDKs

AWS fornece API comandos para um amplo conjunto de linguagens de programação. Para obter mais informações sobre os conceitos básicos, consulte Usando Explorador de recursos da AWS com um AWS SDK.

Consulta API

Se você não usa uma das linguagens de programação suportadas, a Resource Explorer HTTPS Query API fornece acesso programático ao Resource Explorer. Com o Resource ExplorerAPI, você pode emitir HTTPS solicitações diretamente para o serviço. Ao usar o Resource ExplorerAPI, você deve incluir um código que possa assinar digitalmente suas solicitações usando suas AWS credenciais. Para obter mais informações, consulte a Explorador de recursos da AWS APIReferência.

# Termos e conceitos do Explorador de Recursos

O Explorador de recursos da AWS é um serviço de pesquisa e descoberta de recursos. Com o Explorador de Recursos, você pode explorar os recursos usando uma experiência semelhante à

do mecanismo de pesquisa na Internet. Você pode pesquisar seus recursos, como instâncias do Amazon Elastic Compute Cloud, fluxos do Amazon Kinesis ou tabelas do Amazon DynamoDB, usando os metadados dos recursos, como nomes, tags e IDs. O Explorador de Recursos funciona entre Regiões da AWS na sua conta para simplificar as workloads inter-regionais.

O Explorador de Recursos fornece respostas rápidas às suas consultas de pesquisa usando índices criados e mantidos pelo serviço Explorador de recursos da AWS. O Explorador de Recursos usa várias fontes de dados para coletar informações sobre os recursos na sua Conta da AWS. O Explorador de Recursos armazena essas informações nos índices para o Explorador de Recursos pesquisar.

Você deve entender os conceitos a seguir para administrar e configurar corretamente o Explorador de recursos da AWS para os usuários.

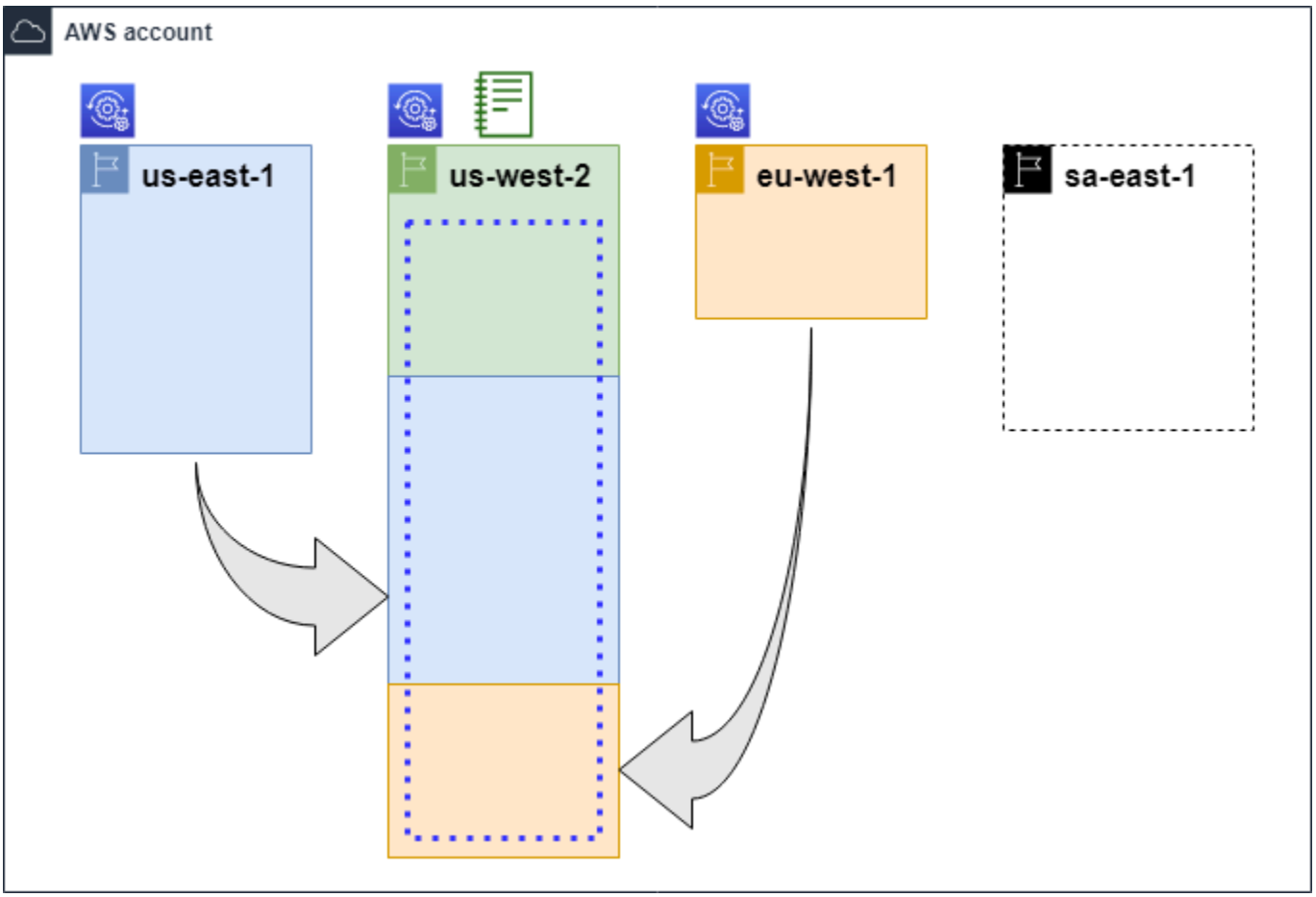
Conceitos

- Administrador do Explorador de Recursos
- Usuário do Explorador de Recursos
- Índice
- Visão
- Recurso
- Pesquisa unificada no AWS Management Console
- Pesquisa em várias contas

O diagrama a seguir mostra três Regiões da AWS em que o administrador ativou o Explorador de Recursos e uma região em que o administrador preferiu não ativá-lo. A região em que o Explorador de Recursos não está ativado não tem índice. Portanto, os recursos dessa região não podem ser pesquisados pelas consultas do Explorador de Recursos.

Neste exemplo de cenário, o administrador escolheu a região Oeste dos EUA (Oregon) (`us-west-2`) para conter o índice agregador da conta. Todas as regiões que você ativa replicam seus índices locais na região que tem o índice agregador.

A visualização padrão criada pelo Explorador de Recursos não tem filtros. Portanto, os resultados obtidos pesquisando com essa visualização podem incluir recursos de qualquer tipo em todas as regiões na conta em que o Explorador de Recursos está ativado.




| Legenda | |
|---|---|
| | O Explorador de Recursos está ativado nessa Região da AWS e as informações sobre os recursos da região estão armazenadas em um índice local na região. O índice local de cada região também é replicado (indicado pelas setas) na região que contém o índice agregador. |
| | O índice nessa Região da AWS está configurado para ser o índice agregador da conta. O Explorador de Recursos replica, no índice agregador dessa região, as informaçõ es dos recursos coletadas nos índices locais de todas as outras regiões em que o Explorador de Recursos está ativado. As pesquisas feitas nessa região podem incluir resultados de todas as regiões na conta. |
| | A visualização padrão criada pela Configuração rápida inclui todos os recursos em todas as Regiões da AWS. |

# Administrador do Explorador de Recursos

Um administrador do Explorador de Recursos é uma entidade principal do AWS Identity and Access Management (IAM) que tem permissão para gerenciar o Explorador de Recursos e suas configurações na Conta da AWS . O administrador do Explorador de Recursos pode configurar os seguintes atributos:

- Ativar o Explorador de Recursos para Regiões da AWS individuais na Conta da AWS criando índices nessas regiões. Isso permite que o Explorador de Recursos descubra os recursos e preencha o índice com informações sobre esses recursos para que os usuários possam pesquisar recursos nessa região.
- Atualizar o tipo de índice em uma Região da AWS para torná-lo o índice agregador para a Conta da AWS. O índice agregador nessa região recebe cópias replicadas das informações dos recursos de todas as outras regiões na conta em que o Explorador de Recursos está ativado.
- Criar visualizações que definem o subconjunto de informações indexadas que os usuários podem pesquisar e descobrir no Explorador de Recursos.
- Embora não faça parte das ações do Explorador de Recursos, o administrador do Explorador de Recursos também deve poder conceder permissões de pesquisa às entidades principais na conta. O administrador pode conceder essas permissões às entidades principais adicionando as permissões relevantes às políticas de permissão do IAM existentes ou usando a política somente leitura gerenciada pela AWS do Explorador de Recursos.

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

  - Usuários e grupos no AWS IAM Identity Center:

    Crie um conjunto de permissões. Siga as instruções em Create a permission set (Criação de um conjunto de permissões) no Guia do usuário do AWS IAM Identity Center.
  - Usuários gerenciados no IAM com provedor de identidades:

    Crie um perfil para a federação de identidades. Siga as instruções em Criar um perfil para um provedor de identidades de terceiros (federação) no Guia do usuário do IAM.
  - Usuários do IAM:
    - Crie um perfil que seu usuário possa assumir. Siga as instruções em Creating a role for an IAM user (Criação de um perfil para um usuário do IAM) no Guia do usuário do IAM.

- (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

O administrador normalmente tem todas as permissões do Explorador de Recursos (`resource-explorer-2:*`) em todos os recursos do Explorador de Recursos, incluindo os índices e as visualizações. Essas permissões podem ser concedidas usando a política de acesso total do Explorador de Recursos gerenciada pela AWS.

## Usuário do Explorador de Recursos

Um usuário do Explorador de Recursos é uma entidade principal do IAM que tem permissão para fazer uma ou mais das seguintes tarefas:

- Realizar uma pesquisa de recursos usando uma visualização para consultar o Explorador de Recursos. Um usuário do Explorador de Recursos deseja descobrir e encontrar recursos da AWS e normalmente usa o console do Explorador de Recursos ou as operações `Search` do Explorador de Recursos fornecidas pelos SDKs da AWS ou pela AWS CLI.

  Um perfil ou usuário pode usar a permissão de get do IAM para pesquisar com um de dois métodos:

  - A política somente leitura gerenciada pela AWS do Explorador de Recursos para o perfil, grupo ou usuário do IAM.
  - Uma política de permissão do IAM com uma instrução contendo as permissões mínimas a seguir para o perfil, o grupo ou o usuário do IAM.

    ```
    {
        "Effect": "Allow",
        "Action": [
            "resource-explorer-2:Search",
            "resource-explorer-2:GetView",
        "Resource": "<ARN of the view>"
    }
    ```

- Embora normalmente seja considerada uma tarefa do administrador, você pode delegar a usuários confiáveis a capacidade de definir e criar visualizações. Para fazer isso, o administrador pode conceder permissão para chamar a operação `resource-explorer-2:CreateView` em uma política de permissão do IAM anexada aos perfis, grupos ou usuários relevantes. Se a visualização

exigir permissões específicas, faça uma provisão para adicionar ou modificar as políticas do IAM para os usuários relevantes.

Veja informações sobre como pesquisar recursos usando o Explorador de Recursos em Usar o Explorador de recursos da AWS para pesquisar recursos.

## Índice

Um índice é um conjunto de informações mantidas pelo Explorador de Recursos sobre todos os recursos da AWS em uma Região da AWS na sua Conta da AWS. O Explorador de Recursos mantém um índice em cada região em que você ativa o Explorador de Recursos. O Explorador de Recursos atualiza o índice automaticamente quando você cria ou exclui recursos na sua Conta da AWS. No diagrama anterior, as caixas abaixo dos nomes das Região da AWS representam os índices do Explorador de Recursos mantidos em cada Região da AWS. O índice em uma região é a fonte de informações para todas as visualizações criadas nessa região. Os usuários não podem consultar o índice diretamente. Em vez disso, eles devem consultar sempre usando uma visualização.

Existem dois tipos de índices:

Índice local

Existe um índice local em cada Região da AWS em que você ativa o Explorador de Recursos. Um índice local só contém informações sobre recursos na mesma região.

Índice agregador

O administrador do Explorador de Recursos também pode designar o índice em uma Região da AWS como o índice agregador da Conta da AWS. O índice agregador recebe e armazena uma cópia do índice para todas as outras regiões em que o Explorador de Recursos está ativado na conta. O índice agregador também recebe e armazena informações sobre os recursos em sua própria região. No diagrama anterior, a região `us-west-2` contém o índice agregador da conta. O principal motivo para designar um índice agregador para a conta é poder criar visualizações que possam incluir os recursos de todas as regiões na conta. Só pode haver um índice agregador em uma Conta da AWS.

Ao ativar o Explorador de Recursos, você pode especificar qual Região da AWS deve conter o índice do agregador. Você também pode alterar a Região da AWS usada para o índice agregador posteriormente. Para obter informações sobre como promover um índice local para torná-lo o

índice agregador de sua própria Conta da AWS, consulte Ativar a pesquisa inter-regional criando um índice agregador.

Um índice é um recurso com um nome do recurso da Amazon (ARN). Porém, você só pode usar esse ARN em políticas de permissão para conceder acesso às operações que interagem diretamente com o índice. Com essas operações, você pode criar visualizações e defini-las como padrão em uma região, ativar ou desativar o Explorador de Recursos em uma região e criar um índice agregador para a conta. O ARN de um índice é semelhante ao seguinte exemplo:

```
arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

## Visão

Uma visualização é o mecanismo usado para consultar os recursos listados em um índice. A visualização define quais informações do índice estão visíveis e disponíveis para pesquisa e descoberta. Um usuário nunca consulta diretamente o índice do Explorador de Recursos. Em vez disso, as consultas devem sempre passar por uma visualização que permita ao criador da visualização limitar quais recursos o usuário pode ver nos resultados de pesquisa.

Ao criar uma visualização, você especifica filtros que restringem quais recursos serão incluídos nos resultados de pesquisa. Por exemplo, você poderia escolher incluir somente os recursos de alguns tipos especificados que são usados pelas pessoas a quem você concede acesso a essa visualização. Os resultados das consultas que os usuários fazem com uma visualização são sempre filtrados automaticamente para incluir apenas os recursos que correspondem aos critérios da visualização.

Para conceder acesso ao uso de uma visualização, você pode atribuir permissões usando um dos métodos a seguir.

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

- Usuários e grupos no AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Create a permission set (Criação de um conjunto de permissões) no Guia do usuário do AWS IAM Identity Center.
- Usuários gerenciados no IAM com provedor de identidades:

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

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

Conceda permissão para que seus perfis, grupos ou usuários possam invocar as operações `resource-explorer-2:GetView` e `resource-explorer-2:Search` em uma visualização identificada pelo nome do recurso da Amazon (ARN). Como alternativa, você pode usar a política somente leitura gerenciada pela AWS do Explorador de Recursos para todas as entidades principais que precisam usar a visualização para pesquisar. Você pode criar várias visualizações com filtros e escopos diferentes e, assim, retornar diferentes subconjuntos de informações sobre os recursos. Depois, você pode conceder permissões para cada visualização aos usuários que precisam ver as informações incluídas nos resultados dessa visualização.

Para pesquisar com o Explorador de Recursos, cada usuário deve ter permissão para usar pelo menos uma visualização. Não é possível fazer uma pesquisa no Explorador de Recursos sem usar uma visualização.

As visualizações são armazenadas por região. Uma visualização só pode acessar o índice do Explorador de Recursos nessa Região da AWS. Para acessar resultados de pesquisa de toda a conta, você deve usar uma visualização na região que contém o índice agregador da conta. A opção Configuração rápida cria uma visualização padrão na Região da AWS com o índice agregador e com filtros que incluem todos os recursos em todas as Regiões da AWS usadas pela conta.

Para obter informações sobre como criar visualizações, consulte Gerenciar visualizações do Explorador de Recursos para fornecer acesso para pesquisa. Veja informações sobre como usar visualizações em uma consulta em Usar o Explorador de recursos da AWS para pesquisar recursos.

Toda visualização tem um nome do recurso da Amazon (ARN) que você pode referenciar nas políticas de permissão para conceder acesso a visualizações individuais. Você também pode passar o ARN de uma visualização como parâmetro para qualquer API ou operação da AWS CLI que interaja com uma visualização. O ARN de uma visualização é semelhante ao exemplo a seguir.

```
arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-View-
Name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

> **Note**
>
> Todo ARN de visualização inclui no final um UUID gerado pela AWS. Isso ajuda a garantir que os usuários que talvez tenham tido acesso a visualizações com um nome específico que foi excluído não possam acessar automaticamente uma nova visualização criada com o mesmo nome.

## Recurso

Um recurso é uma entidade na AWS com a qual você pode trabalhar. Os recursos são criados pela Serviços da AWS à medida que você usa os recursos do serviço. Os exemplos incluem uma instância do Amazon EC2, um bucket do Amazon S3 ou uma pilha do AWS CloudFormation. Alguns tipos de recursos podem conter dados de clientes. Todos os tipos de recursos têm atributos ou metadados para descrever o recurso, incluindo um nome, uma descrição e o nome do recurso da Amazon (ARN) que você usa para referenciá-lo de modo exclusivo. A maioria dos tipos de recursos também é compatível com tags. As tags são metadados personalizados que você pode anexar aos recursos com diversas finalidades, como alocação de custos no faturamento, autorização de segurança usando controle de acesso baseado em atributo ou para atender a outras necessidades de categorização.

O objetivo principal do Explorador de Recursos é ajudá-lo a encontrar os recursos que existem na sua Conta da AWS. O Explorador de Recursos usa várias técnicas para descobrir todos os seus recursos e colocar informações sobre eles em um índice. Depois, você pode consultar o índice por meio de qualquer visualização que seu administrador disponibilize para você.

> **Important**
>
> O Explorador de Recursos exclui intencionalmente os tipos de recursos cuja inclusão exporia os dados do cliente. Os tipos de recursos a seguir não são indexados pelo Explorador de Recursos e, portanto, nunca são retornados nos resultados de pesquisa.
>
> - Objetos do Amazon S3 que estão contidos dentro de um bucket
> - Itens de tabelas do Amazon DynamoDB

- Valores de atributos do DynamoDB

## Pesquisa unificada no AWS Management Console

Na parte superior do AWS Management Console, em todo AWS service (Serviço da AWS), existe uma barra de pesquisa que você pode usar para pesquisar vários itens relacionados à AWS. Você pode pesquisar serviços e recursos, e obter links diretamente para a página relevante no console do serviço. Você também pode pesquisar documentação e artigos de blogs relacionados ao termo da pesquisa.

Depois de ativar o Explorador de Recursos e criar um índice agregador e uma visualização padrão, a pesquisa unificada também pode incluir os recursos da sua conta nos resultados da pesquisa. A pesquisa unificada usa automaticamente a visualização padrão na Região da AWS que contém o índice agregador da conta. Isso permite pesquisar um recurso de qualquer página noAWS Management Console, sem precisar primeiro abrir o Explorador de Recursos. Se você não promover um índice local para ser o índice agregador da conta ou não criar uma visualização padrão na região do índice agregador, a pesquisa unificada não incluirá nenhum recurso em seus resultados. Além disso, qualquer entidade principal que faça uma pesquisa deve ter permissão para usar a visualização padrão na região que contém o índice agregador, ou a pesquisa unificada não incluirá nenhum recurso em seus resultados.

> **Important**
>
> A pesquisa unificada insere automaticamente um operador de caractere curinga (*) no final da primeira palavra-chave da string. Isso significa que os resultados da pesquisa unificada incluem os recursos que correspondem a qualquer string que comece com a palavra-chave especificada.
> A pesquisa realizada pela caixa de texto Consulta na página Pesquisa de recursos no console do Explorador de Recursos não adiciona automaticamente um caractere curinga. Você pode inserir um * manualmente depois de qualquer termo na string de pesquisa.

Veja mais informações sobre a pesquisa unificada e sua integração com o Explorador de Recursos em Usar a pesquisa unificada no AWS Management Console.

## Pesquisa em várias contas

Com a pesquisa em várias contas, você pode pesquisar e descobrir recursos no AWS Organizations e nas Regiões da AWS com uma única pesquisa de palavra-chave.

Veja mais informações sobre a pesquisa em várias contas e como habilitá-la para o Explorador de Recursos, em Ativar a pesquisa em várias contas.

# Pré-requisitos para usar o Explorador de Recursos

Antes de usar Explorador de recursos da AWS pela primeira vez, conclua as tarefas a seguir conforme necessário.

Tarefas

- Inscreva-se para um Conta da AWS
- Criar um usuário com acesso administrativo

## Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário raiz tem acesso a todos os Serviços da AWS e atributos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo Minha conta.

# Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, insira sua senha.

   Para obter ajuda ao fazer login usando o usuário raiz, consulte Fazer login como usuário raiz no Guia do usuário do Início de Sessão da AWS .
2. Ative a autenticação multifator (MFA) para seu usuário root.

   Para obter instruções, consulte Habilitar um MFA dispositivo virtual para seu usuário Conta da AWS root (console) no Guia IAM do usuário.

Criar um usuário com acesso administrativo

1. Ative o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No IAM Identity Center, conceda acesso administrativo a um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para entrar com seu usuário do IAM Identity Center, use o login URL que foi enviado ao seu endereço de e-mail quando você criou o usuário do IAM Identity Center.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No IAM Identity Center, crie um conjunto de permissões que siga as melhores práticas de aplicação de permissões com privilégios mínimos.

   Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Add groups no Guia do usuário do AWS IAM Identity Center .

# Instalar e configurar o Explorador de Recursos

Antes de poder instalar e configurar Explorador de recursos da AWS, primeiro verifique se você atende aos pré-requisitos. Depois disso, entre como uma IAM função ou usuário que tenha as permissões necessárias para realizar as operações do Resource Explorer para o procedimento a seguir.

Você pode usar esse procedimento de instalação e configuração para configurar o Resource Explorer em contas existentes e em qualquer nova conta adicionada à sua organização.

Há duas maneiras de configurar o Explorador de Recursos:

- Configuração Rápida
- Configuração avançada

> **Important**
>
> Se você optar por configurar o Resource Explorer usando qualquer opção que diga “tudo Regiões da AWS“, ele ativará somente aquelas Regiões da AWS que existem e que estão habilitadas no Conta da AWS momento em que você executa o procedimento. O Resource Explorer não é ativado automaticamente em nenhum Regiões da AWS que seja AWS adicionado no futuro. Ao AWS introduzir uma nova região, você pode optar por ativar o Resource Explorer na região manualmente quando ele aparecer na página Configurações do console do Resource Explorer ou chamando a CreateIndexoperação.

> **Note**
>
> A configuração do Explorador de Recursos também pode ativar a capacidade de pesquisar recursos usando a barra de pesquisa unificada no AWS Management Console. Para que os usuários vejam os recursos nos resultados da pesquisa unificada, você deve configurar o Explorador de Recursos com um índice agregador inter-regiões e uma visualização padrão. Veja os detalhes no procedimento a seguir. Você também deve garantir que os usuários que estão pesquisando tenham permissão para usar a visualização padrão na Região da AWS que contém o índice agregador. Para obter mais informações, consulte Usar a pesquisa unificada no AWS Management Console.

## Configurar o Explorador de Recursos usando a Configuração rápida

Se você escolher a opção Configuração rápida, o Explorador de Recursos fará o seguinte:

- Cria um índice Região da AWS em cada um dos seus Conta da AWS.
- Atualizará o índice na região que você especificar para ser o índice agregador para a conta.
- Criará uma visualização padrão na região do índice agregador. Essa visualização não terá filtros, portanto, retornará todos os recursos encontrados no índice.

### Permissões mínimas

Para realizar as etapas do procedimento a seguir, você deve ter as seguintes permissões:

- Ação: `resource-explorer-2:*` - Recurso: nenhum recurso específico (`*`)
- Ação: `iam:CreateServiceLinkedRole` - Recurso: nenhum recurso específico (`*`)

### AWS Management Console

Para configurar o Explorador de Recursos usando a Configuração rápida

1. Abra o console do Explorador de recursos da AWS em https://console.aws.amazon.com/resource-explorer.
2. Escolha Ativar o Explorador de Recursos.
3. Na página Ativar o Explorador de Recursos, escolha Configuração rápida.

4. Escolha qual Região da AWS você deseja que contenha o índice agregador. Você deve selecionar a região apropriada para a localização geográfica dos usuários.
5. Na parte inferior da página, selecione Ativar o Explorador de Recursos.
6. Na página Progresso, você pode monitorar cada Região da AWS enquanto o Explorador de Recursos cria seu índice. A página exibe o status da criação do índice agregador e da visualização padrão.

Depois que todas as etapas mostrarem que foram concluídas com êxito, você e os usuários poderão navegar até a página Pesquisa de recursos e começar a pesquisar os recursos.

> **Note**
>
> Os recursos marcados locais para o índice aparecem nos resultados de pesquisa em poucos minutos. Os recursos não marcados normalmente levam menos de duas horas para aparecer, mas podem levar mais tempo quando há muita demanda. A replicação inicial de todos os índices locais existentes em um novo índice agregador também pode levar até uma hora.

Próximas etapas: antes que os usuários possam pesquisar com a visualização padrão que você acabou de criar, será necessário conceder a eles permissões para fazê-lo. Para obter mais informações, consulte Conceder acesso às visualizações do Explorador de Recursos para pesquisa.

AWS CLI

Configurar o Resource Explorer no seu Conta da AWS usando o AWS CLI é, por definição, equivalente à opção de configuração avançada. Isso ocorre porque as CLI operações do Resource Explorer não executam nenhuma das etapas automaticamente como o console do Resource Explorer. Consulte a AWS CLI guia no Configurar o Explorador de Recursos usando a Configuração avançada para ver quais comandos são equivalentes ao uso do console.

## Configurar o Explorador de Recursos usando a Configuração avançada

Se você escolher a opção Configuração avançada, poderá fazer o seguinte:

- Escolha o Regiões da AWS em que ativar o Resource Explorer.

- Escolher se deseja configurar uma região com um índice agregador. Se você fizer isso, você especifica o Região da AWS para colocá-lo. Esse índice permite que você crie visualizações que podem incluir recursos de todas as regiões da conta. Para obter mais informações, consulte Ativar a pesquisa inter-regiões criando um índice agregador.
- Escolher se deseja criar uma visualização padrão. Essa visualização permite pesquisar automaticamente qualquer AWS recurso nas regiões nas quais você ativa o Resource Explorer. Você deve garantir que todas as entidades principais que precisarem usar a visualização padrão para pesquisar no Explorador de Recursos tenham permissões na visualização. Para obter mais informações, consulte Conceder acesso às visualizações do Explorador de Recursos para pesquisa.

> **Note**
>
> Você pode configurar o Explorador de Recursos para incluir seus recursos nos resultados de pesquisa fornecidos pelo atributo de pesquisa unificada no AWS Management Console. Para ativar esse atributo, você deve configurar o Explorador de Recursos com um índice agregador e uma visualização padrão que todos os perfis e usuários possam usar ao pesquisar. A opção Configuração rápida cria ambos, o índice agregador e a visualização padrão, e é como recomendamos que você ative o Explorador de Recursos.

Permissões mínimas

Para realizar as etapas do procedimento a seguir, você deve ter as seguintes permissões:

- Ação: `resource-explorer-2:*` - Recurso: nenhum recurso específico (*)
- Ação: `iam:CreateServiceLinkedRole` - Recurso: nenhum recurso específico (*)

AWS Management Console

Para ativar o Explorador de Recursos usando a Configuração avançada

1. Abra o console do Explorador de recursos da AWS em https://console.aws.amazon.com/resource-explorer.
2. Escolha Ativar o Explorador de Recursos.
3. Na página Ativar o Explorador de Recursos, escolha Configuração avançada.

4. Na Regiões da AWScaixa, em Regiões, escolha se você deseja ativar o Explorador de Recursos em todas Regiões da AWS ou somente regiões específicas.

   Se você escolher Ativar o Explorador de Recursos apenas nas Regiões da AWS especificadas nessa conta, selecione todas as regiões cujos recursos você deseja incluir nos resultados da pesquisa.

5. Em Índice agregador, escolha se você deseja criar um índice agregador. Se você optar por criar um índice agregador, todos os outros Regiões da AWS replicarão seus índices para essa região. Isso permite que os usuários pesquisem recursos em todas as regiões selecionadas no Conta da AWS. Escolha o Região da AWS que contém o índice agregador. Recomendamos que você especifique a região em que os usuários passam a maior parte do tempo ou, pelo menos, onde você espera que eles realizem a maior parte de suas pesquisas de recursos.

6. Na caixa Visualização padrão, em Criação de visualização, escolha se uma visualização padrão deve ser criada. Essa opção só estará disponível se você criar um índice agregador. Se você optar por criar uma exibição padrão, o Resource Explorer colocará essa exibição no Região da AWS mesmo índice do agregador. Isso permite que a exibição padrão inclua resultados de tudo Regiões da AWS em que você registrou o Resource Explorer. Sempre que um usuário realiza uma pesquisa em uma região com uma visualização padrão e não especifica explicitamente uma visualização, a pesquisa usa a visualização padrão daquela região.

   > **Note**
   >
   > Antes que os usuários possam pesquisar com uma visualização, você deve conceder a eles permissões para usar essa visualização. Para obter mais informações, consulte Conceder acesso às visualizações do Explorador de Recursos para pesquisa.

7. Escolha Ativar Explorador de Recursos.

   > **Note**
   >
   > Os recursos marcados locais para o índice aparecem nos resultados de pesquisa em poucos minutos. Os recursos não marcados normalmente levam menos de duas horas para aparecer, mas podem levar mais tempo quando há muita demanda. A

replicação inicial de todos os índices locais existentes em um novo índice agregador também pode levar até uma hora.

AWS CLI

Para configurar o Explorador de Recursos usando a Configuração avançada

O console do Resource Explorer API executa várias chamadas de operação em seu nome com base nas escolhas que você faz. Os exemplos de AWS CLI comandos a seguir ilustram como realizar os mesmos procedimentos básicos fora do console usando o. AWS CLI

Example Etapa 1: ativar o Explorador de Recursos criando índices na Regiões da AWS desejada

Execute o comando a seguir Região da AWS em cada um dos quais você deseja ativar o Resource Explorer. O exemplo de comando a seguir ativa o Explorador de Recursos na Região da AWS que é padrão para a AWS CLI.

```
$ aws resource-explorer-2 create-index
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-27T16:17:12.130000+00:00",
    "State": "CREATING"
}
```

Example Etapa 2: atualize o índice em um Região da AWS para ser o índice agregador da conta

Execute o comando a seguir Região da AWS no qual você deseja que o Resource Explorer atualize o índice local para o índice agregador da conta. O exemplo de comando a seguir atualiza o índice agregador na região Leste dos EUA (Norte da Virgínia) (`us-east-1`).

```
$ aws resource-explorer-2 update-index-type \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --type AGGREGATOR
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "LastUpdatedAt": "2022-07-27T16:29:49.231000+00:00",
    "State": "UPDATING",
```

```
    "Type": "AGGREGATOR"
}
```

Example Etapa 3: criar uma visualização no Região da AWS que contenha o índice agregador

Execute o comando a seguir Região da AWS no qual você criou o índice agregador. O exemplo de comando a seguir cria uma visualização idêntica à criada pelo processo de configuração do console do Explorador de Recursos. Essa nova visualização inclui as tags anexadas ao recurso como parte das informações indexadas e permite a pesquisa de recursos por chave ou valor de tag.

```
$ aws resource-explorer-2 create-view \
    --view-name My-New-View \
    --included-properties Name=tags
{
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [
            {
                "Name": "tags"
            }
        ],
        "LastUpdatedAt": "2022-07-27T16:34:14.960000+00:00",
        "Owner": "123456789012",
        "Scope": "arn:aws:iam::123456789012:root",
        "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-New-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222"
    }
}
```

Example Etapa 4: defina sua nova visualização como padrão para sua Região da AWS

O exemplo a seguir define a visualização que você criou na etapa anterior como padrão para a região. Você deve executar o comando a seguir no mesmo Região da AWS em que criou a exibição padrão.

```
$ aws resource-explorer-2 associate-default-view \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-New-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
{
```

```
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-New-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
}
```

Antes que os usuários possam pesquisar com uma visualização, você deve conceder a eles permissões para usar essa visualização. Para obter mais informações, consulte Conceder acesso às visualizações do Explorador de Recursos para pesquisa.

Depois de executar esses comandos, o Explorador de Recursos é executado nas regiões especificadas na sua Conta da AWS. O Explorador de Recursos cria e mantém um índice em cada região com os detalhes dos recursos nela localizados. O Explorador de Recursos replica todos os índices individuais de região no índice agregador na região especificada. Essa região também contém uma visualização que permite que qualquer IAM função ou usuário na conta pesquise recursos em todas as regiões indexadas.

> **Note**
>
> Os recursos marcados locais para o índice aparecem nos resultados de pesquisa em poucos minutos. Os recursos não marcados normalmente levam menos de duas horas para aparecer, mas podem levar mais tempo quando há muita demanda. A replicação inicial de todos os índices locais existentes em um novo índice agregador também pode levar até uma hora.

# Identifique quais Regiões da AWS têm o Resource Explorer ativado

Você pode identificar quais Regiões da AWS foram Explorador de recursos da AWS ativados verificando se a região contém um índice para o Resource Explorer. Para ver quais regiões têm um índice, use os procedimentos desta página.

> **Important**
>
> Os usuários só podem pesquisar recursos nas regiões que têm o Explorador de Recursos ativado. Você também pode criar um índice agregador em uma região para possibilitar a pesquisa de recursos em todas as regiões. O Explorador de Recursos replica, na região com o índice agregador, as informações dos recursos de todas as outras regiões que contêm um índice do Explorador de Recursos. Os usuários não podem usar o Explorador de Recursos para descobrir recursos em regiões que não têm um índice.

## Verificar o status do Explorador de Recursos em uma região

Você pode verificar quais regiões têm índices para o Resource Explorer usando o AWS Management Console, usando comandos no AWS Command Line Interface (AWS CLI) ou usando API operações em um AWS SDK.

AWS Management Console

Para verificar quais regiões têm índices para o Explorador de Recursos

1. Abra a página Configurações no Explorador de Recursos.
2. A lista na seção Índices inclui somente as regiões que contêm um índice do Explorador de Recursos. O valor na coluna Tipo indica se o índice é local para a sua região ou o índice agregador para a Conta da AWS.
3. Para ver quais regiões não contêm um Explorador de Recursos, escolha Criar índices. Se uma região não estiver presente, isso significará que ela não contém o Explorador de Recursos.

AWS CLI

Para verificar quais regiões têm índices para o Explorador de Recursos

Execute o comando a seguir para ver quais Regiões da AWS têm índices para o Resource Explorer.

```
$ aws resource-explorer-2 list-indexes
{
    "Indexes": [
        {
            "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
            "Region": "us-east-1",
            "Type": "AGGREGATOR"
        },
        {
            "Arn": "arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222",
            "Region":"us-west-2",
            "Type":"LOCAL"
        }
    ]
}
```

# Ativando o Resource Explorer em um Região da AWS para indexar seus recursos

Ao ativar Explorador de recursos da AWS inicialmente o seu Conta da AWS, você criou índices para o serviço em um ou mais Regiões da AWS. Se você usou a opção Configuração rápida, o Explorador de Recursos criou os índices automaticamente em todas as Regiões da AWS que estão ativadas na sua Conta da AWS. O serviço Explorador de Recursos também promoveu o índice na região especificada para ser o índice agregador da conta. Se usou a opção Configuração avançada, você especificou as regiões nas quais criar os índices.

Tópicos

- Criar um índice do Explorador de Recursos em uma região
- Considerações sobre regiões AWS opcionais

Quando você ativa o Resource Explorer em um Região da AWS, o serviço executa as seguintes ações:

- Quando você inicia o Resource Explorer na primeira região de um Conta da AWS, o Resource Explorer cria uma função vinculada ao serviço na conta chamada. `AWSServiceRoleForResourceExplorer` Esse perfil concede permissões para o Explorador de Recursos descobrir e indexar os recursos na sua conta usando serviços como o AWS CloudTrail e o serviço de marcação. A criação da função vinculada ao serviço acontece somente quando você registra a primeira Região da AWS na conta. O Explorador de Recursos usa o mesmo perfil vinculado ao serviço para todas as regiões adicionadas posteriormente.
- O Explorador de Recursos cria um índice na região especificada para armazenar os detalhes dos recursos dessa região.
- O Explorador de Recursos começa a descobrir os recursos na região especificada e adiciona as informações encontradas sobre eles ao índice dessa região.
- Se sua conta já contiver um índice agregador em outra região, o Explorador de Recursos começará a replicar as informações do índice da nova região no índice agregador para possibilitar a pesquisa inter-regiões.

Quando essas etapas são concluídas, as informações sobre os recursos ficam disponíveis para serem descobertas pelos usuários. Eles podem pesquisar usando uma das visualizações definidas na mesma região ou na região que contém o índice agregador.

# Criar um índice do Explorador de Recursos em uma região

Você pode criar um índice do Resource Explorer em um adicional Região da AWS usando o AWS Management Console, usando comandos no AWS Command Line Interface (AWS CLI) ou usando API operações em um AWS SDK. Você não pode criar mais de um índice em uma região.

Permissões mínimas

Para realizar as etapas do procedimento a seguir, você deve ter as seguintes permissões:

- Ação: `resource-explorer-2:*` - Recurso: nenhum recurso específico (*)
- Ação: `iam:CreateServiceLinkedRole` - Recurso: nenhum recurso específico (*)

AWS Management Console

Para criar um índice do Resource Explorer em um Região da AWS

1. Na página Configurações do Explorador de Recursos.
2. Na seção Índices, escolha Criar índices.
3. Na página Criar índices, marque as caixas de seleção ao lado das Regiões da AWS quais você deseja criar um índice para apoiar a pesquisa dos recursos dessa região. Caixas de seleção indisponíveis indicam regiões que já contêm um índice do Explorador de Recursos.
4. (Opcional) Na seção Tags, você pode especificar pares de chave e valor de tag para o índice.
5. Escolha Criar índice.

   O Explorador de Recursos exibe um banner verde na parte superior da página para indicar sucesso ou um banner vermelho se ocorrer um erro ao criar um índice em uma ou mais das regiões selecionadas.

   > **Note**
   >
   > Os recursos marcados locais para o índice aparecem nos resultados de pesquisa em poucos minutos. Os recursos não marcados normalmente levam menos de duas

horas para aparecer, mas podem levar mais tempo quando há muita demanda. A replicação inicial de todos os índices locais existentes em um novo índice agregador também pode levar até uma hora.

Próxima etapa: se você já criou um índice agregador, as novas regiões começarão automaticamente a replicar suas informações de índice no índice agregador. Se os usuários fizerem ali todas as pesquisas, os recursos na nova região aparecerão nesses resultados de pesquisa e pronto.

Porém, se quiser que os usuários possam pesquisar recursos apenas na região recém-indexada, você deverá criar também uma visualização para os usuários nessa região e conceder a eles permissões para essa visualização. Para obter instruções sobre como criar uma visualização, consulte Gerenciar visualizações do Explorador de Recursos para fornecer acesso para pesquisa.

AWS CLI

Para criar um índice do Resource Explorer em um Região da AWS

Execute o comando a seguir para cada um Região da AWS em que você deseja criar um índice para apoiar a pesquisa dos recursos dessa região. O exemplo de comando a seguir registra o Explorador de Recursos na região Leste dos EUA (Norte da Virgínia) (`us-east-1`).

```
$ aws resource-explorer-2 create-index \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-11-01T20:00:59.149Z",
    "State": "CREATING"
}
```

Repita esse comando para cada região na qual você deseja ativar o Explorador de Recursos, substituindo o parâmetro `--region` pelo código de região apropriado.

Como o Explorador de Recursos executa parte da criação do índice como tarefas assíncronas em segundo plano, a resposta pode ser `CREATING`, o que indica que os processos em segundo plano ainda não foram concluídos.

> **Note**
>
> Os recursos marcados locais para o índice aparecem nos resultados de pesquisa em poucos minutos. Os recursos não marcados normalmente levam menos de duas horas para aparecer, mas podem levar mais tempo quando há muita demanda. A replicação inicial de todos os índices locais existentes em um novo índice agregador também pode levar até uma hora.

Você pode verificar a conclusão final executando o comando a seguir e verificando se o status é `ACTIVE`.

```
$ aws resource-explorer-2 get-index \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "LOCAL"
}
```

Próxima etapa: se você já criou um índice agregador, as novas regiões começarão automaticamente a replicar suas informações de índice no índice agregador. Se os usuários fizerem ali todas as pesquisas, os recursos na nova região aparecerão nesses resultados de pesquisa e pronto.

Porém, se quiser que os usuários possam pesquisar recursos apenas na região recém-indexada, você deverá criar também uma visualização para os usuários nessa região e conceder a eles permissões para essa visualização. Para obter instruções sobre como criar uma visualização, consulte Gerenciar visualizações do Explorador de Recursos para fornecer acesso para pesquisa.

# Considerações sobre regiões AWS opcionais

As regiões opt-in têm requisitos de segurança mais altos do que as regiões comerciais no que diz respeito ao compartilhamento de IAM dados por meio de contas em regiões opcionais. Todos os dados gerenciados por meio do IAM serviço são considerados dados de identidade.

Você pode ativar regiões de adesão usando o console do Explorador de recursos da AWS. Consulte Ativando o Resource Explorer em um Região da AWS para indexar seus recursos para obter mais informações.

## Comportamentos de cancelamento de adesão

Considere os seguintes comportamentos antes cancelar a adesão a uma região de adesão:

> **Important**
>
> Antes de cancelar sua adesão a uma região com um índice agregador, sugerimos que você exclua o índice agregador ou o rebaixe a um índice local. O Explorador de Recursos só permite que haja um único índice agregador entre todas as regiões da partição.

- O índice não foi excluído, só foi desabilitado. Se você escolher voltar a aderir posteriormente, suas configurações serão revertidas.
- IAMdesativa o IAM acesso aos recursos na Região.
- O Explorador de Recursos desabilita o índice da região em que a adesão foi cancelada e interrompe a ingestão de dados. Eles `ListIndexes` API não mostrarão mais o índice da região.
- Se o índice agregador estiver em outra região, o Explorador de Recursos interromperá a replicação de dados da região em que a adesão foi cancelada e limpará os dados em 24 horas.
- Se você cancelar a adesão à região do índice agregador, terá que aderir novamente para excluir ou rebaixar o índice.
- Se você aderir à região novamente, o Explorador de Recursos reabilitará o índice e começará a ingerir dados.
- Qualquer alteração no status de uma região de adesão leva cerca de 24 horas para entrar em vigor.

# Ativar a pesquisa inter-regional criando um índice agregador

Com a pesquisa entre regiões ativada, você pode pesquisar recursos em todas as regiões do seu Conta da AWS.

Tópicos



## Sobre o índice agregador

Explorador de recursos da AWS armazena as informações coletadas sobre os recursos em um Região da AWS índice local que o Resource Explorer cria e mantém nessa região. Por exemplo, suponha que você tenha uma EC2 instância da Amazon na região Oeste dos EUA (Oregon). O Explorador de Recursos armazena os detalhes sobre esse recurso no índice local na região Oeste dos EUA (Oregon).

Para apoiar a pesquisa de recursos Regiões da AWS em toda a sua conta, você pode converter o índice local em uma região para ser o índice agregador da sua conta.

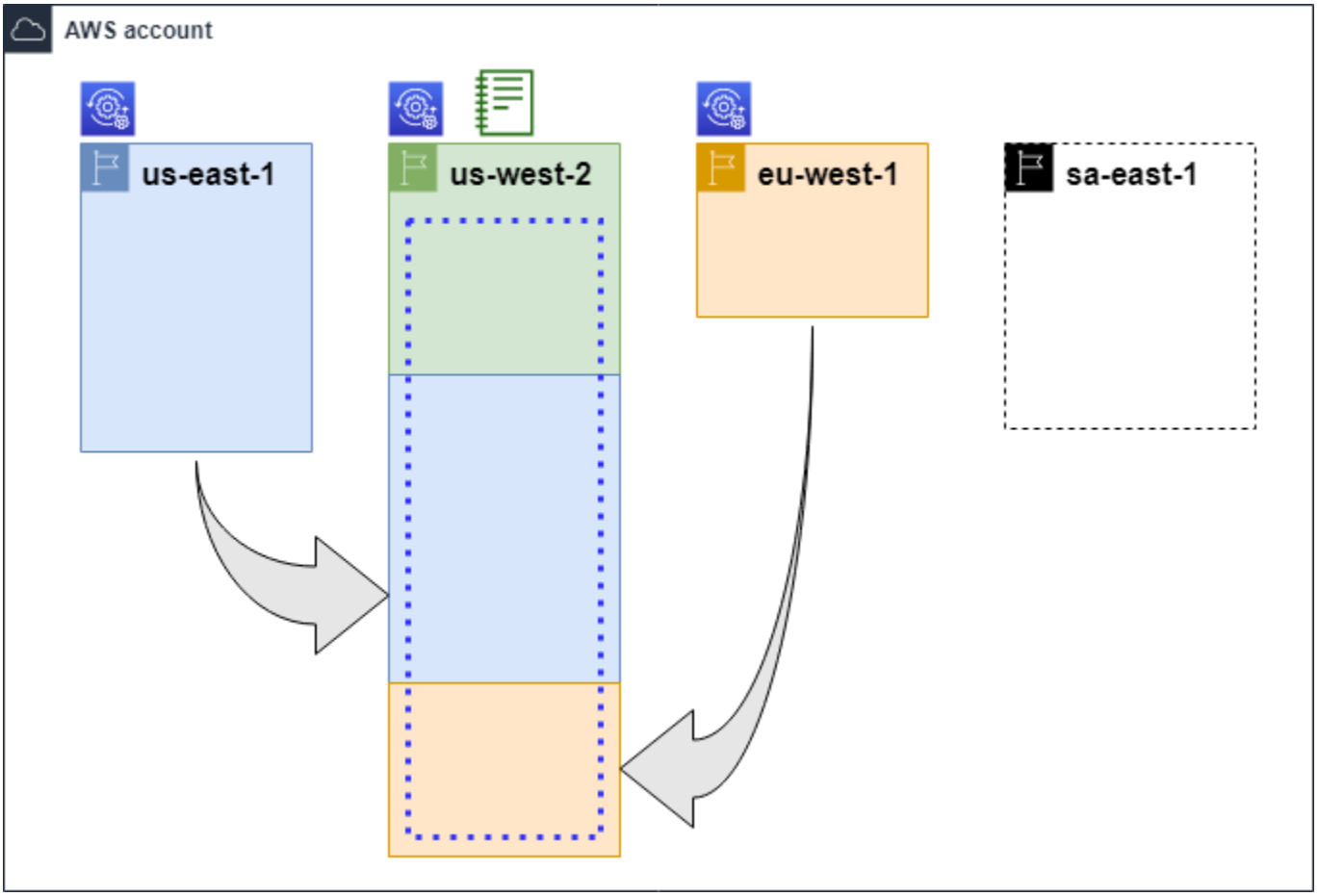
O índice agregador contém uma cópia replicada do índice local em todas as outras regiões em que você ativou o Explorador de Recursos. Isso permite criar visualizações na região que contêm o índice agregador cujos resultados podem incluir recursos de todos Regiões da AWS na conta.

O diagrama a seguir mostra um exemplo de como o índice do agregador funciona. Neste exemplo de Conta da AWS, o administrador faz o seguinte:

- Ativa o Resource Explorer em três Regiões da AWS (`us-east-1us-west-2`, `eeu-west-1`) criando índices nessas regiões. Cada região contém seu próprio índice local.
- Escolhe não criar um índice na região `sa-east-1`. Os usuários não podem fazer pesquisas na região `sa-east-1` e nenhum recurso dessa região aparece nos resultados de pesquisa.
- Cria o índice agregador para a conta na região `us-west-2`. Isso faz com que o Explorador de Recursos replique no índice agregador as informações dos índices locais de todas as outras regiões em que o Explorador de Recursos está ativado. Isso permite que as pesquisas feitas na

região `us-west-2` incluam recursos de todas as três regiões nas quais o Explorador de Recursos está ativado.

Essa configuração significa que um usuário sópode fazer pesquisas inter-regionais na região `us-west-2`, que contém o índice agregador. Somente visualizações dessa região podem retornar resultados de todas as regiões na conta.




| Legenda | |
|---|---|
|  | O Resource Explorer é ativado nessa Região da AWS opção e seus recursos são catalogados em um índice nessa região. O índice dessa região também é replicado (indicado pelas setas) para o Região da AWS que contém o índice agregador. |
|  | Isso Região da AWS contém o índice agregador. O Resource Explorer replica as informações de recursos coletadas em todos os outros Regiões da AWS nesta região. |

A visualização padrão criada pela Configuração rápida inclui todos os recursos em todas as Regiões da AWS.

# Promover um índice local para ser o índice agregador da conta

Você tem a opção de criar um índice agregador em uma Região da AWS quando configura o Explorador de recursos da AWS pela primeira vez. Veja mais informações em Instalar e configurar o Explorador de Recursos. Esse procedimento consiste em promover um dos índices locais para ser o índice agregador da conta, caso você não tenha feito isso na configuração inicial.

**Important**

- Você não pode ter mais de um índice agregador em uma Conta da AWS. Se a conta já tiver um índice agregador, você deverá primeiro rebaixá-lo a um índice local ou excluí-lo.
- Depois de excluir ou alterar a região que contém o índice agregador, você deve esperar 24 horas antes de poder promover outro índice para ser o índice agregador.

AWS Management Console

Para promover um índice local para ser o índice agregador da conta

1. Abra a página Configurações do Explorador de Recursos.
2. Na seção Índices, marque a caixa de seleção ao lado do índice que você deseja promover e escolha Alterar tipo de índice.
3. Na caixa de diálogo Alterar tipo de índice para <Nome da região>, escolha Índice agregador e depois Salvar alterações.

AWS CLI

Para promover um índice local para ser o índice agregador da conta

O exemplo de comando a seguir atualiza o índice na Região da AWS especificada do tipo `LOCAL` para o tipo `AGGREGATOR`. É necessário chamar a operação na Região da AWS que você deseja que contenha o índice agregador.

```
$ aws resource-explorer-2 update-index-type \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --type AGGREGATOR \
    --region us-east-1
{
    "Arn":"arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "LastUpdatedAt":"2022-07-13T18:41:58.799Z",
    "State":"UPDATING",
    "Type":"AGGREGATOR"
}
```

A operação funciona de forma assíncrona e começa com `State` definido como `UPDATING`. Para verificar se a operação foi concluída, você pode executar o comando a seguir e procurar o valor `ACTIVE` no campo `State` da resposta. Você deve executar esse comando na região que contém o índice que você deseja verificar.

```
$ aws resource-explorer-2 get-index --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-10-12T21:31:37.277000+00:00",
    "LastUpdatedAt": "2022-10-12T21:31:37.677000+00:00",
    "ReplicatingFrom": [
        "us-west-2",
        "us-east-2",
        "us-west-1"
    ],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "AGGREGATOR"
}
```

# Rebaixar o índice agregador a um índice local

É possível rebaixar um índice agregador a um índice local, por exemplo, quando você quer transferir o índice agregador para outra Região da AWS.

Quando você rebaixa um índice agregador a um índice local, o Explorador de Recursos deixa de replicar os índices de outras Regiões da AWS. Ele também inicia uma tarefa assíncrona em segundo plano para excluir qualquer informação replicada das outras regiões. Até que a tarefa assíncrona seja concluída, alguns resultados inter-regionais podem continuar aparecendo nos resultados de pesquisa.

Observações

- Depois de rebaixar um índice agregador, você deve esperar 24 horas antes de poder promover o mesmo índice ou o índice de uma outra região para ser o novo índice agregador da conta.
- Depois de rebaixar um índice agregador, pode levar até 36 horas para que os processos em segundo plano sejam concluídos e todas as informações de recursos de outras regiões desapareçam dos resultados das pesquisas realizadas nessa região.
- Se você rebaixar uma conta-membro em uma visão ampla da organização, a conta-membro poderá ser removida da pesquisa de várias contas.

Você pode verificar o status da tarefa em segundo plano visualizando a lista de índices na página Configurações ou usando a GetIndexoperação. Quando as tarefas assíncronas são concluídas, o campo `Status` do índice muda de `UPDATING` para `ACTIVE`. Nesse momento, somente os resultados da região local aparecem nos resultados das consultas.

AWS Management Console

Para rebaixar o índice agregador a um índice local

1. Abra a página Configurações do Explorador de Recursos.
2. Na seção Índices, marque a caixa de seleção ao lado da região que contém o índice agregador que você deseja rebaixar a um índice local e escolha Alterar tipo de índice.
3. Na caixa de diálogo Alterar tipo de índice para <Nome da região>, escolha Índice local e depois Salvar alterações.

AWS CLI

Para rebaixar o índice agregador a um índice local

O exemplo a seguir rebaixa o índice agregador especificado a um índice local. Você deve chamar a operação na Região da AWS que contém o índice agregador no momento.

```
$ aws resource-explorer-2 update-index-type \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --type LOCAL \
    --region us-east-1
{
    "Arn":"arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "LastUpdatedAt":"2022-07-13T18:41:58.799Z",
    "State":"UPDATING",
    "Type":"LOCAL"
}
```

A operação funciona de forma assíncrona e começa com `State` definido como `UPDATING`. Para verificar se a operação foi concluída, você pode executar o comando a seguir e procurar o valor `ACTIVE` no campo `State` da resposta. Você deve executar esse comando na região que contém o índice que você deseja verificar.

```
$ aws resource-explorer-2 get-index --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-10-12T21:31:37.277000+00:00",
    "LastUpdatedAt": "2022-10-12T21:31:37.677000+00:00",
    "ReplicatingFrom": [
        "us-west-2",
        "us-east-2",
        "us-west-1"
    ],
    "State": "ACTIVE",
    "Tags": {},
    "Type": "LOCAL"
}
```

# Ativar a pesquisa em várias contas

Com a pesquisa em várias contas, você pode pesquisar recursos em várias contas com índices ativos em sua unidade organizacional ( AWS Organizations OU).

Tópicos



## Pré-requisitos

Para ativar a pesquisa em várias contas para sua organização, faça o seguinte:

- Para regiões opcionais, verifique se sua conta de gerenciamento também está ativada quando você está ativando a pesquisa em várias contas.
- Crie um usuário administrativo.
- Crie um perfil vinculado ao serviço na conta do administrador com o `aws iam create-service-linked-role --aws-service-name resource-explorer-2.amazonaws.com`.
- Habilite o acesso confiável em AWS Organizations. Isso permite a integração total com o Explorador de Recursos para listar recursos em todas as contas na sua organização.
- Designe um administrador delegado (recomendado). Para obter mais informações, consulte Administrador delegado para AWS serviços que funcionam com Organizations no Guia do AWS Organizations Usuário.
  - O Explorador de Recursos aceita apenas um único administrador delegado que executa ações semelhantes às da conta de gerenciamento.
  - Remover ou alterar o administrador delegado da sua organização resulta na remoção de todas as visualizações de várias contas criadas na conta do administrador.

## Habilitar a pesquisa em várias contas

Para pesquisar e descobrir recursos nas contas de sua organização, você deve realizar as etapas a seguir:

1. Ative Explorador de recursos da AWS em uma ou mais contas em seu AWS Organizations.
2. Registre uma região para conter o índice agregador.
3. Escolha uma região na qual criar um índice agregador. Esta região deve ser consistente em todo o seu AWS Organizations.
4. Crie uma visualização do Resource Explorer que tenha como escopo sua AWS Organizations unidade organizacional. Crie essa visualização na região agregadora da etapa anterior.
5. Compartilhe a visualização com as contas de toda a sua organização.

## Configuração rápida de várias contas

Habilite o Explorador de Recursos em várias contas da sua organização com a Configuração rápida.

> **Note**
>
> Esse processo não implanta nenhum recurso na conta de gerenciamento. Se estiver usando a conta de gerenciamento e quiser índices na conta, deverá adicioná-los manualmente com o fluxo de integração do Explorador de Recursos.

1. Navegue até configuração rápida do Explorador de Recursos no console do Systems Manager.
2. Escolha a região do índice agregador. Isso permite que você pesquise recursos localizados em todas as regiões nas contas de destino selecionadas. Se alguma das contas de destino selecionadas já tiver um índice agregador configurado em outra região, o índice agregador existente será automaticamente substituído por essa nova região.
3. Escolha os destinos da sua conta. Você pode ativar o Resource Explorer para toda a sua organização ou para unidades organizacionais específicas (OUs).

   > **Note**
   >
   > Você pode implantar no máximo 50.000 AWS CloudFormation pilhas por vez. Se tiver uma organização grande que abranja várias regiões, você deverá implantar no nível da OU em lotes menores.

4. Leia todo o resumo das confirmações antes de escolher Criar.

# Efeito das ações de conta na pesquisa de várias contas do Explorador de Recursos

> **Note**
>
> A remoção de contas e recursos dos resultados da pesquisa de várias contas leva até 24 horas.

As ações da conta têm os seguintes efeitos na pesquisa Explorador de recursos da AWS de várias contas.

## Explorador de Recursos desabilitado

Quando você desabilita o Explorador de Recursos em uma conta, ele é desabilitado apenas nessa conta na Região da AWS selecionada quando ele é desabilitado.

Você deve desabilitar o Explorador de Recursos separadamente em cada região em que ele está habilitado.

Depois de 24 horas, os recursos dessa conta não aparecerão mais nos resultados de pesquisa.

Outros dados e configurações do Explorador de Recursos não serão removidos.

## Uma conta-membro é removida de uma organização

Quando uma conta-membro é removida de uma organização, a conta de administrador do Explorador de Recursos perde as permissões para visualizar recursos na conta-membro.

Se a conta removida for uma conta de administrador ou de administrador delegado, todas as visualizações de várias contas criadas anteriormente por essas contas também serão removidas.

O Explorador de Recursos continua em execução em ambas as contas.

Os resultados de pesquisa de recursos não incluem mais os recursos dessa conta.

## Minha conta foi suspensa

Quando uma conta é suspensa AWS, a conta perde as permissões para visualizar recursos no Resource Explorer. A conta de administrador de uma conta suspensa pode visualizar os recursos existentes.

Para uma conta da organização, o status da conta-membro também pode mudar para Conta suspensa. Isso acontecerá se a conta for suspensa ao mesmo tempo que a conta do administrador tentar habilitá-la. A conta de administrador de uma conta suspensa não pode visualizar os recursos dessa conta.

Do contrário, o status de suspensa não afetará o status da conta-membro.

Após 90 dias, a conta é desativada ou reativada. Quando a conta é reativada, suas permissões do Explorador de Recursos são restauradas. Se o status da conta-membro for Conta suspensa, a conta do administrador deverá habilitar a conta manualmente.

## A conta é fechada

Quando uma AWS conta é fechada, o Resource Explorer responde ao encerramento da seguinte forma:

- O Explorador de Recursos mantém os recursos da conta por 90 dias a partir da data efetiva de encerramento da conta. No fim do período de 90 dias, o Explorador de Recursos exclui permanentemente todos os dados da conta.
- Para reter recursos por mais de 90 dias, você pode usar uma ação personalizada com uma EventBridge regra para armazenar os recursos em um bucket do Amazon S3. Desde que o Explorador de Recursos retenha os recursos, quando você reabrir a conta, ele restaurará os recursos para a conta.
- Se a conta for uma conta de administrador do Explorador de Recursos, ela será removida como administrador e todas as contas-membros serão removidas. Se a conta for uma conta-membro, ela será desassociada e removida como membro da conta de administrador do Explorador de Recursos.
- Para obter mais informações, consulte Encerrar uma conta.

## Cancelamento da adesão da conta

Se a adesão de uma conta a uma região for cancelada, você ainda verá os recursos delas nos resultados de pesquisa por até 24 horas.

Depois de 24 horas, os recursos dessa conta não aparecerão mais nos resultados de pesquisa. Para obter mais informações, consulte Comportamentos de cancelamento de adesão.

# Possibilitar a pesquisa unificada no AWS Management Console

AWS Management Console Tem uma barra de pesquisa na parte superior de cada página do console. Isso fornece uma experiência de pesquisa unificada para todos Serviços da AWS. Os resultados da pesquisa unificada podem incluir, por exemplo:

- AWS service (Serviço da AWS) e apresentam páginas do console.
- AWS páginas de documentação.
- AWS artigos do blog e da Base de Conhecimento
- Recursos em suas contas: se você seguir as etapas abaixo.

Para ver os recursos da sua conta nos resultados da pesquisa unificada, você deve realizar as etapas a seguir. Você pode fazer isso durante a configuração inicial do Explorador de recursos da AWS. Tudo será feito automaticamente se você usar a opção Configuração rápida.

- Você deve criar um índice agregador em um Região da AWS para o. Conta da AWS
- Você precisa criar uma visualização padrão na Região da AWS que contém o índice agregador.
- Você deve conceder a todas as entidades principais que precisam pesquisar recursos na barra de pesquisa unificada permissão para pesquisar usando essa visualização padrão.

A pesquisa unificada sempre usa a visualização padrão Região da AWS que contém o índice agregador para realizar todas as pesquisas.

# Implantar o Explorador de Recursos nas contas de uma organização

Ao usar AWS CloudFormation StackSets, você pode definir e implantar em todas as contas gerenciadas em uma organização pelo AWS Organizations. Ao definir um conjunto de pilhas, você especifica AWS os recursos que deseja criar na sua Regiões da AWS e em todas as contas de destino que você especificar. Quando todas as contas fazem parte da mesma organização, você pode aproveitar a AWS CloudFormation integração com o Organizations e deixar que esses serviços lidem com a criação de funções entre contas. Você pode habilitar a implantação automática em uma organização, o que implantará automaticamente instâncias de pilha nas novas contas que você venha a adicionar à organização ou a uma unidade organizacional (UO) de destino no futuro. Se você remover uma conta da organização, o AWS CloudFormation excluirá automaticamente todos os recursos que foram implantados como parte de uma instância de pilha da organização. Para obter mais informações sobre StackSets, consulte Trabalhando com AWS CloudFormation StackSets no Guia AWS CloudFormation do Usuário.

Você pode usar AWS CloudFormation StackSets para ativar e configurar Explorador de recursos da AWS em todas as contas da sua organização, criando índices em cada região habilitada e criando visualizações onde você precisar delas.

> **Important**
>
> Se você tentar configurar um índice agregador em uma região, certifique-se de que a conta não tenha um índice agregador existente em nenhuma outra região. Depois de rebaixar um índice agregador a um índice local, você deve esperar 24 horas antes de poder promover outro índice para ser o novo índice agregador da conta.

## Pré-requisitos

Para usar AWS CloudFormation StackSets para implantar o Resource Explorer nas contas da sua organização, você ou o administrador da sua organização deve primeiro executar as seguintes etapas para habilitar pilhas com permissões gerenciadas pelo serviço:

1. A organização deve ter todos os atributos habilitados. Se a organização só tiver atributos de faturamento consolidado habilitados, você não poderá criar um conjunto de pilhas com permissões gerenciadas pelo serviço.

2. Ative o acesso confiável entre AWS CloudFormation e Organizations. Isso concede AWS CloudFormation permissão para criar as funções necessárias na conta de gerenciamento da organização e as contas dos membros AWS CloudFormation implantarão índices e visualizações do Resource Explorer.

Agora você pode criar um conjunto de pilhas com permissões gerenciadas pelo serviço.

> **Important**
>
> Você deve criar os conjuntos de pilhas na conta de gerenciamento da organização. AWS CloudFormation é um serviço regional, portanto, você pode visualizar e gerenciar os conjuntos de pilhas criados somente na região em que os criou originalmente.

## Criar conjuntos de pilhas para o Explorador de Recursos

Para implantar totalmente o Explorador de Recursos, você deve implantar dois conjuntos de pilhas.

- O primeiro conjunto de pilhas cria o índice agregador e a visualização padrão que permite que os usuários pesquisem recursos em todas as regiões da conta.

  Implante esse conjunto de pilhas apenas na região em que você deseja criar o índice agregador.
- O segundo conjunto de pilhas cria um índice local e uma visualização padrão. O índice local replica seu conteúdo no índice agregador.

  Implante esse conjunto de pilhas em todas as regiões habilitadas na conta, exceto na região que contém o índice agregador. Não escolha nenhuma região que não esteja habilitada nas contas em que você implantar a pilha. Do contrário, ocorrerá falha na implantação.

Veja exemplos de modelos para cada uma dessas na próxima seção. Para step-by-step obter instruções sobre como criar um conjunto de pilhas usando esses modelos, consulte Criar um conjunto de pilhas com permissões gerenciadas por serviços no Guia do usuário.AWS CloudFormation

Depois de implantar esses conjuntos de pilhas em sua organização, toda conta dentro do escopo selecionado, organização ou unidade organizacional, terá um índice agregador na região especificada e índices locais em todas as outras regiões.

# AWS CloudFormation Modelos de amostra

O exemplo de modelo a seguir cria o índice agregador da conta e uma visualização padrão que pode pesquisar recursos em todas as regiões da conta em que você implanta um índice.

YAML

```
Description: >-
  CFN Stack setting up ResourceExplorer with an Aggregator Index, and a new Default
 View.
Resources:
  Index:
    Type: 'AWS::ResourceExplorer2::Index'
    Properties:
      Type: AGGREGATOR
      Tags:
        Purpose: ResourceExplorer CFN Stack
  View:
    Type: 'AWS::ResourceExplorer2::View'
    Properties:
      ViewName: DefaultView
      IncludedProperties:
        - Name: tags
      Tags:
        Purpose: ResourceExplorer CFN Stack
    DependsOn: Index
  DefaultViewAssociation:
    Type: 'AWS::ResourceExplorer2::DefaultViewAssociation'
    Properties:
      ViewArn: !Ref View
```

JSON

```
{
    "Description": "CFN Stack setting up ResourceExplorer with an Aggregator Index,
 and a new Default View.",
    "Resources": {
        "Index": {
            "Type": "AWS::ResourceExplorer2::Index",
            "Properties": {
                "Type": "AGGREGATOR",
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
```

```
                }
            }
        },
        "View": {
            "Type": "AWS::ResourceExplorer2::View",
            "Properties": {
                "ViewName": "DefaultView",
                "IncludedProperties": [{
                    "Name": "tags"
                }],
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            },
            "DependsOn": "Index"
        },
        "DefaultViewAssociation": {
            "Type": "AWS::ResourceExplorer2::DefaultViewAssociation",
            "Properties": {
                "ViewArn": {
                    "Ref": "View"
                }
            }
        }
    }
}
```

O exemplo de modelo a seguir cria um índice local em todas as regiões habilitadas de todas as contas, exceto a que contém o índice agregador. Ele também cria uma visualização padrão com a qual os usuários podem pesquisar recursos apenas nessa região. Para pesquisar recursos em todas as regiões, os usuários devem pesquisar com uma visualização na região de agregação.

YAML

```
Description: >-
  CFN Stack setting up ResourceExplorer with a Local Index, and a new Default View.
Resources:
  Index:
    Type: 'AWS::ResourceExplorer2::Index'
    Properties:
      Type: LOCAL
      Tags:
```

```
        Purpose: ResourceExplorer CFN Stack
  View:
    Type: 'AWS::ResourceExplorer2::View'
    Properties:
      ViewName: DefaultView
      IncludedProperties:
        - Name: tags
      Tags:
        Purpose: ResourceExplorer CFN Stack
    DependsOn: Index
  DefaultViewAssociation:
    Type: 'AWS::ResourceExplorer2::DefaultViewAssociation'
    Properties:
      ViewArn: !Ref View
```

JSON

```
{
    "Description": "CFN Stack setting up ResourceExplorer with a Local Index, and a
 new Default View.",
    "Resources": {
        "Index": {
            "Type": "AWS::ResourceExplorer2::Index",
            "Properties": {
                "Type": "LOCAL",
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            }
        },
        "View": {
            "Type": "AWS::ResourceExplorer2::View",
            "Properties": {
                "ViewName": "DefaultView",
                "IncludedProperties": [{
                    "Name": "tags"
                }],
                "Tags": {
                    "Purpose": "ResourceExplorer CFN Stack"
                }
            },
            "DependsOn": "Index"
        },
```

```
        "DefaultViewAssociation": {
            "Type": "AWS::ResourceExplorer2::DefaultViewAssociation",
            "Properties": {
                "ViewArn": {
                    "Ref": "View"
                }
            }
        }
    }
}
```

# Desativando o Resource Explorer

Quando não precisar mais pesquisar recursos em uma região específica Região da AWS, você pode desativá-los somente Explorador de recursos da AWS nessa região excluindo seu índice, ou pode excluir o Resource Explorer de todas Regiões da AWS. Quando você faz isso, o Explorador de Recursos deixa de verificar se há recursos novos ou atualizados nessa região. Se sua conta contiver um índice agregador, a replicação do índice excluído será interrompida e as informações do índice excluído serão removidas do índice agregador e não aparecerão mais nos resultados de pesquisa. Pode levar até 24 horas para que todos os recursos do índice excluído parem se aparecer os resultados de pesquisa na região com o índice agregador.

> **Note**
>
> Quando você registra a primeira Região da AWS, o Resource Explorer cria uma função vinculada ao serviço (SLR) nomeada `AWSServiceRoleForResourceExplorer` no Conta da AWS. O Resource Explorer não exclui isso SLR automaticamente. Depois de excluir o índice do Resource Explorer em todas as regiões da conta, você pode usar o IAM console para excluir o SLR caso não use o Resource Explorer no futuro. Se você excluir a função e optar por ativar o Resource Explorer novamente em pelo menos uma Região da AWS, o Resource Explorer recriará a função vinculada ao serviço automaticamente.

## Desativando o Resource Explorer em um Região da AWS

Você pode desativar o Resource Explorer em um Região da AWS usando o AWS Management Console, usando comandos no AWS Command Line Interface (AWS CLI) ou usando API operações em um AWS SDK.

Se você desativar o Explorador de Recursos de uma conta-membro e ela estiver em uma visão ampla da organização, ela será removida dos resultados da pesquisa de várias contas.

Se você não quiser mais possibilitar a pesquisa de recursos em uma ou mais Regiões da AWS da sua conta, realize as etapas do procedimento a seguir.

> **Note**
>
> Se o índice excluído for o índice agregador do Conta da AWS, você deverá esperar 24 horas antes de promover outro índice local para ser o índice agregador da conta. Os usuários não

poderão realizar pesquisas que abranjam toda a conta usando o Explorador de Recursos até que outro índice agregador seja configurado.

### AWS Management Console

Para excluir o índice do Resource Explorer em um Região da AWS

1. Abra a página Configurações do Explorador de Recursos.
2. Na seção Índices, marque as caixas de seleção Regiões da AWS ao lado dos índices que você deseja excluir e escolha Excluir.
3. Na página Excluir índices, confirme que você selecionou apenas os índices deseja excluir. Digite **`delete`** na caixa de texto Confirmar e escolha Excluir índices.

   O Explorador de Recursos exibe um banner verde na parte superior da página para indicar sucesso ou um banner vermelho se ocorrer um erro em uma ou mais das regiões selecionadas.

### AWS CLI

Para excluir o índice do Resource Explorer em um Região da AWS

Se você não quiser mais oferecer suporte à pesquisa de recursos em um ou mais dos recursos da Regiões da AWS sua conta, execute os comandos a seguir.

Execute o comando a seguir para cada região com os índices que você deseja excluir. Você deve executar o comando na região com o índice que você deseja excluir. O exemplo de comando a seguir exclui o índice do Explorador de Recursos na região Oeste dos EUA (Oregon) (`us-west-2`).

```
$ aws resource-explorer-2 delete-index \
    --arn arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222 \
    --region us-west-2
{
    "Arn": "arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222",
    "State": "DELETING"
}
```

Como o Explorador de Recursos faz parte do trabalho de limpeza de exclusão como tarefas assíncronas em segundo plano, a resposta pode indicar que a operação está `DELETING`. Esse status indica que os processos em segundo plano ainda não foram concluídos. Você pode verificar a conclusão final executando o comando a seguir e verificando se `State` muda para `DELETED`.

```
$ aws resource-explorer-2 get-index \
    --region us-west-2
{
    "Arn": "arn:aws:resource-explorer-2:us-
west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [],
    "State": "DELETED",
    "Tags": {},
    "Type": "LOCAL"
}
```

# Desativando o Resource Explorer em todos Regiões da AWS

Se você quiser desligar Explorador de recursos da AWS completamente, execute o procedimento a seguir.

> **Note**
>
> O Resource Explorer cria uma função vinculada ao serviço nomeada AWSServiceRoleForResourceExplorer na conta quando você cria um índice no primeiro Região da AWS para uma conta. O Explorador de Recursos não exclui automaticamente esse perfil vinculado ao serviço. Depois de excluir o índice do Resource Explorer em cada região, você poderá usar o IAM console para excluir a função se tiver certeza de que não usará o Resource Explorer novamente no futuro. Se você excluir a função e optar por iniciar o Resource Explorer em pelo menos uma Região da AWS, o Resource Explorer recriará a função vinculada ao serviço.

Você pode desativar o Resource Explorer usando o AWS Management Console, usando comandos no AWS Command Line Interface (AWS CLI) ou usando API operações em um AWS SDK.

AWS Management Console

Se você não quiser mais oferecer suporte à pesquisa de recursos Região da AWS em qualquer um dos seus Conta da AWS, execute as etapas no procedimento a seguir.

Para desativar o Resource Explorer em todos Regiões da AWS

1. Abra a página Configurações do Explorador de Recursos.
2. Na seção Índices, marque as caixas de seleção ao lado de todos os registrados Regiões da AWS e escolha Excluir.

   > **Tip**
   >
   > Você pode marcar a caixa na linha do cabeçalho da tabela ao lado de Índice para marcar as caixas de todas as regiões em uma única etapa.

3. Na página Excluir índices, confirme que você deseja excluir todos os índices. Digite **`delete`** na caixa de texto Confirmar e escolha Excluir índices.

   O Explorador de Recursos exibe um banner verde na parte superior da página para indicar sucesso ou um banner vermelho se ocorrer um erro em uma ou mais das regiões selecionadas.

AWS CLI

Para desativar o Resource Explorer em todos Regiões da AWS

Se você não quiser mais oferecer suporte à pesquisa de recursos Regiões da AWS em qualquer parte da sua conta, execute o comando a seguir para encontrar todos os índices Região da AWS em cada um ARN dos quais você ativou anteriormente o Resource Explorer.

```
$ aws resource-explorer-2 list-indexes --query Indexes[*].Arn[
"arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
"arn:aws:resource-explorer-2:us-west-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd22222222",
"arn:aws:resource-explorer-2:us-west-2:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd33333333"
]
```

Para cada resposta, execute o comando a seguir para excluir o índice do Explorador de Recursos daquela região.

```
$ aws resource-explorer-2 delete-index \
    --arn arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "State": "DELETING"
}
```

Repita o comando anterior em cada região adicional.

Como o Explorador de Recursos faz parte da limpeza como tarefas assíncronas em segundo plano, a resposta pode indicar que a operação está `DELETING`. Esse status indica que os processos em segundo plano ainda não foram concluídos. Você pode verificar a conclusão final executando o comando a seguir e verificando se o status muda para `DELETED`.

```
$ aws resource-explorer-2 get-index \
    --region us-east-1
{
    "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
    "CreatedAt": "2022-07-12T18:59:10.503000+00:00",
    "LastUpdatedAt": "2022-07-13T18:41:58.799000+00:00",
    "ReplicatingFrom": [],
    "State": "DELETED",
    "Tags": {},
    "Type": "LOCAL"
}
```

# Gerenciar visualizações do Explorador de Recursos para fornecer acesso para pesquisa

As visualizações são a chave para pesquisar os recursos. Cada operação de Explorador de recursos da AWS pesquisa deve usar uma visualização. As visualizações são o método que o administrador pode usar para controlar o acesso às informações sobre os recursos na sua Conta da AWS.

Uma exibição pode ser acessada somente por diretores (IAMfunções ou usuários) que tenham permissão para usar essa visualização. Para pesquisar com sucesso com o Resource Explorer, o diretor deve ter `Allow` acesso às `resource-explorer-2:Search` operações `resource-explorer-2:GetView` e na exibição ARN.

As visualizações contêm filtros integrados que o administrador pode usar para limitar os resultados apenas aos itens de interesse. Por exemplo, você pode criar uma visualização que só inclua os recursos relacionados a um determinado projeto. Os usuários que não precisam ver informações sobre outros projetos podem usar essa visualização para ver apenas os recursos de interesse.

Uma visualização é um recurso regional. A visualização é criada e armazenada em uma Região da AWS específica e só retorna nos resultados as informações do índice dessa região. Para incluir resultados de todas as regiões da conta, a visualização deve residir na região que contém o índice agregador. Essa região contém uma réplica dos índices de todas as outras regiões da conta.

Toda visualização tem vários elementos essenciais:

Permissões para pesquisar

Você pode usar políticas de AWS permissão padrão para controlar quem pode usar cada visualização. Isso é fornecido pelas políticas de permissão baseadas em identidade anexadas às entidades principais que dão a você controle granular sobre quem pode ver as informações fornecidas por cada visualização. Por exemplo, você pode conceder acesso à visualização `Production-resources` para só permitir que os engenheiros que operam os serviços de produção a pesquisem. Depois, você pode conceder permissões diferentes à visualização `Pre-production-resources` para permitir que os desenvolvedores pesquisem os recursos de pré-produção.

Se você usar a política AWS gerenciada nomeada `AWSResourceExplorerReadOnlyAccess` com seus diretores, ela concederá a eles a capacidade de pesquisar usando qualquer visualização na conta.

Como alternativa, você pode criar sua própria política de permissões e conceder as seguintes permissões apenas para visualizações específicas:

- `resource-explorer-2:GetView`
- `resource-explorer-2:Search`

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 Criação de 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 Criação de uma função para um IAM usuário no Guia IAM do 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 obter mais informações sobre as permissões relacionadas às visualizações, consulte Conceder acesso às visualizações do Explorador de Recursos para pesquisa.

Filtrar a pesquisa

Uma visualização serve como uma janela virtual através da qual o usuário pode ver os recursos da conta. Você pode criar várias visualizações, cada uma apresentando uma visão diferente do quadro mais amplo. Por exemplo, você pode criar uma visualização que permita pesquisar somente recursos associados ao ambiente de pré-produção, conforme identificado pelas tags anexadas aos recursos. Depois, você pode criar uma visualização separada que só permita pesquisar recursos no ambiente de produção, com base nos diferentes valores das tags. Se você configurar várias visualizações com valores de `FilterString` diferentes, não precisará inserir novamente esses parâmetros de consulta toda vez que pesquisar.

As visualizações também podem especificar quais informações opcionais sobre os recursos devem ser incluídas nos resultados. A lista de campos padrão é sempre incluída nos resultados.

Além da lista padrão, você pode solicitar que a visualização também inclua todas as tags anexadas ao recurso.

Escopo da pesquisa

- Escopo da região — Quando você pesquisa em um Região da AWS com o Resource Explorer, os resultados podem incluir somente recursos indexados nessa região. O índice da maioria das regiões é rotulado como `LOCAL` porque só contém informações sobre os recursos dentro daquela região. As pesquisas nessas regiões só podem retornar esses recursos.
- Escopo de conta: você pode promover um índice local para ser o índice agregador da conta. Quando você faz isso, todas as outras regiões em que o Explorador de Recursos está ativado replicam suas informações de índice na região com o índice agregador. Se você pesquisar nessa região, os resultados incluirão recursos de todas as regiões na conta. Quando você usa a opção Configuração rápida para configurar o servidor, o Explorador de Recursos cria automaticamente um índice agregador na região especificada. Além disso, a opção Configuração rápida cria uma visualização padrão nessa região para possibilitar a pesquisa de todos os recursos da conta em todas as regiões.

# Visualizações padrão

Se um usuário tentar pesquisar sem especificar explicitamente uma visualização, o Explorador de Recursos usará a visualização padrão definida para a Região da AWS.

Se não existir uma visualização padrão para a região e o usuário não especificar uma visualização para ser usada, ocorrerá uma falha na pesquisa e será gerada uma exceção.

O Explorador de Recursos cria automaticamente uma visualização padrão da seguinte maneira:

- Se você ativar o Resource Explorer usando o AWS Management Console e escolher a opção Configuração rápida, deverá especificar qual região contém o índice agregador da conta. O Explorador de Recursos cria automaticamente uma visualização padrão na região especificada do índice agregador.
- Se você registrar o Resource Explorer usando o AWS Management Console e escolher a opção Configuração avançada, você pode optar por criar o índice agregador para a conta em uma região especificada. Se fizer isso, o Explorador de Recursos criará automaticamente uma visualização padrão na região do índice agregador especificada.

- Se você registrar o Explorador de Recursos usando o console e escolher não registrar uma região de índice agregador, o Explorador de Recursos criará uma visualização padrão para o índice local em cada região.
- Se você registrar o Resource Explorer usando as API operações AWS CLI ou, o Resource Explorer não criará automaticamente uma exibição padrão. Em vez disso, você deverá configurar manualmente a visualização padrão para cada região na qual espera que os usuários pesquisem.

# Criar visualizações do Explorador de Recursos para usar em pesquisas

Todas as pesquisas devem usar uma visualização. Uma visualização define os filtros que determinam quais recursos podem ser retornados pelas consultas que usam a visualização. As visualizações também controlam quem pode pesquisar recursos.

Uma visualização é armazenada em um Região da AWS e retorna os resultados da pesquisa somente do índice dessa região. Se a região contiver o índice agregador, a visualização retornará os resultados de pesquisa dos índices em todas as regiões da conta.

As visualizações de várias contas permitem que você pesquise recursos nas contas em toda a organização. Qualquer conta que você deseje pesquisar requer índices. Apenas a conta de gerenciamento ou conta de administrador delegado de uma organização podem criar uma visualização de várias contas.

Explorador de recursos da AWS pode criar uma exibição padrão para você durante a configuração inicial se você escolher as opções relevantes na Configuração rápida do Resource Explorer no console do Systems Manager ou na configuração avançada. Posteriormente, você poderá criar visualizações adicionais com filtros diferentes para diferentes conjuntos de usuários a qualquer momento.

Você pode criar uma visualização usando o AWS Management Console ou executando AWS CLI comandos ou suas API operações equivalentes em um AWS SDK.

Permissões mínimas

Para executar esse comando, você deve ter as seguintes permissões:

- Ação: `resource-explorer-2:CreateView`

Recurso: Isso pode * permitir a criação de uma visualização Região da AWS em qualquer parte da conta.

AWS Management Console

Para criar uma visualização

1. Abra a página Visualizações do console do Explorador de Recursos e escolha Criar visualização.
2. Na página Criar visualização, em Nome, insira um nome para a visualização.

   O nome não deve ter mais de 64 caracteres e pode incluir letras, dígitos e o caractere hífen (-). O nome deve ser exclusivo em seu Região da AWS.
3. Escolha aquela Região da AWS na qual você deseja criar a exibição. Para criar uma visualização que retorne recursos de todas as regiões da conta, escolha Região da AWS aquela que contém o índice agregador.
4. (Opcional) Em Escopo, escolha se sua pesquisa retorna recursos de várias contas ou somente da sua conta. O escopo do nível de conta é o padrão.

   Somente a conta de gerenciamento ou conta de administrador delegado de uma organização podem criar uma visualização de várias contas.
5. Escolha se deseja filtrar os resultados.

   - Incluir todos os recursos

     Nenhum filtro de consulta é incluído. Todos os recursos no índice associado à visualização podem ser retornados nos resultados de pesquisa.
   - Incluir somente os recursos que correspondem a um filtro especificado

     Ativa a caixa de seleção Filtros de recursos, na qual você pode escolher nomes e operadores de filtro. Para obter uma explicação de cada um dos nomes e operadores de filtro disponíveis, consulte Filtros.
   - Escolha os atributos opcionais do recurso a serem incluídos nos resultados dessa visualização. Marque a caixa de seleção ao lado de Tags para permitir que os usuários pesquisem recursos com base nos nomes e nos valores das chaves de tag. Se você não incluir tags na visualização, os usuários não poderão fazer solicitações de pesquisa que usem chaves e valores de tag para filtrar ainda mais os resultados.

- Opcionalmente, você pode anexar tags à visualização. Expanda a caixa Tags e insira até 50 pares de chave/valor de tag. Você pode usar tags para categorizar recursos ou como parte de uma estratégia de permissão de segurança de controle de acesso (ABAC) baseada em atributos. Para obter mais informações, consulte Adicionar tags a visualizações.
- Escolha Criar visualização.

O console retorna à página Pesquisar, na qual você pode usar a nova visualização para realizar uma pesquisa.

Próxima etapa: conceda às entidades principais da conta permissões para pesquisar com a nova visualização. Para ter mais informações, consulte Conceder acesso às visualizações do Explorador de Recursos para pesquisa

AWS CLI

Para criar uma visualização

Execute o comando a seguir para criar uma visualização na Região da AWS especificada. O exemplo a seguir cria uma visualização que retorna somente recursos relacionados ao EC2 serviço da Amazon que estão marcados com uma `Stage` chave e o valor`prod`.

```
$ aws resource-explorer-2 create-view \
    --region us-west-2 \
    --view-name "My-EC2-Prod-Resources" \
    --filters FilterString="service:ec2 tag:stage=prod" \
    --included-properties Name=tags
{
    "View": {
        "Filters": {
            "FilterString": "service:ec2 tag:stage=prod"
        },
        "IncludedProperties": [
            {
                "Name": "tags"
            }
        ],
        "LastUpdatedAt": "2022-08-03T16:13:37.625000+00:00",
        "Owner": "123456789012",
        "Scope": "arn:aws:iam::123456789012:root",
```

```
        "ViewArn": "arn:aws:resource-explorer-2:us-west-2:123456789012:view/My-EC2-
Prod-Resources/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }
}
```

Para criar uma visualização no nível da organização

O exemplo a seguir cria uma visualização que retorna os recursos de toda a organização. Isso deve ser realizado pela conta de gerenciamento da organização ou por uma conta de administrador delegado.

1. Execute o `aws organizations describe-organization` comando para obter sua organizaçãoARN.
2. Execute o comando a seguir para criar uma visualização para a organização especificada.

```
$ aws resource-explorer-2 create-view \
    --region us-west-2 \
    --view-name entire-org-view \
    --scope "arn:aws:organizations::111111111111:organization/o-exampleorgid"
{
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [],
        "LastUpdatedAt": "2022-08-03T16:13:37.625000+00:00",
        "Owner": "111111111111",
        "Scope": "arn:aws:organizations::111111111111:organization/o-
exampleorgid",
        "ViewArn": "arn:aws:resource-explorer-2:us-west-2:111111111111:view/
entire-org-view/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }
}
```

Para criar uma visualização no nível da unidade organizacional

O exemplo a seguir cria uma visualização que retorna os recursos de todos os membros dessa unidade organizacional. Essa visualização se comporta de forma semelhante a uma visualização do nível organizacional. Isso deve ser realizado pela conta de gerenciamento da organização ou por uma conta de administrador delegado.

1. Execute o `aws organizations describe-organizational-unit` comando para obter sua organizaçãoARN.
2. Execute o comando a seguir para criar uma visualização para a unidade organizacional especificada.

```
$ aws resource-explorer-2 create-view \
    --region us-west-2 \
    --view-name entire-ou-view \
    --scope "arn:aws:organizations::222222222222:ou/o-exampleorgid/ou-
exampleouid"
{
    "View": {
        "Filters": {
            "FilterString": ""
        },
        "IncludedProperties": [],
        "LastUpdatedAt": "2022-08-03T16:13:37.625000+00:00",
        "Owner": "222222222222",
        "Scope": "arn:aws:organizations::222222222222:ou/o-exampleorgid/ou-
exampleouid",
        "ViewArn": "arn:aws:resource-explorer-2:us-west-2:222222222222:view/
entire-ou-view/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }
}
```

Próxima etapa: conceda às entidades principais da conta permissões para pesquisar com a nova visualização. Para ter mais informações, consulte Conceder acesso às visualizações do Explorador de Recursos para pesquisa

# Conceder acesso às visualizações do Explorador de Recursos para pesquisa

Antes de pesquisar com uma nova visualização, você deve conceder acesso às visualizações do Explorador de recursos da AWS. Para fazer isso, use uma política de permissão baseada em identidade para as entidades principais do AWS Identity and Access Management (IAM) que precisam pesquisar com a visualização.

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

- Usuários e grupos no AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Create a permission set (Criação de um conjunto de permissões) no Guia do usuário do AWS IAM Identity Center.
- Usuários gerenciados no IAM usando um provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criar um perfil para um provedor de identidades de terceiros (federação) no Guia do usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Creating a role for an IAM user (Criação de um perfil para um usuário do IAM) no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adicionar permissões a um usuário (console) no Guia do usuário do IAM.

Você pode usar um destes dois métodos:

- Use uma política gerenciada pela AWS existente. O Explorador de Recursos fornece várias políticas gerenciadas pela AWS predefinidas para seu uso. Para obter detalhes sobre todas as políticas gerenciadas pela AWS disponíveis, consulte AWS políticas gerenciadas para Explorador de recursos da AWS.

  Por exemplo, você pode usar a política `AWSResourceExplorerReadOnlyAccess` para conceder permissões de pesquisa a todas as visualizações na conta.
- Crie sua própria política de permissão e atribuí-la às entidades principais. Se você criar sua própria política, poderá restringir o acesso a uma única visualização ou a um subconjunto das visualizações disponíveis especificando o nome do recurso da Amazon (ARN) de cada visualização no elemento `Resource` da instrução da política. Por exemplo, você pode usar o exemplo de política a seguir para conceder a essa entidade principal a capacidade de pesquisar usando somente essa única visualização.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:Search",
```

```
                "resource-explorer-2:GetView"
            ],
            "Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyTestView/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
        }
    ]
}
```

Use o console do IAM para criar as políticas de permissão e use-as com as entidades principais que precisam dessas permissões. Para obter mais informações sobre as políticas de permissões do IAM, consulte os seguintes tópicos:

- Políticas e permissões no IAM
- Adicionar e remover permissões de identidade do IAM
- Noções básicas sobre as permissões concedidas por uma política

## Usar autorização baseada em tags para controlar o acesso às visualizações

Se você escolher criar várias visualizações com filtros que só retornem resultados com determinados recursos, talvez também queira restringir o acesso a essas visualizações apenas às entidades principais que precisam ver tais recursos. Você pode fornecer esse tipo de segurança para as visualizações da sua conta usando uma estratégia de controle de acesso por atributo (ABAC). Os atributos usados pelo ABAC são as tags anexadas às entidades principais que tentam realizar operações na AWS e aos recursos que elas tentam acessar.

O ABAC usa as políticas de permissão padrão do IAM anexadas às entidades principais. As políticas usam os elementos `Condition` nas instruções das políticas para só permitir acesso quando as tags anexadas à entidade principal solicitante e as tags anexadas ao recurso afetado corresponderem aos requisitos da política.

Por exemplo, você pode anexar uma tag `"Environment" = "Production"` a todos os recursos da AWS compatíveis com a aplicação de produção da sua empresa. Para garantir que somente as entidades principais autorizadas a acessar o ambiente de produção possam ver esses recursos, crie uma visualização do Explorador de Recursos que use essa tag como filtro. Depois, para restringir o acesso à visualização somente às entidades principais apropriadas, você concede permissões usando uma política que tem uma condição semelhante aos elementos do exemplo a seguir.

```
{
```

```
    "Effect": "Allow",
    "Action": [ "service:Action1", "service:Action2" ],
    "Resource": "arn:aws:arn-of-a-resource",
    "Condition": { "StringEquals": {"aws:ResourceTag/Environment":
 "${aws:PrincipalTag/Environment}"} }
}
```

A `Condition` do exemplo anterior especifica que a solicitação só será permitida se a tag `Environment` anexada à entidade principal solicitante corresponder à tag `Environment` anexada ao recurso especificado na solicitação. Se essas duas tags não corresponderem exatamente ou se alguma delas não estiver presente, o Explorador de Recursos negará a solicitação.

> **Important**
>
> Para usar o ABAC com sucesso para proteger o acesso aos recursos, você deve primeiro restringir o acesso à capacidade de adicionar ou modificar as tags anexadas às entidades principais e aos recursos. Se um usuário puder adicionar ou modificar as tags anexadas a uma entidade principal ou a um recurso da AWS, ele poderá afetar as permissões controladas por essas tags. Em um ambiente seguro de ABAC, somente os administradores de segurança aprovados têm permissão para adicionar ou modificar as tags anexadas às entidades principais, e somente os administradores de segurança e os proprietários dos recursos podem adicionar ou modificar as tags anexadas aos recursos.

Para obter mais informações sobre como implementar com sucesso uma estratégia de ABAC, consulte os seguintes tópicos no Guia do usuário do IAM:

- Tutorial do IAM: Definir permissões para acessar recursos da AWS com base em etiquetas
- Controlar o acesso a recursos da AWS usando tags

Depois de instalar a infraestrutura de ABAC necessária, você pode começar a usar tags para controlar quem pode pesquisar usando as visualizações do Explorador de Recursos em sua conta. Para obter exemplos de políticas que ilustram esse princípio, consulte os seguintes exemplos de políticas de permissões:

- Conceder acesso a uma visualização com base em tags
- Conceder acesso para criar uma visualização baseada em tags

# Definir uma visualização padrão em uma Região da AWS

No Explorador de recursos da AWS, você pode definir várias visualizações em uma Região da AWS, e cada visualização aborda diferentes requisitos de pesquisa. Recomendamos que você defina uma única visualização em cada região como a visualização padrão daquela região.

O Explorador de Recursos usa a visualização padrão sempre que um usuário realiza uma pesquisa e não especifica explicitamente qual visualização usar. A barra de pesquisa unificada na parte superior de cada página do AWS Management Console também usa automaticamente a visualização padrão da região que contém o índice agregador para encontrar os recursos que correspondem à consulta de pesquisa do usuário.

Você só pode selecionar uma visualização que já exista na região para ser a visualização padrão daquela região. Se outra região tiver uma visualização que você deseja usar, primeiro crie uma cópia dessa visualização na região em que deseja torná-la a visualização padrão.

> **Tip**
>
> Não existe uma operação copiar visualização. Você deve criar uma visualização na região de destino e, depois, copiar as configurações da visualização existente para a nova visualização.

Você pode especificar uma visualização como padrão para a região usando o AWS Management Console ou executando os comandos da AWS CLI ou as operações de API equivalentes em um SDK da AWS.

AWS Management Console

Para definir uma visualização padrão

1. Na página Visualizações do Explorador de Recursos, escolha o botão de opção ao lado da visualização que você deseja tornar padrão para a sua região.
2. Escolha Ações e depois Definir como padrão.

AWS CLI

Para definir uma visualização padrão

Execute o comando a seguir para definir a visualização especificada como padrão para a sua região. O exemplo a seguir define a visualização especificada como padrão para todas as pesquisas realizadas na região us-east-1. Essa visualização deve existir na região em que você executa o comando.

```
$ aws resource-explorer-2 associate-default-view \
    --region us-east-1 \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
}
```

# Adicionar tags a visualizações

Você pode adicionar tags às visualizações para categorizá-las. As tags são metadados fornecidos pelo cliente na forma de uma string de nome de chave e uma string opcional de valor associada. Para obter mais informações sobre como marcar os recursos da AWS, consulte Tagging AWS Resources no Referência geral da Amazon Web Services.

## Adicionar tags às visualizações

Você pode criar uma visualização do Explorador de Recursos usando o AWS Management Console ou executando os comandos da AWS CLI ou as operações da API equivalentes em um SDK da AWS.

AWS Management Console

Para adicionar tags a uma visualização

1. Abra a página Visualizações do Explorador de Recursos e escolha o nome da visualização que você deseja marcar para exibir sua página Detalhes.
2. Em Tags, selecione Manage tags (Gerenciar tags).
3. Para adicionar uma tag, escolha Adicionar tag e insira um nome de chave e um valor opcional de tag.

> **Note**
>
> Você também pode excluir uma tag escolhendo o X ao lado dela.

É possível anexar até 50 tags definidas pelo usuário a um recurso. As tags criadas e gerenciadas automaticamente pela AWS não contam para essa cota.

4. Quando terminar de fazer as alterações, escolha Salvar alterações.

AWS CLI

Para adicionar tags a uma visualização

Execute o comando a seguir para adicionar tags a uma visualização. O exemplo a seguir adiciona tags com o nome de chave `environment` e o valor `production` à visualização especificada.

```
$ aws resource-explorer-2 tag-resource \
    --resource-id arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111 \
    --tags environment=production
```

Se tiver sucesso, o comando anterior não produzirá nenhuma saída.

> **Note**
>
> Para remover uma tag existente de uma visualização, use o comando `untag-resource`.

## Controlar permissões com tags

Um dos principais usos das tags é possibilitar uma estratégia de controle de acesso por atributo (ABAC). O ABAC pode ajudar a simplificar o gerenciamento de permissões deixando que você marque os recursos. Depois, você concede aos usuários permissão para os recursos marcados de uma determinada maneira.

Por exemplo, considere este cenário: Em uma visualização denominada `ViewA`, você anexa a tag `environment=prod` (nome da chave = valor). Outra `ViewB` pode estar marcada como

`environment=beta`. Você marca os perfis e os usuários com as mesmas tags e valores, de acordo com o ambiente que cada perfil ou usuário deve poder acessar.

Depois, você pode atribuir uma política de permissão do AWS Identity and Access Management (IAM) aos perfis, grupos e usuários do IAM. A política só concederá permissão para acessar e pesquisar usando uma visualização se o perfil ou o usuário que fizer a solicitação de pesquisa tiver uma tag `environment` com o mesmo valor da tag `environment` anexada à visualização.

A vantagem dessa abordagem é que ela é dinâmica e não exige que você mantenha uma lista de quem tem acesso a quais recursos. Em vez disso, você garante que todos os recursos (suas visualizações) e entidades principais (perfis e usuários do IAM) sejam marcados corretamente. Assim, as permissões são atualizadas automaticamente sem que você precise alterar nenhuma política.

## Referenciar tags em uma política de ABAC

Depois que as visualizações são marcadas, você pode escolher usar essas tags para controlar dinamicamente o acesso às visualizações. O exemplo de política a seguir pressupõe que tanto as entidades principais do IAM quanto as visualizações estejam marcadas com a chave de tag `environment` e algum valor. Quando isso é concluído, você pode anexar o exemplo de política a seguir às entidades principais. Os perfis e usuários podem então `Search` usando qualquer visualização marcada com um valor de tag `environment` que corresponda exatamente à tag `environment` anexada à entidade principal.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetView",
                "resource-explorer-2:Search"
            ],
            "Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:ResourceTag/environment": "${aws:PrincipalTag/environment}"
                }
            }
        }
```

```
    ]
}
```

Se a entidade principal e a visualização tiverem a tag `environment`, mas os valores não corresponderem, ou se a tag `environment` estiver ausente, o Explorador de Recursos negará a solicitação de pesquisa.

Para obter mais informações sobre como usar o ABAC para conceder acesso seguro aos recursos, consulte O que é ABAC para a AWS?

## Compartilhar visualizações do Explorador de Recursos

As visualizações usam Explorador de recursos da AWS principalmente políticas baseadas em recursos para conceder acesso. Como acontece com as políticas de bucket do Amazon S3, essas políticas são anexadas à visualização e especificam quem pode usá-la. Isso contrasta com as políticas baseadas em identidade AWS Identity and Access Management (IAM). Uma política IAM baseada em identidade é atribuída a uma função, grupo ou usuário e especifica quais ações e recursos essa função, grupo ou usuário pode acessar. Você pode usar qualquer tipo de política com as visualizações do Explorador de Recursos, da seguinte maneira:

- Na conta de gerenciamento ou na conta de administrador delegado que é a proprietária do recurso, use um dos dois tipos de política para conceder acesso, desde que nenhuma outra política negue explicitamente o acesso à visualização dessa entidade principal.
- Entre contas, você deve usar ambos os tipos de política. A política baseada em recurso anexada à visualização na conta compartilhadora ativa o compartilhamento com outra conta consumidora. Porém, essa política não concede acesso a usuários ou perfis individuais na conta consumidora. O administrador da conta consumidora também deve atribuir uma política baseada em identidade aos perfis e usuários desejados na conta consumidora. Essa política concede acesso ao nome do recurso Amazon (ARN) da visualização.

Para compartilhar visualizações com outras contas, você deve usar AWS Resource Access Manager (AWS RAM). AWS RAM lida com a complexidade das políticas baseadas em recursos para você. Antes de poder compartilhar, você deve realizar as seguintes tarefas:

- Ative a pesquisa em várias contas.
- Certifique-se de que sua política baseada em recursos ou a política IAM baseada em identidade que você usa para compartilhar e não compartilhar visualizações inclua

as permissões e. `resource-explorer-2:GetResourcePolicy` `resource-explorer-2:PutResourcePolicy` `resource-explorer-2:DeleteResourcePolicy`

Para compartilhar uma visualização, você deve ser o administrador da conta de gerenciamento da organização ou um administrador delegado. Você especifica as contas ou identidades com as quais deseja compartilhar o recurso. AWS RAM suporta totalmente as visualizações do Resource Explorer. AWS RAM usa políticas semelhantes às descritas nas seções a seguir, com base nos tipos de diretores com os quais você escolhe compartilhar. Para obter instruções sobre como compartilhar recursos, consulte Sharing your AWS resources no AWS Resource Access Manager User Guide.

Administradores e administradores delegados podem criar e compartilhar três tipos de visualizações: visualização com escopo do nível de organização, visualizações com escopo do nível de unidade organizacional (UO) e visualizações com escopo do nível de conta. Eles podem compartilhar com organizações ou contas. OUs Quando as contas entram ou saem da organização, concede ou revoga AWS RAM automaticamente a visualização compartilhada.

## Política de permissões para compartilhar a visualização com as Contas da AWS

O exemplo de política a seguir mostra como você pode disponibilizar uma visualização para os diretores de duas maneiras diferentes Contas da AWS:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [ "111122223333", "444455556666" ]
            },
            "Action": [
                "resource-explorer-2:Search",
                "resource-explorer-2:GetView",
            ],
            "Resource": "arn:aws:resource-explorer-2:us-
east-1:123456789012:view/policy-name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
            "Condition": {"StringEquals": {"aws:PrincipalOrgID": "o-123456789012"},
                "StringNotEquals": {"aws:PrincipalAccount": "123456789012"}
            }
        }
```

```
    ]
    }"
}
```

O administrador de cada uma das contas especificadas deve especificar agora quais funções e usuários podem acessar a visualização anexando políticas de permissões baseadas em identidade aos perfis, grupos e usuários. Os administradores das contas 111122223333 ou 444455556666 podem criar o exemplo de política a seguir. Depois, eles podem atribuir a política aos perfis, grupos e usuários dessas contas que tem permissão para pesquisar usando a visualização compartilhada da conta de origem.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:Search",
                "resource-explorer-2:GetView",
            "Resource": "arn:aws:resource-explorer-2:us-
east-1:123456789012:view/policy-name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
        }
    ]
}
```

Você pode usar essas políticas IAM baseadas em identidade como parte de uma estratégia de segurança de controle de acesso () ABAC baseada em atributos. Nesse paradigma, você garante que todos os seus recursos e identidades estejam marcados. Depois, você especifica nas políticas quais chaves e valores de tag devem corresponder entre a identidade e o recurso para que o acesso seja permitido. Para obter informações sobre como marcar as visualizações da sua conta, consulte Adicionar tags a visualizações. Para obter mais informações sobre controle de acesso baseado em atributos, consulte Para que serveABAC? AWS e Controle do acesso aos AWS recursos usando tags, ambos no Guia IAM do usuário.

# Excluir visualizações no Explorador de Recursos

Quando você não precisar mais de uma visualização do Explorador de recursos da AWS, poderá excluí-la. Você pode excluir visualizações usando o AWS Management Console ou executando os comandos da AWS CLI ou as operações de API equivalentes em um SDK da AWS.

> **Note**
>
> Você não pode excluir uma visualização que esteja designada como padrão para a sua Região da AWS. Para excluir a visualização, você deve remover a visualização como o padrão. Para fazer isso, você pode executar a operação de API DisassociateDefaultView naquela região.

### Permissões mínimas

Para executar esse comando, você deve ter as seguintes permissões:

- Ação: `resource-explorer-2:DeleteView`

  Recurso: o ARN da visualização a ser excluída

### AWS Management Console

Para excluir uma visualização

1. Na página Visualizações do console do Explorador de Recursos, escolha o botão de opção ao lado da visualização que você deseja excluir.
2. Escolha Actions (Ações) e, em seguida, escolha Delete (Excluir).
3. Na caixa de confirmação, digite o nome da visualização e escolha Excluir.

### AWS CLI

Para excluir uma visualização

Execute o comando a seguir para excluir a visualização com o nome do recurso da Amazon (ARN) especificado.

```
$ aws resource-explorer-2 delete-view \
    --view-arn arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
{
    "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
MyViewName/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
}
```

# Usar o Explorador de recursos da AWS para pesquisar recursos

O objetivo principal de habilitar o Explorador de recursos da AWS em sua Conta da AWS é permitir que os usuários pesquisem recursos na conta. Use o AWS Management Console ou a AWS Command Line Interface (AWS CLI) para pesquisar recursos usando o Explorador de Recursos.

A seguir estão algumas das principais características da pesquisa do Explorador de Recursos.

- Toda pesquisa deve usar uma visualização.

  A visualização é o que o Explorador de Recursos usa para determinar quem tem permissões para ver quais recursos. Para usar uma visualização em uma operação de pesquisa do Explorador de Recursos, o usuário deve ter uma permissão `Allow` na operação `resource-explorer-2:Search` da visualização especificada. Essa permissão vem de uma política de permissão baseada em identidade anexada à entidade principal que fez a solicitação.

  A visualização pode incluir um filtro que limite quais recursos podem ser incluídos nos resultados. Criando visualizações diferentes que usam filtros e concedendo a diferentes entidades principais acesso a diferentes visualizações, você pode configurar um ambiente em que cada grupo de usuários só pode visualizar os recursos relevantes para eles.

  Para obter mais informações sobre visualizações, consulte Gerenciar visualizações do Explorador de Recursos para fornecer acesso para pesquisa.

- O Explorador de Recursos usa processos assíncronos em segundo plano para manter seus índices.

  O Explorador de Recursos pode levar algum tempo para que seus processos de indexação descubram os recursos recém-criados ou modificados e os adicionem ao índice local. Pode levar um tempo adicional para que o Explorador de Recursos replique as alterações feitas nos índices locais no índice agregador.

  O mesmo se aplica aos recursos que você exclui. Pode levar algum tempo para que essa exclusão seja descoberta pelo processo de indexação e para que as informações daquele recurso sejam removidas do índice local. É necessário tempo adicional para que o Explorador de Recursos replique essa exclusão do índice local no índice agregador da conta.

O Explorador de Recursos pode levar até 36 horas para mostrar as adições, modificações e exclusões feitas nos recursos nos resultados de pesquisa em todas as regiões em que você ativou o Explorador de Recursos.

- Uma pesquisa no Explorador de Recursos ocorre em uma Região da AWS.

  Cada região em que você ativa o Explorador de Recursos contém um índice apenas dos recursos armazenados naquela região. As visualizações também estão associadas às regiões e só podem retornar os recursos encontrados no índice daquela região. A única exceção é o índice agregador, que recebe uma cópia replicada de todos os índices locais para possibilitar a pesquisa em todas as regiões da conta.

- A pesquisa entre regiões exige um índice agregador para a conta.

  Para permitir que os usuários pesquisem recursos em todas as Regiões da AWS, o administrador deve designar uma região para conter o índice agregador da conta. Uma cópia de cada índice local é automaticamente replicada no índice agregador.

  Por isso, apenas as visualizações na região do índice agregador podem retornar resultados que incluam recursos de todas as Regiões da AWS na conta.

- Uma consulta consiste em qualquer número de palavras-chave e filtros de texto em formato livre.

  Palavras-chave em formato livre são combinadas na consulta usando operadores lógicos **OR**. Os filtros que usam nomes de filtro definidos pelo Explorador de Recursos são combinados na consulta usando operadores lógicos **AND**. Considere o exemplo de consulta a seguir.

  ```
  test instance service:EC2 region:us-west-2
  ```

  Isso é avaliado pelo Explorador de Recursos como se segue.

  ```
  test OR instance AND service:EC2 AND region:us-west-2
  ```

  Essa consulta exige que os recursos correspondentes sejam recursos do Amazon EC2 na região Oeste dos EUA (Oregon) e tenham pelo menos uma das palavras-chave (teste, instância) anexada de alguma forma, como nome, descrição ou tags.

> **Note**
>
> Por causa do AND implícito, você só pode usar com sucesso um único filtro para um atributo que só pode ter um valor associado ao recurso. Por exemplo, um recurso não pode fazer parte de mais de uma Região da AWS. Portanto, a consulta a seguir não retorna nenhum resultado.
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> Essa limitação não se aplica aos filtros de atributos que podem ter vários valores ao mesmo tempo, como `tag:`, `tag.key:` e `tag.value:`.

- Uma pesquisa só pode retornar os primeiros 1.000 resultados.

  Esse requisito inclui uma pesquisa com uma string de consulta vazia que corresponde a todos os recursos. Para ver recursos além dos 1.000 retornados por uma string de consulta vazia, você deve usar consultas para restringir os resultados encontrados aos que deseja ver e limitar o número de correspondências a menos de 1.000.
- Existe uma cota por conta para o número de operações de pesquisa que podem ser executadas.

  As cotas limitam quantas consultas você pode fazer por segundo e quantas consultas pode fazer por mês. Para obter as cotas específicas, consulte Cotas do Explorador de Recursos.

AWS Management Console

Para pesquisar recursos usando o Explorador de Recursos

1. Na página Pesquisa de recursos, comece escolhendo a visualização que deseja usar. Você só pode escolher entre as visualizações para as quais tem permissão de acesso.
2. Em Consulta, insira os termos e filtros de pesquisa que identificam os recursos que você deseja ver. Para obter informações sobre todas as opções de sintaxe disponíveis, consulte Referência da sintaxe de consulta de pesquisa do Explorador de Recursos.
3. Pressione Enter para enviar sua escolha.

   O Explorador de Recursos exibe todos os resultados que correspondem ao `Filter` definido na visualização e à consulta fornecida. Os resultados são classificados por relevância, com

os recursos que correspondem a mais termos da consulta aparecendo no topo da lista e os recursos que correspondem a menos termos aparecendo mais abaixo na lista.

4. Escolha o identificador de um recurso para navegar até o console nativo desse tipo de recurso, onde você pode interagir com o recurso de todas as formas compatíveis com esse serviço.

AWS CLI

Para pesquisar recursos usando o Explorador de Recursos

Execute o comando a seguir para pesquisar recursos usando a visualização especificada. Essa visualização deve existir na região em que você executa a operação. O exemplo a seguir pesquisa instâncias do Amazon EC2 que estão marcadas como `env=production` na região Leste dos EUA (Ohio) (us-east-2). Para obter informações sobre todas as opções de sintaxe disponíveis para o parâmetro `query-string`, consulte Referência da sintaxe de consulta de pesquisa do Explorador de Recursos.

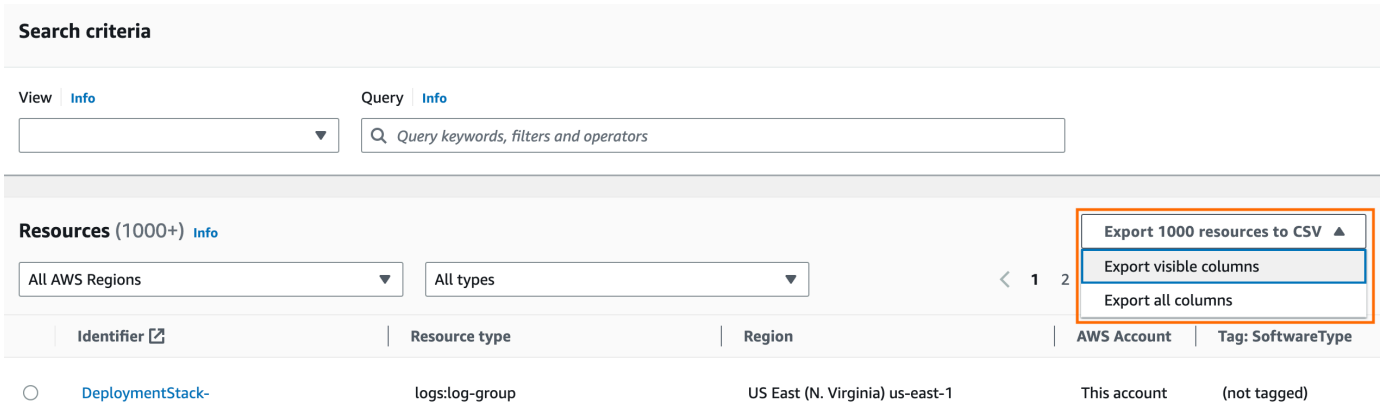
```
$ aws resource-explorer-2 search \
    --region us-east-1 \
    --query-string "resourcetype:AWS::EC2::Instance tag:env=production"
    --view-arn arn:aws:resource-explorer-2:us-east-2:123456789012:view/My-Resources-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

# Exportar resultados da pesquisa para um arquivo.csv

Você pode exportar os resultados de uma consulta de pesquisa de recurso para um arquivo de valores separados por vírgulas (.csv). O arquivo .csv inclui o identificador, o tipo de recurso, a região, a Conta da AWS, o número total de tags e uma coluna para cada chave de tag exclusiva no conjunto. O arquivo .csv pode ajudar a configurar os recursos da AWS na sua organização ou a determinar onde há sobreposições ou inconsistências na marcação entre recursos.

1. Nos resultados da consulta Pesquisa de recurso, escolha Exportar recursos para CSV.

   Você pode escolher exportar os resultados apenas com as colunas que pode ver no momento ou com todas as colunas disponíveis.




2. Quando solicitado pelo navegador, escolha abrir o arquivo .csv ou salvá-lo em um local conveniente.

# Tipos de recursos que você pode pesquisar com o Explorador de Recursos

O Resource Explorer oferece suporte a tipos de recursos em vários AWS serviços.

Tópicos



Alguns tipos de recursos são identificados por cadeias de caracteres de nome de recurso (ARN) da Amazon que compartilham um formato comum com outro tipo de recurso. Quando isso acontece, o Explorador de Recursos pode listar esses recursos como sendo esse outro tipo de recurso. Para obter uma lista dos tipos de recursos afetados por esse problema, consulte Tipos de recursos que aparecem como outros tipos.

No momento, as tags anexadas aos recursos AWS Identity and Access Management (IAM), como funções ou usuários, não podem ser usadas para pesquisa.

Se você tiver acesso criptografado a alguns dos recursos, o Explorador de Recursos não conseguirá descobri-los. Você não verá esses recursos nos resultados da pesquisa.

As tabelas a seguir listam os tipos de recursos que são compatíveis com pesquisa no Explorador de recursos da AWS.

> **Note**
>
> A partir de 9 de julho de 2024, o Resource Explorer não oferece mais suporte aos seguintes tipos de recursos:
>
> - Amazon Elastic Container Service — `ecs:task`
> - AWS Systems Manager — `ssm:automation-execution`
> - AWS Systems Manager — `ssm:patchbaseline`

Você ainda pode usar esses tipos de recursos em seus próprios serviços, mas eles não são mais indexados ou pesquisáveis no Resource Explorer.

# Serviços e tipos de recursos compatíveis

Suportado Serviços da AWS

- Amazon API Gateway
- AWS App Runner
- Amazon AppStream 2.0
- AWS AppSync
- Amazon Athena
- AWS Backup
- AWS Batch
- AWS CloudFormation
- Amazon CloudFront
- AWS CloudTrail
- Amazon CloudWatch
- Amazon, CloudWatch evidentemente
- CloudWatch Registros da Amazon
- AWS CodeArtifact
- AWS CodeBuild
- AWS CodeCommit
- Amazon CodeGuru Profiler
- AWS CodePipeline
- Conexões de código da AWS
- Amazon Cognito
- Amazon Connect
- Amazon Connect Wisdom
- Amazon Detective

- Amazon DynamoDB
- EC2Image Builder
- Amazon ECR Public
- AWS Elastic Beanstalk
- Amazon ElastiCache
- Nuvem de computação elástica da Amazon (AmazonEC2)
- Amazon Elastic Container Registry
- Amazon Elastic Container Service
- Amazon Elastic File System
- Elastic Load Balancing
- AWS Elemental MediaPackage
- AWS Elemental MediaTailor
- Amazon sem EMR servidor
- Amazon EventBridge
- AWS Fault Injection Service
- Amazon Forecast
- Amazon Fraud Detector
- Amazon GameLift
- AWS Global Accelerator
- AWS Glue
- AWS Glue DataBrew
- AWS Identity and Access Management
- Amazon Interactive Video Service
- AWS IoT
- AWS IoT Analytics
- AWS IoT Events
- AWS IoT Greengrass Version 1
- AWS IoT SiteWise

- AWS IoT TwinMaker
- AWS Key Management Service
- Amazon Kinesis
- Amazon Data Firehose
- Amazon Kinesis Video Streams
- AWS Lambda
- Amazon Lex
- Amazon Location Service
- Amazon Lookout for Metrics
- Amazon Lookout for Vision
- Amazon Managed Service for Apache Flink
- Amazon Managed Service para Prometheus
- Amazon Managed Service para Prometheus
- Amazon Managed Streaming for Apache Kafka
- AWS Migration Hub Refactor Spaces
- AWS Network Firewall
- AWS Network Manager
- OpenSearch Serviço Amazon
- AWS Panorama
- Amazon Personalize
- AWS Private Certificate Authority
- Amazon QLDB
- Amazon Redshift
- Amazon Rekognition
- Amazon Relational Database Service (AmazonRDS)
- AWS Resilience Hub
- AWS Resource Groups
- Explorador de recursos da AWS
- Amazon Route 53

- Amazon Route 53 Recovery Readiness
- Amazon Route 53 Resolver
- Amazon SageMaker
- AWS Secrets Manager
- AWS Service Catalog
- Amazon Simple Notification Service
- Amazon Simple Queue Service
- Amazon Simple Storage Service (Amazon S3)
- AWS Step Functions
- AWS Systems Manager
- Acesso Verificado pela AWS
- AWS Wavelength

## Amazon API Gateway

- `apigateway:restapis`

## AWS App Runner

- `apprunner:vpcconnector`

## Amazon AppStream 2.0

- `appstream:appblock`
- `appstream:application`
- `appstream:fleet`
- `appstream:stack`

## AWS AppSync

- `appsync:apis`

## Amazon Athena

- athena:datacatalog
- athena:workgroup

## AWS Backup

- backup:backupplan

## AWS Batch

- batch:computeenvironment
- batch:jobqueue
- batch:schedulingpolicy

## AWS CloudFormation

- cloudformation:stack
- cloudformation:stackset

## Amazon CloudFront

- cloudfront:cache-policy
- cloudfront:distribution
- cloudfront:function
- cloudfront:fieldlevelencryptionconfig
- cloudfront:fieldlevelencryptionprofile
- cloudfront:origin-access-identity
- cloudfront:originaccesscontrol
- cloudfront:origin-request-policy
- cloudfront:realtime-log-config
- cloudfront:response-headers-policy

## AWS CloudTrail

- cloudtrail:trail

## Amazon CloudWatch

- cloudwatch:alarm
- cloudwatch:dashboard
- cloudwatch:insight-rule
- cloudwatch:metric-stream
- evidently:project

## Amazon, CloudWatch evidentemente

- evidently:project/experiment
- evidently:project/feature
- evidently:project/launch

## CloudWatch Registros da Amazon

- logs:destination
- logs:log-group

## AWS CodeArtifact

- codeartifact:domain
- codeartifact:repository

## AWS CodeBuild

- codebuild:project

## AWS CodeCommit

- codecommit:repository

## Amazon CodeGuru Profiler

- codeguru-profiler:profilingGroup

## AWS CodePipeline

- codepipeline:pipeline

## Conexões de código da AWS

- codestarconnections:connect

## Amazon Cognito

- cognito:identitypool
- cognito:userpool

## Amazon Connect

- appintegrations:eventintegration

## Amazon Connect Wisdom

- wisdom:assistant
- wisdom:association
- wisdom:knowledge-base

## Amazon Detective

- detective:graph

## Amazon DynamoDB

- dynamodb:table

## EC2Image Builder

- imagebuilder:component
- imagebuilder:containerrecipe
- imagebuilder:distributionconfiguration
- imagebuilder:image
- imagebuilder:imagepipeline
- imagebuilder:imagerecipe
- imagebuilder:infrastructureconfiguration

## Amazon ECR Public

- ecrpublic:repository

## AWS Elastic Beanstalk

- elasticbeanstalk:application
- elasticbeanstalk:applicationversion
- elasticbeanstalk:configurationtemplate
- elasticbeanstalk:environment

## Amazon ElastiCache

- elasticache:cluster
- elasticache:globalreplicationgroup

- elasticache:parametergroup
- elasticache:replicationgroup
- elasticache:reserved-instance
- elasticache:snapshot
- elasticache:subnetgroup
- elasticache:user
- elasticache:usergroup

## Nuvem de computação elástica da Amazon (AmazonEC2)

- ec2:capacity-reservation
- ec2:capacity-reservation-fleet
- ec2:client-vpn-endpoint
- ec2:customer-gateway
- ec2:dedicated-host
- ec2:dhcp-options
- ec2:egress-only-internet-gateway
- ec2:elastic-gpu
- ec2:elastic-ip
- ec2:fleet
- ec2:fpga-image
- ec2:host-reservation
- ec2:image
- ec2:instance
- ec2:instance-event-window
- ec2:internet-gateway
- ec2:ipam
- ec2:ipam-pool
- ec2:ipam-scope
- ec2:ipv4pool-ec2

- ec2:key-pair
- ec2:launch-template
- ec2:natgateway
- ec2:network-acl
- ec2:network-insights-access-scope
- ec2:network-insights-access-scope-analysis
- ec2:network-insights-analysis
- ec2:network-insights-path
- ec2:network-interface
- ec2:placement-group
- ec2:prefix-list
- ec2:reserved-instances
- ec2:route-table
- ec2:security-group
- ec2:security-group-rule
- ec2:snapshot
- ec2:spot-fleet-request
- ec2:spot-instances-request
- ec2:subnet
- ec2:subnet-cidr-reservation
- ec2:traffic-mirror-filter
- ec2:traffic-mirror-filter-rule
- ec2:traffic-mirror-session
- ec2:traffic-mirror-target
- ec2:transit-gateway
- ec2:transit-gateway-attachment
- ec2:transit-gateway-connect-peer
- ec2:transit-gateway-multicast-domain
- ec2:transit-gateway-policy-table
- ec2:transit-gateway-route-table

- ec2:transitgatewayroutetableannouncement
- ec2:volume
- ec2:vpc
- ec2:vpc-endpoint
- ec2:vpc-flow-log
- ec2:vpc-peering-connection
- ec2:vpn-connection
- ec2:vpn-gateway

## Amazon Elastic Container Registry

- ecr:repository

## Amazon Elastic Container Service

- ecs:cluster
- ecs:container-instance
- ecs:service
- ecs:task-definition
- ecs:task-set

## Amazon Elastic File System

- efs:filesystem
- efs:accesspoint

## Elastic Load Balancing

- elasticloadbalancing:listener
- elasticloadbalancing:listener-rule
- elasticloadbalancing:listener-rule/app
- elasticloadbalancing:listener/app

- elasticloadbalancing:listener/net
- elasticloadbalancing:loadbalancer
- elasticloadbalancing:loadbalancer/app
- elasticloadbalancing:loadbalancer/net
- elasticloadbalancing:targetgroup

## AWS Elemental MediaPackage

- mediapackage:channel
- mediapackage:originendpoint
- mediapackage-vod:packaging-configurations
- mediapackage-vod:packaging-groups

## AWS Elemental MediaTailor

- mediatailor:playbackConfiguration

## Amazon sem EMR servidor

- emr-serverless:applications

## Amazon EventBridge

- events:event-bus
- events:rule

## AWS Fault Injection Service

- fis:experimenttemplate

## Amazon Forecast

- forcast:dataset

- forcast:dataset-group

## Amazon Fraud Detector

- frauddetector:detector
- frauddetector:entity-type
- frauddetector:event-type
- frauddetector:label
- frauddetector:outcome
- frauddetector:variable

## Amazon GameLift

- gamelift:alias

## AWS Global Accelerator

- globalaccelerator:accelerator
- globalaccelerator:accelerator/listener
- globalaccelerator:accelerator/listener/endpoint-group

## AWS Glue

- glue:database
- glue:job
- glue:table
- glue:trigger

## AWS Glue DataBrew

- databrew:dataset
- databrew:recipe

- databrew:ruleset

## AWS Identity and Access Management

- iam:group
- iam:instance-profile
- iam:oidc-provider
- iam:policy
- iam:role
- iam:saml-provider
- iam:server-certificate
- iam:user
- iam:virtualmfadevice

## Amazon Interactive Video Service

- ivs:channel
- ivs:streamkey

## AWS IoT

- iot:authorizer
- iot:jobtemplate
- iot:mitigationaction
- iot:policy
- iot:provisioningtemplate
- iot:rolealias
- iot:securityprofile
- iot:thing
- iot:topicrule

## AWS IoT Analytics

- iotanalytics:channel
- iotanalytics:dataset
- iotanalytics:datastore
- iotanalytics:pipeline

## AWS IoT Events

- iotevents:alarmModel
- iotevents:detectorModel
- iotevents:input

## AWS IoT Greengrass Version 1

- greengrass:components
- greengrass:groups

## AWS IoT SiteWise

- iotsitewise:asset
- iotsitewise:assetmodel
- iotsitewise:gateway

## AWS IoT TwinMaker

- iottwinmaker:workspace
- iottwinmaker:workspace/component-type
- iottwinmaker:workspace/entity

## AWS Key Management Service

- kms:key

## Amazon Kinesis

- `kinesis:stream`

## Amazon Data Firehose

- `kinesisfirehose:deliverystream`

## Amazon Kinesis Video Streams

- `kinesisvideo:stream`

## AWS Lambda

- `lambda:code-signing-config`
- `lambda:event-source-mapping`
- `lambda:function`

## Amazon Lex

- `lex:bot`

## Amazon Location Service

- `geo:place-index`
- `geo:tracker`

## Amazon Lookout for Metrics

- `lookoutmetrics:Alert`

## Amazon Lookout for Vision

- lookoutvision:project

## Amazon Managed Service for Apache Flink

- kinesisanalytics:application

## Amazon Managed Service para Prometheus

- aps:rulegroupsnamespace
- aps:workspace

## Amazon Managed Service para Prometheus

- memorydb:cluster
- memorydb:parametergroup
- memorydb:user

## Amazon Managed Streaming for Apache Kafka

- kafka:cluster
- kafka:configuration

## AWS Migration Hub Refactor Spaces

- refactor-spaces:environment
- refactor-spaces:environment/application
- refactor-spaces:environment/application/route
- refactor-spaces:environment/application/service

## AWS Network Firewall

- network-firewall:firewall-policy

## AWS Network Manager

- networkmanager:core-network
- networkmanager:device
- networkmanager:global-network
- networkmanager:link

## OpenSearch Serviço Amazon

- es:domain

## AWS Panorama

- panorama:package

## Amazon Personalize

- personalize:dataset
- personalize:dataset-group
- personalize:schema

## AWS Private Certificate Authority

- acmpca:certificateauthority

## Amazon QLDB

- qldb:ledger
- qldb:stream

## Amazon Redshift

- redshift:cluster
- redshift:eventsubscription
- redshift:parametergroup
- redshift:snapshot
- redshift:snapshotcopygrant
- redshift:snapshotschedule
- redshift:subnetgroup
- redshift:usagelimit

## Amazon Rekognition

- rekognition:project

## Amazon Relational Database Service (AmazonRDS)

- rds:auto-backup
- rds:cev
- rds:cluster
- rds:cluster-endpoint
- rds:cluster-pg
- rds:cluster-snapshot
- rds:db
- rds:db-proxy
- rds:db-proxy-endpoint
- rds:deployment
- rds:es
- rds:global-cluster
- rds:og
- rds:pg

- rds:ri
- rds:secgrp
- rds:snapshot
- rds:subgrp

## AWS Resilience Hub

- resiliencehub:resiliencypolicy

## AWS Resource Groups

- resourcegroups:group

## Explorador de recursos da AWS

- resource-explorer-2:index
- resource-explorer-2:view

## Amazon Route 53

- route53:healthcheck
- route53:hostedzone

## Amazon Route 53 Recovery Readiness

- route53-recover-readiness:recovery-group
- route53-recover-readiness:resource-set

## Amazon Route 53 Resolver

- route53resolver:firewalldomainlist
- route53resolver:firewallrulegroup
- route53resolver:resolverendpoint

- route53resolver:resolverrule

## Amazon SageMaker

- sagemaker:model
- sagemaker:notebookinstance

## AWS Secrets Manager

- secretsmanager:secret

## AWS Service Catalog

- servicecatalog:applications
- servicecatalog:attribute-groups

## Amazon Simple Notification Service

- sns:topic

## Amazon Simple Queue Service

- sqs:queue

## Amazon Simple Storage Service (Amazon S3)

- s3:accesspoint
- s3:bucket
- s3:storage-lens

## AWS Step Functions

- states:statemachine

- `stepfunctions:activity`

### AWS Systems Manager

- `ssm:association`
- `ssm:document`
- `ssm:maintenancewindow`
- `ssm:managed-instance`
- `ssm:parameter`
- `ssm:resourcedatasync`
- `ssm:windowtarget`
- `ssm:windowtask`

### Acesso Verificado pela AWS

- `ec2:verifiedaccessendpoint`
- `ec2:verifiedaccessgroup`
- `ec2:verifiedaccessinstance`
- `ec2:verifiedaccesstrustprovider`

### AWS Wavelength

- `ec2:carriergateway`

## Acessar programaticamente a lista de tipos de recursos compatíveis

Para acessar a lista de tipos de recursos compatíveis a partir do código, você pode invocar a ListSupportedResourceTypesoperação a partir de qualquer AWS SDK um.

Por exemplo, você pode executar o comando list-supported-resource-types AWS Command Line Interface (AWS CLI), conforme mostrado no exemplo a seguir.

```
$ aws resource-explorer-2 list-supported-resource-types
{
    "ResourceTypes": [
        {
            "ResourceType": "acm-pca:certificate-authority",
            "Service": "acm-pca"
        },
        {
            "ResourceType": "airflow:environment",
            "Service": "airflow"
        },
        {
            "ResourceType": "amplify:branches",
            "Service": "amplify"
        },
... truncated for brevity ...
```

## Tipos de recursos que aparecem como outros tipos

Alguns tipos de recursos são identificados por cadeias de caracteres de nome de recurso (ARN) da Amazon que compartilham um formato comum com outro tipo de recurso. Quando isso acontece, o Explorador de Recursos pode listar esses recursos como sendo esse outro tipo de recurso. Isso afeta os tipos de recurso da tabela a seguir.

| Tipo de recurso real | Listado como tipo de recurso |
| --- | --- |
| `ec2:securitygroupegress`<br>`ec2:securitygroupingress` | `ec2:security-group-rule` |
| `elasticloadbalancingv2:loadbalancer` | `elasticloadbalancing:loadbalancer` |
| `docdb:dbcluster`<br>`neptune:dbcluster`<br>`rds:dbcluster` | `rds:cluster` |
| `docdb:dbclusterparametergroup` | `rds:cluster-pg` |

| Tipo de recurso real | Listado como tipo de recurso |
| --- | --- |
| neptune:dbclusterparametergroup<br>rds:dbclusterparametergroup | |
| docdb:clustersnapshot<br>neptune:dbclustersnapshot<br>rds:clustersnapshot | rds:cluster-snapshot |
| docdb:dbinstance<br>neptune:dbinstance<br>rds:dbinstance | rds:db |
| docdb:eventsubscription<br>neptune:eventsubscription<br>rds:eventsubscription | rds:es |
| docdb:globalcluster<br>rds:globalcluster | rds:global-cluster |
| neptune:dbparametergroup<br>rds:dbparametergroup | rds:pg |
| docdb:dbsubnetgroup<br>neptune:dbsubnetgroup<br>rds:dbsubnetgroup | rds:subgrp |

# Referência da sintaxe de consulta de pesquisa do Explorador de Recursos

Explorador de recursos da AWS ajuda você a encontrar AWS recursos individuais em seu Contas da AWS. Para ajudar você a encontrar os recursos exatos que está procurando, o Explorador de Recursos aceita strings de consulta de pesquisa que sigam a sintaxe descrita neste tópico. Para obter exemplos de consultas que demonstram como usar os recursos descritos aqui, consulte Exemplo de consultas de pesquisa do Explorador de Recursos.

> **Note**
>
> No momento, as tags anexadas aos recursos AWS Identity and Access Management (IAM), como funções ou usuários, não são indexadas.

## Como as consultas funcionam no Explorador de Recursos

As consultas de pesquisa sempre usam uma visualização. Se você não especificar explicitamente uma, o Resource Explorer usará a visualização designada como padrão para Região da AWS aquela em que você está trabalhando.

As visualizações determinam quais recursos estão disponíveis para você consultar. Você pode criar diferentes visualizações, cada uma retornando um conjunto diferente de recursos.

Por exemplo, você pode criar uma visualização que inclua somente os recursos marcados com a chave `Environment` e o valor `Production`. Depois, você pode escolher só conceder acesso a essa visualização aos usuários que têm um motivo comercial para visualizar esses recursos. Uma visualização separada que inclua os recursos do ambiente `Alpha` ou `Beta` pode ser acessada por diferentes usuários que precisam visualizar esses recursos. Para obter mais informações sobre como controlar quem tem acesso a qual visualização, consulte Conceder acesso às visualizações do Explorador de Recursos para pesquisa.

## Sintaxe da string de consulta

Esta seção fornece informações sobre aspectos básicos da sintaxe de consulta, dos filtros e dos operadores de filtro.

## Conceitos básicos

Basicamente, uma `QueryString` é um conjunto de palavras-chave de texto em formato livre que são unidas implicitamente por um operador lógico **`OR`**. Separe as palavras-chaves umas das outras com um espaço, como mostrado no seguinte exemplo:

```
ec2 billing test gamma
```

O Explorador de Recursos avalia que essa lista de palavras-chave significa:

```
ec2 OR billing OR test OR gamma
```

O Explorador de Recursos classifica os resultados por relevância, dando maior preferência aos recursos que correspondem a um número maior de termos de pesquisa. Os recursos que não correspondem a um ou mais termos não são excluídos dos resultados. Porém, o Explorador de Recursos os considera de menor relevância e os empurra ainda mais para baixo nos resultados de pesquisa.

Se você especificar uma string vazia para o parâmetro `QueryString`, sua consulta retornará os primeiros 1.000 recursos disponíveis por meio da visualização usada para a operação. O número máximo de recursos que podem ser retornados por qualquer consulta é 1.000.

> **Note**
>
> AWS reserva-se o direito de atualizar a lógica de correspondência e os algoritmos de relevância para avaliar palavras-chave de texto de formato livre para que possamos fornecer aos clientes os resultados mais relevantes. Portanto, os resultados retornados para as mesmas consultas usando palavras-chave de texto em formato livre podem mudar com o tempo. Quando você precisar de resultados mais determinísticos, recomendamos que use filtros. A lógica de correspondência dos filtros não muda com o tempo.

## Filtros

Você pode limitar os resultados da sua consulta de modo mais rígido incluindo filtros. Diferentemente das palavras-chave de texto, os filtros são avaliados na consulta com o ANDoperador. Por exemplo, considere a consulta a seguir, que consiste em duas palavras-chave em formato livre e dois filtros:

```
test instance service:EC2 region:us-west-2
```

Essa consulta é avaliada da seguinte maneira:

```
( test OR instance ) AND service:EC2 AND region:us-west-2
```

Os filtros são sempre avaliados usando operadores ANDlógicos. Se um recurso não corresponder ao filtro, ele não será incluído nos resultados. Os resultados da consulta de exemplo incluem todos os recursos que estão associados à Amazon EC2 e estão no Oeste dos EUA (Oregon) Região da AWS e têm pelo menos uma das palavras-chave anexadas de alguma forma.

> **Note**
>
> Por causa do AND implícito, você só pode usar com sucesso um único filtro para um atributo que só pode ter um valor associado ao recurso. Por exemplo, um recurso não pode fazer parte de mais de uma Região da AWS. Portanto, a consulta a seguir não retorna nenhum resultado.
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> Essa limitação não se aplica aos filtros de atributos que podem ter vários valores ao mesmo tempo, como `tag:`, `tag.key:` e `tag.value:`.

A tabela a seguir lista os nomes de filtros disponíveis que podem ser usados em uma consulta de pesquisa do Explorador de Recursos.

| Nome do filtro | Descrição e exemplo |
| --- | --- |
| `accountid:` | O Conta da AWS proprietário do recurso. O Explorador de Recursos só inclui nos resultados os recursos que pertencem à conta especificada.<br><br>`accountid:123456789012` |
| `application:` | Esse filtro permite que você pesquise recursos com uma chave de tag `awsApplication` e um valor de grupo de recursos. Você pode pesquisar pelo nome do aplicativo ou pelo grupo de recursos do aplicativoARN.<br><br>`application:MyApplicationName` |

| Nome do filtro | Descrição e exemplo |
| --- | --- |
| | `application:arn:aws:resource-groups: us-east-1 :123456789012:group/MyApplicationName/123456789abced`<br><br>`arn:aws:resource-groups: us-east-1 :123456789012:group/MyApplicationName/123456789abced`<br><br>**Note**<br>Para usar esse filtro, a visualização deve ter acesso a marcação de dados. |
| `id:` | O identificador de um recurso individual, expresso como um nome de recurso da Amazon (ARN).<br><br>`id:arn:aws:license-manager: us-east-1 :123456789012:license-configuration:lic-ecbd5574fd92cb0d312baea26EXAMPLE` |
| `region:` | O Região da AWS local onde o recurso está localizado. O Resource Explorer inclui nos resultados somente os recursos que residem no especificado Região da AWS.<br><br>`region:us-east-1`<br><br>**Note**<br>Digitar somente o código da região (sem um filtro, como `us-east-1` ) não retorna os mesmos resultados que `region:us-east-1` . Esse resultado ocorre porque, como uma palavra-chave de texto em formato livre que não é um filtro, o código da região é dividido em suas partes individuais. Por exemplo, `us-east-1` é pesquisado como `us`, `east` e `1`. Essa divisão em componentes não ocorre quando você usa o prefixo `region:`. |

| Nome do filtro | Descrição e exemplo |
| --- | --- |
| `region:global` | Um caso especial para o `region:` filtro que você pode usar para encontrar recursos que não estão associados a um indivíduo Região da AWS , mas são considerados de escopo global.<br><br>`region:global`<br><br>**Note**<br>Digitar somente a palavra-chave `global` não retorna os mesmos resultados que `region:global` porque a palavra literal "global" não está anexada aos recursos globais. Digitar `global` como uma palavra-chave só retorna os recursos que têm essa string literal associada a eles. |
| `resourcetype:` | O tipo de recurso na notação de *`service`*`:`*`type`*. O Explorador de Recursos só inclui nos resultados os recursos do tipo especificado.<br><br>`resourcetype:ec2:instance` |
| `resourcetype.supports:` | Esse filtro permite que você pesquise recursos que suportam tags. `tags`é o único valor suportado. O Resource Explorer inclui nos resultados somente os recursos que podem ser marcados.<br><br>`resourcetype.supports:tags` |
| `service:` | O AWS service (Serviço da AWS) que está associado ao tipo do recurso. O Explorador de Recursos só inclui nos resultados os recursos que são criados e gerenciados pelo serviço especificado.<br><br>`service:ec2` |
| `tag:` | Um par de chave/valor de tag expresso como `<key>=<value>` . O Explorador de Recursos só inclui nos resultados os recursos que têm uma tag com uma chave correspondente e o valor especificado.<br><br>`tag:environment=production` |

| Nome do filtro | Descrição e exemplo |
| --- | --- |
| `tag:all` | Um caso especial do `tag:` filtro que permite pesquisar recursos que tenham uma ou mais tags criadas pelo usuário anexadas, mesmo que o tipo de recurso não seja suportado no Resource Explorer.<br><br>**Note**<br>Recursos com tags criadas pelo serviço da AWS ainda aparecem nos resultados desse filtro. |
| `tag:none` | Um caso especial do filtro `tag:` que permite pesquisar qualquer recurso que não tenha nenhuma tag criada pelo usuário anexada.<br><br>**Note**<br>Recursos com tags criadas pelo serviço da AWS ainda aparecem nos resultados desse filtro. |
| `tag.key:` | Uma chave de tag. O Explorador de Recursos só inclui nos resultados os recursos que têm uma tag com uma chave correspondente, qualquer que seja o valor.<br><br>`tag.key:environment` |
| `tag.value:` | Um valor de tag. O Explorador de Recursos só inclui nos resultados os recursos que têm uma tag com um valor correspondente, qualquer que seja nome da chave.<br><br>`tag.value:production` |

## Operadores de filtro

Você pode modificar suas palavras-chave e filtros incluindo um dos operadores mostrados na tabela a seguir como parte da string.

| Operador | Descrição e exemplo |
| --- | --- |
| "*multiple word phrase*"<br><br>ou<br><br>"*hyphenated-phrase* " | Coloque entre aspas duplas (" ") uma frase composta de várias palavras que deve ser tratada como uma única palavra-chave. O Explorador de Recursos só inclui os recursos que correspondem à frase inteira, com todas as palavras juntas e na ordem especificada.<br><br>Se você não usar aspas duplas, o Explorador de Recursos usará espaços ou hífens para dividir a frase em seus componentes e incluirá os recursos que corresponderem aos componentes individuais, mesmo que não estejam juntos ou estejam em uma ordem diferente. As cotações devem estar em torno de tudo após o operador.<br><br>`"This matches only resources with the whole sentence."`<br><br>`This matches resources with any of the words.`<br><br>`"us-east-1"` : faz a correspondência apenas com os recursos associados a essa região exata.<br><br>`us-east-1` : faz a correspondência com qualquer recurso que contenha "us", "east" ou "1".<br><br>`-tag:"environment=production"` |
| *keyword** | Correspondência com caracteres curinga como prefixo. Você só pode colocar um caractere curinga (um asterisco *) no final da string. O Explorador de Recursos só inclui nos resultados os recursos com valores que começam com o texto do prefixo antes do *. O exemplo a seguir corresponde a tudo Regiões da AWS o que começa com`us-east`.<br><br>`region:us-east*`<br><br>**Important**<br>A pesquisa unificada insere automaticamente um operador de caractere curinga (*) no final da primeira palavra-chave da string. Isso significa que os resultados da pesquisa unificada incluem os recursos |

| Operador | Descrição e exemplo |
| --- | --- |
| | que correspondem a qualquer string que comece com a palavra-chave especificada.<br>A pesquisa realizada pela caixa de texto Consulta na página Pesquisa de recursos no console do Explorador de Recursos não adiciona automaticamente um caractere curinga. Você pode inserir um * manualmente depois de qualquer termo na string de pesquisa. |

| Operador | Descrição e exemplo |
| --- | --- |
| `-keyword` | Operador `Not`. Você pode colocar um hífen (`-`) no início da palavra-chave ou do filtro para inverter os resultados da pesquisa. O Explorador de Recursos exclui dos resultados todos os recursos que correspondem à palavra-chave ou ao filtro que vem depois desse operador. O exemplo a seguir faz com que todos os recursos associados ao EC2 serviço da Amazon sejam excluídos dos resultados.<br><br>`-service:ec2`<br><br>**Important**<br><br>Se você usar o AWS CLI `search` comando e o valor do `--query-string` parâmetro tiver o `-` operador como primeiro caractere, você deverá separar o nome do parâmetro de seu valor com um caractere de sinal de igual (=) em vez do caractere de espaço usual. Se você usar o caractere de espaço, ele CLI interpretará mal a string. Por exemplo, a consulta a seguir não funciona.<br><br>`aws resource-explorer-2 search --query-string "-tag:none region:us-east-1"`<br><br>A string de consulta corrigida a seguir, com um = substituindo o espaço, funciona como esperado.<br><br>`aws resource-explorer-2 search --query-string ="-tag:none region:us-east-1"`<br><br>Se você alterar a ordem dos filtros na string de consulta para que `-` não seja o primeiro caractere no valor do parâmetro, poderá usar o caractere de espaço padrão. A string de consulta a seguir funciona.<br><br>`aws resource-explorer-2 search --query-string "region:us-east-1 -tag:none"` |

| Operador | Descrição e exemplo |
| --- | --- |
| `\<special character>` | Você pode ignorar os caracteres especiais que devem ser incluídos exatament e como mostrado, em vez de serem interpretados. Se o texto incluir um dos caracteres especiais ( `* " - : = \`), você deverá preceder esse caractere por uma barra invertida (\) para garantir que o caractere seja interpretado literalmente. O exemplo a seguir mostra como usar uma palavra-chave de texto de formato livre que inclui o caractere hífen (-) (`"my-key-word"` ).<br><br>Além disso, para evitar que o Explorador de Recursos divida a expressão em três palavras-chave separadas nos hífens, você pode colocar a frase inteira entre aspas duplas.<br><br>`"my\-key\-word"`<br><br>Para inserir uma barra invertida literal, insira dois caracteres de barra invertida em sequência. A primeira barra invertida é interpretada como escape e a segunda barra invertida é o caractere literal a ser inserido.<br><br>`"some_text\\some_more_text"` |

> **Note**
>
> Se a visualização incluir as tags anexadas aos recursos, a operação `Search` não gerará erros de validação para as strings de pesquisa, pois um filtro que não é válido também pode ser interpretado como uma pesquisa de texto em formato livre. Por exemplo, embora `cat:blue` pareça um filtro, o Explorador de Recursos não pode analisá-lo como tal porque `cat:` não é um dos filtros definidos válidos. Em vez disso, o Resource Explorer interpreta a string inteira como uma string de pesquisa de formato livre para permitir que ela corresponda a coisas como um nome de chave de tag ou uma parte de uma. ARN
> A operação gerará um erro de validação se uma das seguintes situações for verdadeira:
>
> - A visualização não inclui informações sobre tags
> - A consulta de pesquisa usa explicitamente um filtro de tag (`tag.key:`, `tag.value:` ou `tag:`)

# Exemplo de consultas de pesquisa do Explorador de Recursos

Os exemplos a seguir mostram a sintaxe dos tipos comuns de consultas que você pode usar no Explorador de recursos da AWS.

**Important**

Se usar o comando `search` da AWS CLI e o valor do parâmetro `--query-string` tiver o operador `-` como primeiro caractere, você deverá separar o nome do parâmetro do seu valor com um caractere de sinal de igual (=), em vez de usar o caractere de espaço habitual. Se você usar o caractere de espaço, a CLI interpretará a string incorretamente. Por exemplo, a consulta a seguir não funciona.

```
aws resource-explorer-2 search --query-string "-tag:none region:us-east-1"
```

A consulta corrigida a seguir, com um = substituindo o espaço, funciona como esperado.

```
aws resource-explorer-2 search --query-string="-tag:none region:us-east-1"
```

Se você alterar a ordem dos filtros na string de consulta para que `-` não seja o primeiro caractere no valor do parâmetro, poderá usar o caractere de espaço padrão. A consulta a seguir funciona.

```
aws resource-explorer-2 search --query-string "region:us-east-1 -tag:none"
```

## Pesquisar recursos não marcados

Se você quiser usar o controle de acesso por atributo (ABAC) na sua conta, usar a alocação baseada em custo ou realizar a automação baseada em tags nos recursos, será necessário saber em quais recursos da sua conta podem estar faltando tags. O exemplo de consulta a seguir usa o filtro de caixa especial tag: none para retornar todos os recursos em que faltam tags geradas pelo usuário.

O filtro `tag:none` só se aplica às tags criadas pelo usuário. As tags que são geradas e mantidas pela AWS estão isentas desse filtro e continuam a aparecer nos resultados.

```
tag:none
```

Para excluir também todas as tags do sistema criadas pela AWS, adicione um segundo filtro, como mostrado no exemplo a seguir. O primeiro elemento string de consulta duplica o exemplo anterior filtrando todas as tags criadas pelo usuário. As tags do sistema criadas pela AWS sempre começam com as letras `aws`. Portanto, você pode usar o operador lógico NOT (-) com o filtro tag.key para excluir também todos os recursos que tenham uma tag com um nome de chave que comece com `aws`.

```
tag:none -tag.key:aws*
```

## Pesquisar recursos marcados

Para encontrar todos os recursos que têm uma tag de qualquer tipo, você pode usar o operador lógico NOT (-) com o filtro de caixa especial tag: none como se segue.

```
-tag:none
```

## Pesquisar recursos em que falta uma tag específica

Também relacionado ao ABAC, talvez você queira pesquisar todos os recursos que não têm nenhuma tag com uma chave especificada. O exemplo a seguir usa o operador lógico NOT - para retornar todos os recursos em que falta uma tag com o nome da chave `Department`.

```
-tag.key:Department
```

## Pesquisar os recursos que têm valores de tag inválidos

Por razões de conformidade, talvez você queira pesquisar todos os recursos que com valores de tag faltando ou com erros de ortografia em tags importantes. O exemplo a seguir retorna todos os recursos que têm uma tag com o nome da chave `environment`. Porém, a consulta exclui qualquer recurso que tenha um dos valores válidos `prod`, `integ` ou `dev`. Quaisquer resultados que apareçam nessa consulta têm algum outro valor que você deverá investigar e corrigir.

> **Important**
>
> As pesquisas do Explorador de Recursos não diferenciam maiúsculas de minúsculas e não conseguem distinguir entre nomes de chave e valores cuja única diferença é o uso maiúsculas e minúsculas. Por exemplo, os valores no exemplo a seguir correspondem a `PROD`, `prod`, `PrOd` ou a qualquer variação. Porém, algumas aplicações usam tags de modos que diferenciam entre maiúsculas e minúsculas. Recomendamos que você padronize uma estratégia de uso de maiúsculas e minúsculas para a sua organização, como, por exemplo, usar somente valores e nomes de chaves de tags começando com letra minúscula. Uma abordagem consistente pode ajudar a evitar a confusão que pode ser causada por tags que só diferem no uso de maiúsculas e minúsculas.

```
tag.key:environment -tag:environment=prod -tag:environment=integ -tag:environment=dev
```

## Pesquisar recursos em um subconjunto de Regiões da AWS

Use o operador curinga `'*'` para combinar todas as regiões de determinada área do mundo. O exemplo a seguir retorna todos os recursos que estão nas regiões da Europa (UE).

```
region:eu-*
```

## Pesquisar recursos globais

Use o valor `global` de caso especial do filtro de `region:` para encontrar os recursos que são considerados globais e não associados a uma região individual.

```
region:global
```

## Pesquisar recursos de um determinado tipo que estão localizados em uma região específica

Quando você usa vários filtros, o Explorador de Recursos avalia a expressão combinando os prefixos com operadores lógicos `AND` implícitos. O exemplo a seguir retorna todos os recursos que estão na região Ásia-Pacífico (Hong Kong) `AND` são instâncias do Amazon EC2.

```
region:ap-east-1 resourcetype:ec2:instance
```

> **Note**
>
> Por causa do AND implícito, você só pode usar com sucesso um único filtro para um atributo que só pode ter um valor associado ao recurso. Por exemplo, um recurso não pode fazer parte de mais de uma Região da AWS. Portanto, a consulta a seguir não retorna nenhum resultado.
>
> ```
> region:us-east-1 region:us-west-1
> ```
>
> Essa limitação não se aplica aos filtros de atributos que podem ter vários valores ao mesmo tempo, como `tag:`, `tag.key:` e `tag.value:`.

## Pesquisar recursos que têm um termo composto de várias palavras

Coloque um termo composto de várias palavras entre aspas duplas (") para retornar apenas resultados que tenham o termo inteiro na ordem especificada. Sem aspas duplas, o Explorador de Recursos retorna os recursos que correspondem a qualquer uma das palavras separadas que compõe o termo. Por exemplo, a consulta a seguir usa aspas duplas para retornar somente os recursos que correspondem ao termo `"west wing"`. A consulta não retorna os recursos na Região da AWS `us-west-2` (ou em qualquer outra região que inclua `west` em seu código) ou recursos que correspondam à palavra "wing" sem a palavra "west".

```
"west wing"
```

## Pesquisar recursos que fazem parte de uma pilha do CloudFormation

Quando você cria um recurso como parte de uma pilha do AWS CloudFormation, ele é automaticamente marcado com o nome da pilha. O exemplo a seguir retorna todos os recursos que foram criados como parte da pilha especificada.

```
tag:aws:cloudformation:stack-name=my-stack-name
```

# Usar a pesquisa unificada no AWS Management Console

O AWS Management Console inclui uma barra de pesquisa na parte superior de cada página do console da AWS. Essa barra de pesquisa pode pesquisar a documentação e os tópicos do blog do AWS service (Serviço da AWS) e levar você diretamente às páginas do console do serviço da AWS. Ela também poderá retornar os recursos da sua Conta da AWS, se você ativar o recurso de pesquisa unificada ativando os atributos necessários do Explorador de Recursos.

Com a pesquisa unificada, os usuários podem pesquisar recursos no console de qualquer AWS service (Serviço da AWS) sem ter primeiro que navegar até o console do Explorador de recursos da AWS.

> **Tip**
>
> Quando quiser usar a barra de pesquisa unificada para pesquisar os recursos especificamente, comece a consulta de pesquisa digitando **`/Resources`**. Isso faz com que os recursos da AWS tenham uma classificação mais alta nos resultados da pesquisa do que os resultados que não representam recursos.

Tópicos



> **Important**
>
> A pesquisa unificada insere automaticamente um operador de caractere curinga (*) no final da primeira palavra-chave da string. Isso significa que os resultados da pesquisa unificada incluem os recursos que correspondem a qualquer string que comece com a palavra-chave especificada.
> A pesquisa realizada pela caixa de texto Consulta na página Pesquisa de recursos no console do Explorador de Recursos não adiciona automaticamente um caractere curinga. Você pode inserir um * manualmente depois de qualquer termo na string de pesquisa.

# Verificar se a pesquisa unificada está habilitada

Para ver se a pesquisa unificada está habilitada na sua Conta da AWS, olhe na parte superior da página Configurações. O Explorador de Recursos exibe ali o status atual de cada requisito. Os requisitos para a pesquisa unificada são os seguintes:

- Você deve ativar o Explorador de Recursos em pelo menos uma Região da AWS. Somente recursos em regiões com índices do Explorador de Recursos podem aparecer nos resultados da pesquisa unificada.
- Você deve criar um índice agregador na região de sua escolha. As pesquisas realizadas nessa região retornam resultados de todas as regiões registradas na conta.
- Você deve criar uma visualização padrão na região que contém o índice agregador. Todos os usuários que precisam usar a pesquisa unificada por recursos devem ter permissão para usar essa visualização padrão.
- Os usuários devem ter uma política de permissões do AWS Identity and Access Management (IAM) atribuída à entidade principal do IAM que conceda permissão para a realização das ações `resource-explorer-2:Get*`, `resource-explorer-2:List*`, `resource-explorer-2:Describe*`, `resource-explorer-2:Search`. Você pode conceder essas permissões usando suas próprias políticas personalizadas do IAM. Essas permissões já estão incluídas como parte das políticas gerenciadas pela AWS a seguir que estão disponíveis para seu uso:
  - AWSResourceExplorerReadOnlyAccess
  - AWSResourceExplorerFullAccess

# Ativar a pesquisa unificada

Para permitir a inclusão dos recursos da sua conta nos resultados de pesquisa para a pesquisa unificada em qualquer console da AWS, você deve concluir as seguintes etapas:

1. Ative Explorador de recursos da AWS em uma ou mais Regiões da AWS da sua conta.
2. Registre uma região para conter o índice agregador.
3. Crie uma visualização padrão na região com o índice agregador.

# Criar recursos do Explorador de Recursos com o CloudFormation

O Explorador de recursos da AWS é integrado com o AWS CloudFormation, um serviço que ajuda você a modelar e configurar os recursos da AWS. Essa integração ajuda você a dispender menos tempo criando e gerenciando os recursos e a infraestrutura. Você cria um modelo que descreve todos os recursos da AWS que deseja, e o CloudFormation os provisiona e configura para você. Exemplos de recursos incluem índices, visualizações ou a atribuição de uma visualização padrão para uma Região da AWS.

Quando você usa o CloudFormation, pode reutilizar o modelo para configurar os recursos do Explorador de Recursos repetidas vezes e de modo consistente. Basta descrever os recursos uma vez e depois provisionar os mesmos recursos várias vezes em várias Contas da AWS e regiões.

Usar o AWS CloudFormation para implantar o Explorador de Recursos no AWS Organizations

Você pode usar os StackSets do AWS CloudFormation para implantar o Explorador de Recursos em todas as contas da sua organização. Quando você adiciona ou cria contas-membros na sua organização, os StackSets pode configurar automaticamente índices em cada Região da AWS, incluindo um índice agregador onde você especificar, para cada nova conta-membro. Para obter instruções, consulte Implantar o Explorador de Recursos nas contas de uma organização.

## Modelos do Explorador de Recursos e do CloudFormation

Para provisionar e configurar recursos para o Explorador de Recursos e serviços relacionados, você precisa entender os modelos do AWS CloudFormation. Os modelos são arquivos de texto formatados em JSON ou YAML. Esses modelos descrevem os recursos que você deseja provisionar nas pilhas do CloudFormation. Se você não estiver familiarizado com JSON ou YAML, poderá usar o AWS CloudFormation Designer para ajudá-lo a começar a usar os modelos do CloudFormation. Para obter mais informações, consulte O que é o Designer? (O que é o AWS CloudFormation Designer) no Manual do usuário do AWS CloudFormation.

O Explorador de Recursos é compatível com a criação dos seguintes tipos de recursos no CloudFormation:

- Índice: cria um índice em uma região e ativa o Explorador de Recursos nessa região. Você pode especificar que o índice seja um índice local ou o índice agregador da Conta da AWS. Para obter

mais informações, consulte Ativando o Resource Explorer em um Região da AWS para indexar seus recursos e Ativar a pesquisa inter-regional criando um índice agregador.

- Visualização: cria uma visualização que determina quais resultados podem ser exibidos quando um usuário faz uma pesquisa. Cada operação de pesquisa deve especificar uma visualização. É necessário conceder aos usuários permissão para usar as visualizações que você deseja que eles acessem. Veja mais informações em Gerenciar visualizações do Explorador de Recursos para fornecer acesso para pesquisa.

  > **Note**
  >
  > Você deve criar um índice em uma região antes de criar uma visualização nessa mesma região. Se você criar um índice e uma visualização como parte da mesma pilha, use o atributo `DependsOn` na visualização, conforme mostrado no exemplo de modelo a seguir, para garantir que o índice seja criado primeiro.

- DefaultViewAssociation: designa a visualização especificada para ser o padrão em sua região. Quando um usuário não especifica explicitamente a visualização ser usada em uma operação de pesquisa, o Explorador de Recursos tenta usar a visualização padrão associada à região em que o usuário faz a pesquisa. Para obter mais informações, consulte Definir uma visualização padrão em uma Região da AWS.

O exemplo a seguir ilustra como você pode criar um índice e uma visualização na mesma região e definir a visualização como padrão para a região.

YAML

```
Description: >-
  Sample CFN Stack setting up Resource Explorer with an aggregator index and a default
 view
Resources:
  SampleIndex:
    Type: 'AWS::ResourceExplorer2::Index'
    Properties:
      Type: AGGREGATOR
      Tags:
        Purpose: ResourceExplorer Sample CFN Stack
  SampleView:
    Type: 'AWS::ResourceExplorer2::View'
    Properties:
```

```
      ViewName: mySampleView
      IncludedProperties:
        - Name: tags
      Tags:
        Purpose: ResourceExplorer Sample CFN Stack
    DependsOn: SampleIndex
  SampleDefaultViewAssociation:
    Type: 'AWS::ResourceExplorer2::DefaultViewAssociation'
    Properties:
      ViewArn: !Ref SampleView
```

JSON

```
{
    "Description": "Sample CFN Stack setting up Resource Explorer with an aggregator
 index and a default view ",
    "Resources": {
        "SampleIndex": {
            "Type": "AWS::ResourceExplorer2::Index",
            "Properties": {
                "Type": "AGGREGATOR",
                "Tags": {
                    "Purpose": "ResourceExplorer Sample Stack"
                }
            }
        },
        "SampleView": {
            "Type": "AWS::ResourceExplorer2::View",
            "Properties": {
                "ViewName": "mySampleView",
                "IncludedProperties": [
                    {
                        "Name": "tags"
                    }
                ],
                "Tags": {
                    "Purpose": "ResourceExplorer Sample CFN Stack"
                }
            },
            "DependsOn": "SampleIndex"
        },
        "SampleDefaultViewAssociation": {
            "Type": "AWS::ResourceExplorer2::DefaultViewAssociation",
```

```
            "Properties": {
                "ViewArn": {
                    "Ref": "SampleView"
                }
            }
        }
    }
}
```

Para obter mais informações, incluindo exemplos de modelos JSON e YAML para índices e visualizações do Explorador de Recursos, consulte a ResourceExplorer2 resource type reference no AWS CloudFormation User Guide.

## Saiba mais sobre o AWS CloudFormation

Para saber mais sobre o CloudFormation, consulte os seguintes recursos:

- AWS CloudFormation
- Manual do usuário do AWS CloudFormation
- Guia do usuário da interface de linha de comando do AWS CloudFormation

# Usar o AWS Chatbot para pesquisar recursos

Você pode pesquisar e descobrir informações sobre os Serviços da AWS e seus recursos da AWS fazendo perguntas na linguagem natural do AWS Chatbot. O AWS Chatbot responde a perguntas relacionadas ao serviço diretamente em seus canais de bate-papo com documentação relevante da AWS e trechos de artigos de apoio. O AWS Chatbot usa o Explorador de Recursos para pesquisar e encontrar respostas para perguntas relacionadas ao seu recurso.

Para ter mais informações, consulte What is AWS Chatbot? in the AWS Chatbot Administrator Guide.

## Perguntas sobre recursos da AWS

O AWS Chatbot usa o Explorador de Recursos para pesquisar e descobrir seus recursos. O AWS Chatbot exibe esses resultados de pesquisa em uma lista. Essa lista mostra os cinco principais recursos correspondentes e inclui a capacidade de filtrar ainda mais os resultados por tipo de recurso, Região da AWS e tag.

### Pré-requisitos

Para fazer perguntas relacionadas a recursos do AWS Chatbot, você deve:

- Certificar-se de que tenha índices e visualizações ativos com pelo menos uma visualização padrão na Região da AWS. Os índices e as visualizações permitem que o Explorador de Recursos catalogue e consulte seus recursos. Consulte Termos e conceitos do Explorador de Recursos para obter mais informações.
- Adicione a AWSResourceExplorerReadOnlyAccess política à função do seu canal ou a cada função de usuário apropriada, dependendo do esquema de permissão do seu canal.
- Verifique se as políticas de proteção do seu canal permitem AWSResourceExplorerReadOnlyAccess permissões.

### Perguntas comuns sobre recursos

Você pode fazer essas perguntas diretamente nos canais de bate-papo. Substitua as palavras com texto vermelho por suas próprias informações.

```
@aws What services am I using in Region?
```

```
@aws What are the resources in my account with tags?

@aws What lambda functions do I have?
```

# Segurança em Explorador de recursos da AWS

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 isso como a segurança da nuvem e a segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que é executada Serviços da AWS no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de AWS de . Para saber mais sobre os programas de conformidade que se aplicam ao Resource Explorer, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS service (Serviço da AWS) que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade dos dados, os requisitos da empresa e as leis e os regulamentos aplicáveis

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar Explorador de recursos da AWS. Ela mostra como configurar o Explorador de Recursos para atender aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros Serviços da AWS que o ajudem a monitorar e proteger seus recursos do Resource Explorer.

Conteúdo

# Atualize IAM as políticas para IPv6

Explorador de recursos da AWS os clientes usam IAM políticas para definir um intervalo permitido de endereços IP e impedir que qualquer endereço IP fora do intervalo configurado possa acessar o Resource ExplorerAPIs.

O explorador de recursos-2.*region*O domínio.api.aws em que o Resource Explorer APIs está hospedado está sendo atualizado para oferecer suporteIPv6, além do. IPv4

As políticas de filtragem de endereços IP que não são atualizadas para lidar com IPv6 endereços podem fazer com que os clientes percam o acesso aos recursos no API domínio do Resource Explorer.

## Clientes afetados pela atualização de IPv4 para IPv6

Clientes que estão usando endereçamento duplo com políticas contendo aws: sourceIp são afetados por essa atualização. O endereçamento duplo significa que a rede suporta IPv4 tanto IPv6 e.

Se você estiver usando endereçamento duplo, deverá atualizar suas IAM políticas atualmente configuradas com endereços de IPv4 formato para incluir endereços de IPv6 formato.

Para obter ajuda com problemas de acesso, entre em contato com AWS Support.

> **Note**
>
> Os seguintes clientes não são afetados por essa atualização:
>
> - Clientes que estão apenas em IPv4 redes.
> - Clientes que estão apenas em IPv6 redes.

## O que éIPv6?

IPv6é o padrão IP de próxima geração destinado a ser substituído eventualmenteIPv4. A versão anterior,IPv4, usa um esquema de endereçamento de 32 bits para suportar 4,3 bilhões de dispositivos. IPv6em vez disso, usa endereçamento de 128 bits para suportar aproximadamente 340 trilhões de trilhões de trilhões (ou 2 até a 128ª potência) de dispositivos.

```
2001:cdba:0000:0000:0000:0000:3257:9652
```

```
2001:cdba:0:0:0:0:3257:9652
2001:cdba::3257:965
```

## Atualizando uma IAM política para IPv6

IAMas políticas são usadas atualmente para definir um intervalo permitido de endereços IP usando o `aws:SourceIp` filtro.

O endereçamento duplo suporta tanto o IPV6 tráfego IPv4 quanto o tráfego. Se sua rede usa endereçamento duplo, você deve garantir que todas as IAM políticas usadas para filtragem de endereços IP sejam atualizadas para incluir intervalos de IPv6 endereços.

Por exemplo, essa política de bucket do Amazon S3 identifica os intervalos de IPv4 endereços permitidos `192.0.2.0.*` e `203.0.113.0.*` no elemento. `Condition`

```
# https://docs.aws.amazon.com/IAM/latest/UserGuide/
reference_policies_examples_aws_deny-ip.html
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "*",
        "Resource": "*",
        "Condition": {
            "NotIpAddress": {
                "*aws:SourceIp*": [
                    "*192.0.2.0/24*",
                    "*203.0.113.0/24*"
                ]
            },
            "Bool": {
                "aws:ViaAWSService": "false"
            }
        }
    }
}
```

Para atualizar essa política, o `Condition` elemento da política é atualizado para incluir intervalos de IPv6 endereços `2001:DB8:1234:5678::/64` `2001:cdba:3257:8593::/64` e.

> **Note**
>
> FAÇA NOT REMOVE os IPv4 endereços existentes porque eles são necessários para compatibilidade com versões anteriores.

```
"Condition": {
            "NotIpAddress": {
                "*aws:SourceIp*": [
                    "*192.0.2.0/24*", <<DO NOT REMOVE existing IPv4 address>>
                    "*203.0.113.0/24*", <<DO NOT REMOVE existing IPv4 address>>
                    "*2001:DB8:1234:5678::/64*", <<New IPv6 IP address>>
                    "*2001:cdba:3257:8593::/64*" <<New IPv6 IP address>>
                ]
            },
            "Bool": {
                "aws:ViaAWSService": "false"
            }
        }
```

Para obter mais informações sobre como gerenciar permissões de acesso comIAM, consulte Políticas gerenciadas e políticas embutidas no Guia do AWS Identity and Access Management usuário.

## Verifique se seu cliente pode oferecer suporte IPv6

Clientes usando o resource-explorer-2. Recomenda-se que o endpoint {region} .api.aws verifique se seus clientes podem acessar outros AWS service (Serviço da AWS) endpoints que já estão habilitados. IPv6 As etapas a seguir descrevem como verificar esses endpoints.

Este exemplo usa Linux e curl versão 8.6.0 e usa os endpoints de serviço Amazon Athena, que IPv6 habilitaram endpoints localizados no domínio api.aws.

> **Note**
>
> Mude Região da AWS para a mesma região em que o cliente está localizado. Neste exemplo, usamos o `us-east-1` endpoint Leste dos EUA (Norte da Virgínia).

1. Determine se o endpoint é resolvido com um IPv6 endereço usando o comando curl a seguir.

```
dig +short AAAA athena.us-east-1.api.aws
2600:1f18:e2f:4e05:1a8a:948e:7c08:d2d6
2600:1f18:e2f:4e03:4a1e:83b0:8823:4ce5
2600:1f18:e2f:4e04:34c3:6e9a:2b0d:dc79
```

2. Determine se a rede cliente pode fazer uma conexão IPv6 usando o seguinte comando curl.

```
curl --ipv6 -o /dev/null --silent -w "\nremote ip: %{remote_ip}\nresponse code:
 %{response_code}\n" https://athena.us-east-1.api.aws

remote ip: 2600:1f18:e2f:4e05:1a8a:948e:7c08:d2d6
response code: 404
```

   Se um IP remoto foi identificado e o código de resposta não`0`, uma conexão de rede foi estabelecida com sucesso com o endpoint usandoIPv6.

Se o IP remoto estiver em branco ou o código de resposta estiver`0`, a rede do cliente ou o caminho da rede até o endpoint será somente IPv4 -. Você pode verificar essa configuração com o seguinte comando curl.

```
curl -o /dev/null --silent -w "\nremote ip: %{remote_ip}\nresponse code:
 %{response_code}\n" https://athena.us-east-1.api.aws

remote ip: 3.210.103.49
response code: 404
```

Se um IP remoto foi identificado e o código de resposta não`0`, uma conexão de rede foi estabelecida com sucesso com o endpoint usandoIPv4. O IP remoto deve ser um IPv4 endereço porque o sistema operacional deve selecionar o protocolo válido para o cliente. Se o IP remoto não for um IPv4 endereço, use o comando a seguir para forçar o uso IPv4 do curl.

```
curl --ipv4 -o /dev/null --silent -w "\nremote ip: %{remote_ip}\nresponse code:
 %{response_code}\n" https://athena.us-east-1.api.aws

remote ip: 35.170.237.34
response code: 404
```

# Gerenciamento de identidade e acesso para Explorador de recursos da AWS

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. IAMos administradores controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar os recursos do Resource Explorer. IAMé um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos



## Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no Resource Explorer.

Usuário do serviço: se você usar o serviço Explorador de Recursos para fazer seu trabalho, o administrador fornecerá as credenciais e as permissões necessárias. À medida que você usar mais atributos do Explorador de Recursos para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se não for possível acessar um atributo no Explorador de Recursos, consulte Solução de problemas de Explorador de recursos da AWS permissões.

Administrador do serviço: se você for o responsável pelos recursos do Explorador de Recursos na sua empresa, provavelmente terá acesso total aos recursos do Explorador de Recursos. Cabe a

você determinar quais recursos e funcionalidades do Explorador de Recursos os usuários do serviço devem acessar. Em seguida, você deve enviar solicitações ao IAM administrador para alterar as permissões dos usuários do serviço. Revise as informações nesta página para entender os conceitos básicos doIAM. Para saber mais sobre como sua empresa pode usar o IAM Resource Explorer, consulteComo o Resource Explorer funciona com IAM.

IAMadministrador — Se você for IAM administrador, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao Resource Explorer. Para ver exemplos de políticas baseadas em identidade do Resource Explorer que você pode usar emIAM, consulte. Exemplos de políticas baseadas em identidade do Explorador de recursos da AWS

## Autenticando com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como IAM usuário ou assumindo uma IAM função. Usuário raiz da conta da AWS

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Os usuários (do IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você entra como uma identidade federada, seu administrador configurou previamente a federação de identidades usando IAM funções. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para você mesmo assinar solicitações, consulte Assinar AWS API solicitações no Guia IAM do usuário.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação multifator no Guia AWS IAM Identity Center do usuário e Uso da autenticação multifator (MFA) AWS no Guia do IAMusuário.

## Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para ver a lista completa de tarefas que exigem que você faça login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do IAM usuário.

## Usuários e grupos

Um IAMusuário é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos confiar em credenciais temporárias em vez de criar IAM usuários que tenham credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com IAM os usuários, recomendamos que você alterne as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exigem credenciais de longo prazo no Guia do IAMusuário.

Um IAMgrupo é uma identidade que especifica uma coleção de IAM usuários. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar IAM recursos.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um IAM usuário (em vez de uma função) no Guia do IAM usuário.

## Funções

Uma IAMfunção é uma identidade dentro da sua Conta da AWS que tem permissões específicas. É semelhante a um IAM usuário, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma IAM função no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma AWS API operação AWS CLI or ou usando uma personalizadaURL. Para obter mais informações sobre métodos de uso de funções, consulte Métodos para assumir uma função no Guia IAM do usuário.

IAMfunções com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter informações sobre funções para federação, consulte Criação de uma função para um provedor de identidade terceirizado no Guia IAM do usuário. Se você usa o IAM Identity Center, configura um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a uma função em. IAM Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Manual do Usuário do AWS IAM Identity Center .
- Permissões temporárias IAM de IAM usuário — Um usuário ou função pode assumir uma IAM função para assumir temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas — Você pode usar uma IAM função para permitir que alguém (um diretor confiável) em uma conta diferente acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas IAM no Guia do IAM usuário.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos na Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a serviço.
  - Sessões de acesso direto (FAS) — Quando você usa um IAM usuário ou uma função para realizar ações em AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. FASusa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. FASas solicitações são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer FAS solicitações, consulte Encaminhar sessões de acesso.
  - Função de serviço — Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Um IAM administrador pode criar, modificar e excluir uma função

de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a uma AWS service (Serviço da AWS) no Guia do IAM usuário.

- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões das funções vinculadas ao serviço.

- Aplicativos em execução na Amazon EC2 — Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo AWS CLI AWS API solicitações. Isso é preferível ao armazenamento de chaves de acesso na EC2 instância. Para atribuir uma AWS função a uma EC2 instância e disponibilizá-la para todos os aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a função e permite que os programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Como usar uma IAM função para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia IAM do usuário.

Para saber se usar IAM funções ou IAM usuários, consulte Quando criar uma IAM função (em vez de um usuário) no Guia do IAM usuário.

## Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como JSON documentos. Para obter mais informações sobre a estrutura e o conteúdo dos documentos de JSON política, consulte Visão geral das JSON políticas no Guia IAM do usuário.

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder permissão aos usuários para realizar ações nos recursos de que precisam, um IAM administrador pode criar IAM políticas. O administrador pode então adicionar as IAM políticas às funções e os usuários podem assumir as funções.

IAMas políticas definem permissões para uma ação, independentemente do método usado para realizar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função do AWS Management Console AWS CLI, do ou do AWS API.

## Políticas baseadas em identidade

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um IAM usuário, grupo de usuários ou função. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte Criação de IAM políticas no Guia do IAMusuário.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte Escolha entre políticas gerenciadas e políticas em linha no Guia do IAMusuário.

## Políticas baseadas no recurso

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são as políticas de confiança de IAM funções e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas de uma política baseada IAM em recursos.

Explorador de recursos da AWS não oferece suporte a políticas baseadas em recursos.

## Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLssão semelhantes às políticas baseadas em recursos, embora não usem o formato de documento JSON de política.

Amazon S3, AWS WAF, e Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber maisACLs, consulte a visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Explorador de recursos da AWS não suportaACLs.

## Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões — Um limite de permissões é um recurso avançado no qual você define as permissões máximas que uma política baseada em identidade pode conceder a uma IAM entidade (IAMusuário ou função). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de permissões para IAM entidades no Guia IAM do usuário.
- Políticas de controle de serviço (SCPs) — SCPs são JSON políticas que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em AWS Organizations. AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. Os SCP limites de permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre Organizations eSCPs, consulte Políticas de controle de serviços no Guia AWS Organizations do Usuário.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes

de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia IAM do usuário.

### Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de política estão envolvidos, consulte Lógica de avaliação de políticas no Guia IAM do usuário.

## Como o Resource Explorer funciona com IAM

Antes de usar IAM para gerenciar o acesso ao Explorador de recursos da AWS, você deve entender quais IAM recursos estão disponíveis para uso com o Resource Explorer. Para obter uma visão de alto nível de como o Resource Explorer e outros Serviços da AWS trabalham comIAM, consulte Serviços da AWS esse trabalho IAM no Guia do IAM usuário.

Tópicos

- Políticas baseadas em identidade do Explorador de Recursos
- Autorização baseada em tags do Explorador de Recursos
- IAMFunções do Resource Explo

Como qualquer outro AWS service (Serviço da AWS), o Resource Explorer exige permissões para usar suas operações para interagir com seus recursos. Para pesquisar, os usuários devem ter permissão para recuperar os detalhes de uma visualização e também para pesquisar usando a visualização. Para criar índices ou visualizações, ou para modificá-los ou qualquer outra configuração do Explorador de Recursos, você deve ter permissões adicionais.

Atribua políticas IAM baseadas em identidade que concedam essas permissões aos diretores apropriadosIAM. O Explorador de Recursos fornece várias políticas gerenciadas que predefinem conjuntos comuns de permissões. Você pode atribuí-los aos seus IAM diretores.

### Políticas baseadas em identidade do Explorador de Recursos

Com políticas IAM baseadas em identidade, você pode especificar ações permitidas ou negadas em relação a recursos específicos e as condições sob as quais essas ações são permitidas ou

negadas. O Explorador de Recursos é compatível com ações, recursos e chaves de condição específicos. Para saber mais sobre todos os elementos que você usa em uma JSON política, consulte a referência IAM JSON de elementos de política no Guia IAM do usuário.

Ações

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O `Action` elemento de uma JSON política descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da AWS API operação associada. Há algumas exceções, como ações somente com permissão que não têm uma operação correspondente. API Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

As ações de política no Explorador de Recursos usam o prefixo do serviço `resource-explorer-2` antes da ação. Por exemplo, para conceder a alguém permissão para pesquisar usando uma exibição, com a `Search` API operação Resource Explorer, você inclui a `resource-explorer-2:Search` ação em uma política atribuída a esse principal. As instruções de política devem incluir um elemento `Action` ou `NotAction`. O Explorador de Recursos define seu próprio conjunto de ações que descrevem as tarefas que você pode realizar com esse serviço. Eles se alinham às API operações do Resource Explorer.

Para especificar várias ações em uma única declaração, separe-as com vírgulas, conforme exibido no exemplo a seguir.

```
"Action": [
      "resource-explorer-2:action1",
      "resource-explorer-2:action2"
]
```

É possível especificar várias ações usando caracteres curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `Describe`, inclua a ação a seguir:

```
"Action": "resource-explorer-2:Describe*"
```

Para ver uma lista das ações do Explorador de Recursos, consulte Ações definidas pelo Explorador de recursos da AWS na Referência de autorização do serviço da AWS .

Recursos

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Resource` JSON de política especifica o objeto ou objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu Amazon Resource Name (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Visão

O principal tipo de recurso do Explorador de Recursos é a visualização.

O recurso de visualização do Resource Explorer tem o seguinte ARN formato.

```
arn:${Partition}:resource-explorer-2:${Region}:${Account}:view/${ViewName}/${unique-id}
```

O ARN formato do Resource Explorer é mostrado no exemplo a seguir.

```
arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-Search-
View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

> **Note**
>
> O ARN for a view inclui um identificador exclusivo no final para garantir que cada visualização seja exclusiva. Isso ajuda a garantir que uma IAM política que concedeu acesso a uma exibição antiga excluída não possa ser usada para conceder acesso acidentalmente a uma nova exibição que por acaso tenha o mesmo nome da exibição antiga. Cada nova visualização recebe uma ID nova e exclusiva no final para garantir que nunca ARNs sejam reutilizadas.

Para obter mais informações sobre o formato deARNs, consulte Amazon Resource Names (ARNs).

Você usa políticas IAM baseadas em identidade atribuídas aos IAM diretores e especifica a exibição como a. `Resource` Isso permite que você conceda acesso de pesquisa a um conjunto de entidades principais usando uma visualização e acesso a um conjunto diferente de entidades principais usando uma visualização completamente diferente.

Por exemplo, para conceder permissão a uma única visualização nomeada `ProductionResourcesView` em uma declaração de IAM política, primeiro obtenha o nome do recurso Amazon (ARN) da visualização. Você pode usar a página Visualizações no console para visualizar os detalhes de uma visualização ou invocar a `ListViews` operação para recuperar a visualização completa ARN desejada. Em seguida, você o inclui em uma instrução de política, como a mostrada no exemplo a seguir, que concede permissão para modificar a definição de apenas uma visualização.

```
"Effect": "Allow",
"Action": "UpdateView",
"Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
ProductionResourcesView/<unique-id>"
```

Para permitir as ações em todas as visualizações que pertencem a uma conta específica, use o caractere curinga (*) na parte relevante doARN. O exemplo a seguir concede permissão de pesquisa a todas as visualizações em uma Região da AWS e uma conta especificadas.

```
"Effect": "Allow",
"Action": "Search",
"Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/*"
```

Algumas ações do Explorador de Recursos, como `CreateView`, não são executadas em um recurso específico porque, como no exemplo a seguir, o recurso ainda não existe. Nesses casos, você deve usar o caractere curinga (*) para todo o recursoARN.

```
"Effect": "Allow",
"Action": "resource-explorer-2:CreateView"
"Resource": "*"
```

Se você especificar um caminho que termine com um caractere curinga, poderá restringir a operação `CreateView` à criação de visualizações apenas com o caminho aprovado. O exemplo de política

a seguir mostra como permitir que a entidade principal só crie visualizações no caminho `view/ProductionViews/`.

```
"Effect": "Allow",
"Action": "resource-explorer-2:CreateView"
"Resource": "arn:aws:resource-explorer-2:us-
east-1:123456789012:view/ProductionViews/*""
```

Índice

Outro tipo de recurso que você pode usar para controlar o acesso à funcionalidade do Explorador de Recursos é o índice.

A maneira principal de interagir com o índice é ativar o Explorador de Recursos em uma Região da AWS criando um índice nessa região. Depois disso, você faz quase todo o resto interagindo com a visualização.

Uma das utilidades do índice é permitir que você controle quem pode criar visualizações em cada região.

> **Note**
>
> Depois de criar uma exibição, IAM autoriza todas as outras ações ARN de exibição somente em relação à exibição e não ao índice.

O índice tem um ARNque você pode referenciar em uma política de permissão. Um índice do Resource Explorer ARN tem o seguinte formato.

```
arn:${Partition}:resource-explorer-2:${Region}:${Account}:index/${unique-id}
```

Veja o exemplo a seguir de um índice do Resource ExplorerARN.

```
arn:aws:resource-explorer-2:us-east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-
abcd22222222
```

Algumas ações do Explorador de Recursos verificam a autenticação em relação a vários tipos de recursos. Por exemplo, a CreateViewoperação autoriza tanto o ARN índice quanto a exibição, como ocorrerá após a criação ARN do Resource Explorer. Para conceder permissão aos administradores

para gerenciar o serviço Explorador de Recursos, você pode usar `"Resource": "*"` para autorizar ações para qualquer recurso, índice ou visualização.

Como alternativa, você pode restringir uma entidade principal a só poder trabalhar com determinados recursos do Explorador de Recursos. Por exemplo, para limitar as ações somente aos recursos do Resource Explorer em uma região especificada, você pode incluir um ARN modelo que corresponda ao índice e à exibição, mas que destaque somente uma única região. No exemplo a seguir, o ARN corresponde aos índices ou às visualizações somente na `us-west-2` região da conta especificada. Especifique a Região no terceiro campo doARN, mas use um caractere curinga (*) no campo final para corresponder a qualquer tipo de recurso.

```
"Resource": "arn:aws:resource-explorer-2:us-west-2:123456789012:*
```

Para obter mais informações, consulte Ações definidas pelo Explorador de recursos da AWS na Referência de autorização do serviço da AWS . Para saber com quais ações você pode especificar cada recurso, consulte Ações definidas por Explorador de recursos da AWS. ARN

Chaves de condição

O Explorador de Recursos não fornece nenhuma chave de condição específica do serviço, mas é compatível com o uso de algumas chaves de condição globais. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia IAM do usuário.

Os administradores podem usar AWS JSON políticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, você pode conceder permissão a um IAM usuário para acessar um recurso somente se ele estiver

marcado com o nome de IAM usuário. Para obter mais informações, consulte elementos de IAM política: variáveis e tags no Guia IAM do usuário.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as chaves de contexto de condição AWS global no Guia IAM do usuário.

Para ver uma lista de chaves de condição do CloudTrail, consulte Chaves de condição do Explorador de recursos da AWS na Referência de autorização do serviço da AWS . Para saber com quais ações e recursos é possível usar uma chave de condição, consulte Ações definidas pelo Explorador de recursos da AWS.

Exemplos

Para ver exemplos das políticas baseadas em identidade do Explorador de Recursos, consulte Exemplos de políticas baseadas em identidade do Explorador de recursos da AWS.

## Autorização baseada em tags do Explorador de Recursos

Você pode anexar tags aos recursos do Explorador de Recursos ou passar as tags em uma solicitação do Explorador de Recursos. Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `resource-explorer-2:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou chaves de condição `aws:TagKeys`. Para obter mais informações sobre o uso de tags em recursos do Explorador de Recursos, consulte Adicionar tags a visualizações. Para usar a autorização baseada em tags no Explorador de Recursos, consulte Usar autorização baseada em tags para controlar o acesso às visualizações.

## IAMFunções do Resource Explo

Uma IAMfunção é uma principal dentro da sua Conta da AWS que tem permissões específicas.

Usar credenciais temporárias com o Explorador de Recursos

Você pode usar credenciais temporárias para entrar com a federação, assumir uma IAM função ou assumir uma função entre contas. Você obtém credenciais de segurança temporárias chamando API operações AWS Security Token Service (AWS STS) como AssumeRoleou GetFederationToken.

O Explorador de Recursos é compatível com o uso de credenciais temporárias.

Funções vinculadas a serviço

As funções vinculadas ao serviço permitem Serviços da AWS acessar recursos em outros serviços para concluir uma ação em seu nome. As funções vinculadas ao serviço aparecem em sua IAM conta e são de propriedade do serviço. Um IAM administrador pode visualizar, mas não editar, as permissões para funções vinculadas ao serviço.

O Explorador de Recursos usa perfis vinculados ao serviço para realizar seu trabalho. Para obter detalhes sobre perfis vinculadas ao serviço, consulte Usar perfis vinculados ao serviço para o Explorador de Recursos.

## Exemplos de políticas baseadas em identidade do Explorador de recursos da AWS

Por padrão, as entidades principais do AWS Identity and Access Management (IAM), como perfis, grupos e usuários, não têm permissão para criar ou modificar recursos do Explorador de Recursos. Elas também não podem realizar tarefas usando o AWS Management Console, a AWS Command Line Interface (AWS CLI) ou a API do AWS. Um administrador do IAM deve criar políticas do IAM que concedam às entidades principais permissão para executar operações da API específicas nos recursos especificados de que elas precisam. O administrador deve atribuir essas políticas às entidades principais do IAM que requerem essas permissões.

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

- Usuários e grupos no AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Create a permission set (Criação de um conjunto de permissões) no Guia do usuário do AWS IAM Identity Center.
- Usuários gerenciados no IAM usando um provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criar um perfil para um provedor de identidades de terceiros (federação) no Guia do usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Creating a role for an IAM user (Criação de um perfil para um usuário do IAM) no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adicionar permissões a um usuário (console) no Guia do usuário do IAM.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documentos de política JSON, consulte Criar políticas na guia JSON no Manual do usuário do IAM.

Tópicos



## Práticas recomendadas de políticas

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Explorador de Recursos na sua conta. Essas ações podem incorrer em custos para a Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas gerenciadas pela AWS e avance para as permissões de privilégio mínimo: para começar a conceder permissões a seus usuários e workloads, use as políticas gerenciadas pela AWS que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis na sua Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo cliente da AWS específicas para seus casos de uso. Para obter mais informações, consulte Políticas gerenciadas pela AWS ou Políticas gerenciadas pela AWS para funções de trabalho no Guia do usuário do IAM.
- Aplique permissões de privilégio mínimo: ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em recursos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar o IAM para aplicar permissões, consulte Políticas e permissões no IAM no Guia do usuário do IAM.
- Use condições nas políticas do IAM para restringir ainda mais o acesso: você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode escrever uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso a ações de serviço, se elas forem usadas por meio de um AWS service (Serviço da AWS) específico, como o AWS CloudFormation. Para obter mais informações, consulte Elementos de política JSON do IAM: Condition no Manual do usuário do IAM.

- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais: o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudar você a criar políticas seguras e funcionais. Para obter mais informações, consulte Validação de políticas do IAM Access Analyzer no Guia do usuário do IAM.
- Require multi-factor authentication (MFA) (Exigir autenticação multifator (MFA)): se houver um cenário que exija usuários do IAM ou um usuário raiz em sua Conta da AWS, ative a MFA para obter segurança adicional. Para exigir a MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte Configuração de acesso à API protegido por MFA no Guia do usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte Práticas recomendadas de segurança no IAM no Guia do usuário do IAM.

## Usar o console do Explorador de Recursos

Para que as entidades principais pesquisem no console do Explorador de recursos da AWS, elas devem ter um conjunto mínimo de permissões. Se você não criar uma política baseada em identidade com as permissões mínimas necessárias, o console do Explorador de Recursos não funcionará como pretendido para as entidades principais da conta.

Você pode usar a política gerenciada pela AWS denominada `AWSResourceExplorerReadOnlyAccess` para conceder a capacidade de usar o console do Explorador de Recursos para pesquisar usando qualquer visualização da conta. Para conceder permissões para só pesquisar com uma única visualização, consulte Conceder acesso às visualizações do Explorador de Recursos para pesquisa e os exemplos nas duas próximas seções.

Não é necessário conceder permissões mínimas do console para perfis que fazem chamadas somente à AWS CLI ou à API da AWS. Em vez disso, você pode escolher conceder acesso apenas às ações que correspondem às operações da API que as entidades principais precisam realizar.

## Conceder acesso a uma visualização com base em tags

Neste exemplo, você deseja conceder acesso a uma visualização do Explorador de Recursos na sua Conta da AWS às entidades principais da conta. Para fazer isso, você atribui as políticas baseadas em identidade do IAM às entidades principais que você deseja que sejam capazes pesquisar no Explorador de Recursos. O exemplo a seguir de política do IAM concede acesso a

qualquer solicitação em que a tag `Search-Group` anexada à entidade principal que faz a chamada corresponda exatamente ao valor dessa mesma tag anexada à visualização usada na solicitação.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetView",
                "resource-explorer-2:Search"
            ],
            "Resource": "arn:aws:resource-explorer-2:*:*:view/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Search-Group": "${aws:PrincipalTag/
Search-Group}"}
            }
        }
    ]
}
```

Você pode atribuir essa política às entidades principais do IAM na sua conta. Se uma entidade principal com a tag `Search-Group=A` tentar pesquisar usando uma visualização do Explorador de Recursos, a visualização também deverá estar marcada como `Search-Group=A`. Se não, a entidade principal terá o acesso negado. A chave da tag de condição `Search-Group` corresponde a `Search-group` e a `search-group` porque os nomes de chaves de condição não fazem distinção entre maiúsculas e minúsculas. Para obter mais informações, consulte Elementos de política JSON do IAM: condição no Guia do usuário do IAM.

> **Important**
>
> Para ver seus recursos nos resultados da pesquisa unificada no AWS Management Console, as entidades principais devem ter as permissões `GetView` e `Search` para a visualização padrão na Região da AWS que contém o índice agregador. A maneira mais simples de conceder essas permissões é conservar a permissão baseada em recurso padrão que foi anexada à visualização quando você ativou o Explorador de Recursos usando a Configuração rápida ou a Configuração avançada.

Nesse cenário, você poderia pensar em definir a visualização padrão para filtrar os recursos confidenciais e depois configurar visualizações adicionais às quais você concederia acesso baseado em tags, como descrito no exemplo anterior.

## Conceder acesso para criar uma visualização baseada em tags

Neste exemplo, você deseja permitir que apenas as entidades principais marcadas com a mesma tag que o índice possam criar visualizações na Região da AWS que contém o índice. Para fazer isso, crie permissões baseadas em identidade para permitir que as entidades principais pesquisem com visualizações.

Agora você está pronto para conceder permissões para criar uma visualização. Você pode adicionar as instruções desse exemplo à mesma política de permissão que você usa para conceder permissões de `Search` às entidades principais apropriadas. As ações são permitidas ou negadas com base nas tags anexadas às entidades principais que chamam as operações e o índice aos quais a visualização deverá ser associada. O exemplo a seguir de política do IAM nega qualquer solicitação para criar uma visualização quando o valor da tag `Allow-Create-View` anexada à entidade principal que faz a chamada não corresponde exatamente ao valor dessa mesma tag anexada ao índice da região em que a visualização foi criada.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "resource-explorer-2:CreateView",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {"aws:ResourceTag/Allow-Create-View":
 "${aws:PrincipalTag/Allow-Create-View}"}
            }
        }
    ]
}
```

## Permitir que as entidades principais visualizem suas próprias permissões

Este exemplo mostra como você pode criar uma política que permite que os usuários do IAM visualizem as políticas gerenciadas e em linha anexadas a sua identidade de usuário. Essa política

inclui permissões para concluir essa ação no console ou de forma programática usando a AWS CLI ou a API da AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

## Exemplo de políticas de controle de serviço para o AWS Organizations Resource Explorer

Explorador de recursos da AWS suporta políticas de controle de serviços (SCPs). SCPs são políticas que você anexa a elementos em uma organização para gerenciar permissões dentro dessa organização. Um SCP se aplica a todos Contas da AWS em uma organização sob o elemento

ao qual você anexa o SCP. As SCPs oferecem controle central sobre as permissões máximas disponíveis para todas as contas da organização. Eles podem ajudar você a garantir sua Contas da AWS permanência dentro das diretrizes de controle de acesso da sua organização. Para obter mais informações, consulte Políticas de controle de serviço no Guia do usuário do AWS Organizations .

## Pré-requisitos

Para usar os SCPs, você deve fazer o seguinte:

- Ativar todos os recursos em sua organização. Para obter mais informações, consulte Habilitar todos os atributos na sua organização no Manual do usuário do AWS Organizations .
- Habilitar SCPs para uso na sua organização. Para obter mais informações, consulte Habilitar e desabilitar tipos de política no Guia do usuário do AWS Organizations .
- Criar as SCPs de que você precisa. Para obter mais informações sobre a criação de SCPs, consulte Criação e atualização de SCPs no AWS Organizations Guia do Usuário.

## Políticas de controle de serviço de exemplo

O exemplo a seguir mostra como você pode usar o controle de acesso por atributo (ABAC) para controlar o acesso às operações administrativas do Explorador de Recursos. Esse exemplo de política nega acesso a todas as operações do Explorador de Recursos, exceto pelas duas permissões necessárias para pesquisar, `resource-explorer-2:Search` e `resource-explorer-2:GetView`, a menos que a entidade principal do IAM que fizer a solicitação esteja marcada como `ResourceExplorerAdmin=TRUE`. Para ver uma discussão mais completa sobre o uso do ABAC com o Explorador de Recursos, consulte Usar autorização baseada em tags para controlar o acesso às visualizações.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "resource-explorer-2:AssociateDefaultView",
        "resource-explorer-2:BatchGetView",
        "resource-explorer-2:CreateIndex",
        "resource-explorer-2:CreateView",
        "resource-explorer-2:DeleteIndex",
        "resource-explorer-2:DeleteView",
```

```
        "resource-explorer-2:DisassociateDefaultView",
        "resource-explorer-2:GetDefaultView",
        "resource-explorer-2:GetIndex",
        "resource-explorer-2:ListIndexes",
        "resource-explorer-2:ListSupportedResourceTypes",
        "resource-explorer-2:ListTagsForResource",
        "resource-explorer-2:ListViews",
        "resource-explorer-2:TagResource",
        "resource-explorer-2:UntagResource",
        "resource-explorer-2:UpdateIndexType",
        "resource-explorer-2:UpdateView""
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
          "StringNotEqualsIgnoreCase": {"aws:PrincipalTag/ResourceExplorerAdmin":
 "TRUE"}
      }
    ]
}
```

## AWS políticas gerenciadas para Explorador de recursos da AWS

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

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

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

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

Políticas gerais AWS gerenciadas que incluem permissões do Resource Explorer

- AdministratorAccess— Concede acesso total Serviços da AWS e recursos.
- ReadOnlyAcesso — concede acesso Serviços da AWS e recursos somente para leitura.
- ViewOnlyAcesso — concede permissões para visualizar recursos e metadados básicos para Serviços da AWS.

> **Note**
>
> As permissões de `Get*` do Explorador de Recursos incluídas na política `ViewOnlyAccess` funcionam da mesma forma que as permissões de `List`, embora retornem apenas um único valor, porque uma região só pode conter um índice e uma visualização padrão.

AWS políticas gerenciadas para o Resource Explorer

- AWSResourceExplorerFullAccess
- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerServiceRolePolicy

## AWS política gerenciada: AWSResourceExplorerFullAccess

Você pode atribuir a política `AWSResourceExplorerFullAccess` às identidades do IAM.

Essa política concede permissões que garantem total controle administrativo do serviço Explorador de Recursos. Você pode realizar todas as tarefas envolvidas na ativação e no gerenciamento do Explorador de Recursos nas Regiões da AWS na sua conta.

Detalhes da permissão

Essa política inclui permissões que permitem todas as ações do Resource Explorer, incluindo ativar e desativar o Resource Explorer Regiões da AWS, criar ou excluir um índice agregador para a conta, criar, atualizar e excluir visualizações e pesquisar. Essa política também inclui permissões que não fazem parte do Explorador de Recursos:

- `ec2:DescribeRegions`: permite que o Explorador de Recursos acesse os detalhes sobre as regiões na sua conta.

- `ram:ListResources`: permite que o Explorador de Recursos liste os compartilhamentos de recursos dos quais os recursos fazem parte.
- `ram:GetResourceShares`: permite que o Explorador de Recursos identifique detalhes sobre os compartilhamentos de recursos dos quais você é proprietário ou que são compartilhados com você.
- `iam:CreateServiceLinkedRole`: permite que o Explorador de Recursos crie o perfil vinculado ao serviço requerido quando você ativa o Explorador de Recursos criando o primeiro índice.
- `organizations:DescribeOrganization`: permite que o Explorador de Recursos acesse informações sobre a sua organização.

Para ver a versão mais recente dessa política AWS gerenciada, consulte o Guia *`AWSResourceExplorerFullAccess`* de referência da política AWS gerenciada.

## AWS política gerenciada: AWSResourceExplorerReadOnlyAccess

Você pode atribuir a política `AWSResourceExplorerReadOnlyAccess` às identidades do IAM.

Essa política concede permissões de acesso somente leitura que permitem aos usuários acesso básico à pesquisa para descobrir seus recursos.

Detalhes da permissão

Essa política inclui permissões para que os usuários executem as operações `Get*`, `List*` e `Search` do Explorador de Recursos para visualizar informações sobre os componentes e as definições de configuração do Explorador de Recursos, mas não permite que os usuários os alterem. Os usuários também podem pesquisar. Essa política também inclui duas permissões que não fazem parte do Explorador de Recursos:

- `ec2:DescribeRegions`: permite que o Explorador de Recursos acesse os detalhes sobre as regiões na sua conta.
- `ram:ListResources`: permite que o Explorador de Recursos liste os compartilhamentos de recursos dos quais os recursos fazem parte.
- `ram:GetResourceShares`: permite que o Explorador de Recursos identifique detalhes sobre os compartilhamentos de recursos dos quais você é proprietário ou que são compartilhados com você.
- `organizations:DescribeOrganization`: permite que o Explorador de Recursos acesse informações sobre a sua organização.

Para ver a versão mais recente dessa política AWS gerenciada, consulte o Guia *AWSResourceExplorerReadOnlyAccess* de referência da política AWS gerenciada.

## AWS política gerenciada: AWSResourceExplorerServiceRolePolicy

Você não pode anexar a `AWSResourceExplorerServiceRolePolicy` a nenhuma entidade do IAM. Essa política é anexada a um perfil vinculado ao serviço que permite que o Explorador de Recursos realize ações em seu nome. Para ter mais informações, consulte Usar perfis vinculados ao serviço para o Explorador de Recursos.

Essa política concede as permissões necessárias para que o Explorador de Recursos recupere informações sobre os recursos. O Resource Explorer preenche os índices que mantém em cada um Região da AWS que você registra.

Para ver a versão mais recente dessa política AWS gerenciada, consulte `AWSResourceExplorerServiceRolePolicy` no console do IAM.

## AWS política gerenciada: AWSResourceExplorerOrganizationsAccess

Você pode atribuir a política `AWSResourceExplorerOrganizationsAccess` às identidades do IAM.

Essa política concede permissões administrativas ao Resource Explorer e concede permissões somente de leitura a outras pessoas para oferecer suporte Serviços da AWS a esse acesso. O AWS Organizations administrador precisa dessas permissões para configurar e gerenciar a pesquisa em várias contas no console.

Detalhes da permissão

Essa política inclui permissões que deixam que os administradores configurem a pesquisa em várias contas para a organização:

- `ec2:DescribeRegions`: permite que o Explorador de Recursos acesse os detalhes sobre as regiões na sua conta.
- `ram:ListResources`: permite que o Explorador de Recursos liste os compartilhamentos de recursos dos quais os recursos fazem parte.
- `ram:GetResourceShares`: permite que o Explorador de Recursos identifique detalhes sobre os compartilhamentos de recursos dos quais você é proprietário ou que são compartilhados com você.

- `organizations:ListAccounts`: permite que o Explorador de Recursos identifique as contas em uma organização.
- `organizations:ListRoots`: permite que o Explorador de Recursos identifique as contas raízes em uma organização.
- `organizations:ListOrganizationalUnitsForParent`: permite que o Explorador de Recursos identifique as unidades organizacionais (UOs) em uma unidade organizacional superior ou raiz.
- `organizations:ListAccountsForParent`: permite que o Explorador de Recursos identifique as contas em uma organização que são contidas na raiz de destino especificada ou em uma UO.
- `organizations:ListDelegatedAdministrators`— Permite que o Resource Explorer identifique as AWS contas designadas como administradores delegados nessa organização.
- `organizations:ListAWSServiceAccessForOrganization`— Permite que o Resource Explorer identifique uma lista dos Serviços da AWS que estão habilitados para integração com sua organização.
- `organizations:DescribeOrganization`: permite que o Explorador de Recursos recupere informações sobre a organização à qual a conta do usuário pertence.
- `organizations:EnableAWSServiceAccess`— Permite que o Resource Explorer habilite a integração de um AWS service (Serviço da AWS) (o serviço especificado por`ServicePrincipal`) com AWS Organizations.
- `organizations:DisableAWSServiceAccess`— Permite que o Resource Explorer desative a integração de um AWS service (Serviço da AWS) (o serviço especificado por ServicePrincipal) com AWS Organizations.
- `organizations:RegisterDelegatedAdministrator`— Permite que o Resource Explorer habilite a conta de membro especificada para administrar os recursos da organização do AWS serviço especificado.
- `organizations:DeregisterDelegatedAdministrator`— Permite que o Resource Explorer remova o membro especificado Conta da AWS como administrador delegado para o especificado AWS service (Serviço da AWS).
- `iam:GetRole`: permite que o Explorador de Recursos recupere informações sobre o perfil especificado incluindo o caminho, o GUID, o ARN e a política de confiança do perfil que concede permissão para assumi-lo.
- `iam:CreateServiceLinkedRole`: permite que o Explorador de Recursos crie o perfil vinculado ao serviço requerido quando você ativa o Explorador de Recursos criando o primeiro índice.

Para ver a versão mais recente dessa política AWS gerenciada, consulte `AWSResourceExplorerOrganizationsAccess` no console do IAM.

## Atualizações do Resource Explorer para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do Resource Explorer 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 Histórico de documentos do Explorador de Recursos.

| Alteração | Descrição | Data |
| --- | --- | --- |
| AWSResourceExplorerServiceRolePolicy- Permissões de política atualizadas para visualizar tipos de recursos adicionais | O Resource Explorer adicionou permissões à política de função vinculada ao serviço `AWSResourceExplorerServiceRolePolicy` que permite que o Resource Explorer visualize outros tipos de recursos:<br>• `apprunner:ListVpcConnectors`<br>• `backup:ListReportPlans`<br>• `emr-serverless:ListApplications`<br>• `events:ListEventBuses`<br>• `geo:ListPlaceIndexes`<br>• `geo:ListTrackers`<br>• `greengrass:ListComponents` | 12 de dezembro de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| | • greengrass:ListComponentVersions<br>• iot:ListRoleAliases<br>• iottwinmaker:ListComponentTypes<br>• iottwinmaker:ListEntities<br>• iottwinmaker:ListScenes<br>• kafka:ListConfigurations<br>• kms:ListKeys<br>• kinesisanalytics:ListApplications<br>• lex:ListBots<br>• lex:ListBotAliases<br>• mediapackage-vod:ListPackagingConfigurations<br>• mediapackage-vod:ListPackagingGroups<br>• mq:ListBrokers<br>• personalize:ListDatasetGroups<br>• personalize:ListDatasets<br>• personalize:ListSchemas<br>• route53:ListHealthChecks | |

| Alteração | Descrição | Data |
| --- | --- | --- |
| | • `route53:ListHostedZones`<br>• `secretsmanager:ListSecrets` | |
| Nova política gerenciada pela | O Resource Explorer adicionou a seguinte política AWS gerenciada:<br>• AWSResourceExplorerOrganizationsAccess | 14 de novembro de 2023 |
| Atualização das políticas gerenciadas pela | O Resource Explorer atualizou as seguintes políticas AWS gerenciadas para oferecer suporte à pesquisa em várias contas:<br>• AWSResourceExplorerFullAccess<br>• AWSResourceExplorerReadOnlyAccess | 14 de novembro de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AWSResourceExplorerServiceRolePolicy— Política atualizada para oferecer suporte à pesquisa em várias contas com Organizations | O Explorador de Recursos adicionou permissões à política de perfil vinculado ao serviço AWSResourceExplorerServiceRolePolicy que permite que o Explorador de Recursos seja compatível com a pesquisa em várias contas com o Organizations:<br>• organizations:ListAWSServiceAccessForOrganization<br>• organizations:DescribeAccount<br>• organizations:DescribeOrganization<br>• organizations:ListAccounts<br>• organizations:ListDelegatedAdministrators | 14 de novembro de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AWSResourceExplorerServiceRolePolicy— Política atualizada para oferecer suporte a outros tipos de recursos | O Explorador de Recursos adicionou permissões à política de perfil vinculado ao serviço AWSResourceExplorerServiceRolePolicy que permite que o serviço indexe os seguintes tipos de recursos:<br>• accessanalyzer:analyzer<br>• acmpca:certificateauthority<br>• amplify:app<br>• amplify:backendenvironment<br>• amplify:branch<br>• amplify:domainassociation<br>• amplifyuibuilder:component<br>• amplifyuibuilder:theme<br>• appintegrations:eventintegration<br>• apprunner:service<br>• appstream:appblock<br>• appstream:application<br>• appstream:fleet<br>• appstream:imagebuilder<br>• appstream:stack<br>• appsync:graphqlapi<br>• aps:rulegroupsnamespace<br>• aps:workspace<br>• apigateway:restapi<br>• apigateway:deployment | 17 de outubro de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| | • athena:datacatalog<br>• athena:workgroup<br>• autoscaling:autoscalinggroup<br>• backup:backupplan<br>• batch:computeenvironment<br>• batch:jobqueue<br>• batch:schedulingpolicy<br>• cloudformation:stack<br>• cloudformation:stackset<br>• cloudfront:fieldlevelencryptionconfig<br>• cloudfront:fieldlevelencryptionprofile<br>• cloudfront:originaccesscontrol<br>• cloudtrail:trail<br>• codeartifact:domain<br>• codeartifact:repository<br>• codecommit:repository<br>• codeguruprofiler:profilinggroup<br>• codestarconnections:connection<br>• databrew:dataset<br>• databrew:recipe<br>• databrew:ruleset<br>• detective:graph<br>• directoryservices:directory<br>• ec2:carriergateway | |

| Alteração | Descrição | Data |
| --- | --- | --- |
| | • ec2:verifiedaccessendpoint<br>• ec2:verifiedaccessgroup<br>• ec2:verifiedaccessinstance<br>• ec2:verifiedaccesstrustprovider<br>• ecr:repository<br>• elasticache:cachesecuritygroup<br>• elasticfilesystem:accesspoint<br>• events:rule<br>• evidently:experiment<br>• evidently:feature<br>• evidently:launch<br>• evidently:project<br>• finspace:environment<br>• firehose:deliverystream<br>• faultinjectionsimulator:experimenttemplate<br>• forecast:datasetgroup<br>• forecast:dataset<br>• frauddetector:detector<br>• frauddetector:entitytype<br>• frauddetector:eventtype<br>• frauddetector:label<br>• frauddetector:outcome<br>• frauddetector:variable<br>• gamelift:alias<br>• globalaccelerator:accelerator | |

| Alteração | Descrição | Data |
| --- | --- | --- |
| | • globalaccelerator:endpointgroup<br>• globalaccelerator:listener<br>• glue:database<br>• glue:job<br>• glue:table<br>• glue:trigger<br>• greengrass:group<br>• healthlake:fhirdatastore<br>• iam:virtualmfadevice<br>• imagebuilder:componentbuildversion<br>• imagebuilder:component<br>• imagebuilder:containerrecipe<br>• imagebuilder:distributionconfiguration<br>• imagebuilder:imagebuildversion<br>• imagebuilder:imagepipeline<br>• imagebuilder:imagerecipe<br>• imagebuilder:image<br>• imagebuilder:infrastructureconfiguration<br>• iot:authorizer<br>• iot:jobtemplate<br>• iot:mitigationaction<br>• iot:provisioningtemplate<br>• iot:securityprofile<br>• iot:thing | |

| Alteração | Descrição | Data |
| --- | --- | --- |
| | • iot:topicruledestination<br>• iotanalytics:channel<br>• iotanalytics:dataset<br>• iotanalytics:datastore<br>• iotanalytics:pipeline<br>• iotevents:alarmmodel<br>• iotevents:detectormodel<br>• iotevents:input<br>• iotsitewise:assetmodel<br>• iotsitewise:asset<br>• iotsitewise:gateway<br>• iottwinmaker: espaço de trabalho<br>• ivs: canal<br>• ivs:streamkey<br>• kafka:cluster<br>• kinesisvideo:stream<br>• lambda:alias<br>• lambda:layerversion<br>• lambda:layer<br>• lookoutmetrics:alert<br>• lookoutvision:project<br>• mediapackage:channel<br>• mediapackage:origi nendpoint<br>• mediatailor:playbackconfigu ration<br>• memorydb:acl<br>• memorydb:cluster<br>• memorydb:parametergroup | |

| Alteração | Descrição | Data |
| --- | --- | --- |
| | • memorydb:user<br>• mobiletargeting:app<br>• mobiletargeting:segment<br>• mobiletargeting:template<br>• networkfirewall:firewallpolicy<br>• networkfirewall:firewall<br>• networkmanager:glo balnetwork<br>• networkmanager:device<br>• networkmanager:link<br>• networkmanager:attachment<br>• networkmanager:cor enetwork<br>• panorama:package<br>• qldb:journalkinesisstreamsf orledger<br>• qldb:ledger<br>• rds:bluegreendeployment<br>• refactorspaces:application<br>• refactorspaces:environment<br>• refactorspaces:route<br>• refactorspaces:service<br>• rekognition:project<br>• resiliencehub:app<br>• resiliencehub:resiliencypol icy<br>• resourcegroups:group<br>• route53:recoverygroup<br>• route53:resourceset<br>• route53:firewalldomain | |

| Alteração | Descrição | Data |
| --- | --- | --- |
| | • route53:firewallrulegroup<br>• route53:resolverendpoint<br>• route53:resolverrule<br>• sagemaker:model<br>• sagemaker:notebook instance<br>• signer:signingprofile<br>• ssmincidents:responseplan<br>• ssm:inventoryentry<br>• ssm:resourcedatasync<br>• states:activity<br>• timestream:database<br>• wisdom:assistant<br>• wisdom:assistantassociation<br>• wisdom:knowledgebase | |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AWSResourceExplorerServiceRolePolicy— Política atualizada para oferecer suporte a outros tipos de recursos | O Explorador de Recursos adicionou permissões à política de perfil vinculado ao serviço AWSResourceExplorerServiceRolePolicy que permite que o serviço indexe os seguintes tipos de recursos:<br>• codebuild:project<br>• pipeline de código: pipeline<br>• cognito:identitypool<br>• cognito:userpool<br>• ecr:repository<br>• efs:filesystem<br>• elasticbeanstalk:application<br>• elasticbeanstalk:applicationversion<br>• elasticbeanstalk:environment<br>• iot:policy<br>• iot:topicrule<br>• stepfunctions:statemachine<br>• s3:bucket | 1º de agosto de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| AWSResourceExplorerServiceRolePolicy— Política atualizada para oferecer suporte a outros tipos de recursos | O Explorador de Recursos adicionou permissões à política de perfil vinculado ao serviço `AWSResourceExplorerServiceRolePolicy` que permite que o serviço indexe os seguintes tipos de recursos:<br>• elasticache:cluster<br>• elasticache:globalreplicationgroup<br>• elasticache:parametergroup<br>• elasticache:replicationgroup<br>• elasticache:reserved-instance<br>• elasticache:snapshot<br>• elasticache:subnetgroup<br>• elasticache:user<br>• elasticache:usergroup<br>• lambda:code-signing-config<br>• lambda:event-source-mapping<br>• sqs:queue | 7 de março de 2023 |

| Alteração | Descrição | Data |
| --- | --- | --- |
| Novas políticas gerenciadas | O Resource Explorer adicionou as seguintes políticas AWS gerenciadas:<br>• AWSResourceExplorerFullAccess<br>• AWSResourceExplorerReadOnlyAccess<br>• AWSResourceExplorerServiceRolePolicy | 7 de novembro de 2022 |
| O Explorador de Recursos começou a monitorar alterações | O Resource Explorer começou a monitorar as alterações em suas políticas AWS gerenciadas. | 7 de novembro de 2022 |

## Usar perfis vinculados ao serviço para o Explorador de Recursos

Explorador de recursos da AWS usa AWS Identity and Access Management (IAM) funções vinculadas ao serviço. Uma função vinculada ao serviço é um tipo exclusivo de IAM função vinculada diretamente ao Resource Explorer. As funções vinculadas ao serviço são predefinidas pelo Resource Explorer e incluem todas as permissões que o serviço exige para ligar para outras pessoas Serviços da AWS em seu nome.

Um perfil vinculado ao serviço facilita a configuração do Explorador de Recursos porque você não tem que adicionar as permissões necessárias manualmente. O Explorador de Recursos define as permissões dos perfis vinculados ao serviço e, exceto se definido de outra forma, somente o Explorador de Recursos pode assumir seus perfis. As permissões definidas incluem a política de confiança e a política de permissões, e essa política de permissões não pode ser atribuída a nenhuma outra IAM entidade.

Para obter informações sobre outros serviços que oferecem suporte a funções vinculadas a serviços, consulte AWS serviços que funcionam com IAM no Guia do IAMusuário. Procure os serviços com Sim na coluna Perfis vinculados ao serviço. Escolha um Sim com um link para visualizar a documentação da função vinculada a esse serviço.

## Permissões de perfil vinculado ao serviço para o Explorador de Recursos

O Explorador de Recursos usa o perfil vinculado ao serviço denominado `AWSServiceRoleForResourceExplorer`. Essa função concede permissões ao serviço Resource Explorer para visualizar recursos e AWS CloudTrail eventos Conta da AWS em seu nome e indexar esses recursos para apoiar a pesquisa.

O perfil vinculado ao serviço do `AWSServiceRoleForResourceExplorer` só confia no serviço com a seguinte entidade principal para assumir o perfil:

- `resource-explorer-2.amazonaws.com`

A política de permissões de função denominada AWSResourceExplorerServiceRolePolicy permite que o Resource Explorer tenha acesso somente de leitura para recuperar nomes e propriedades de recursos compatíveis. AWS Para ver os serviços e recursos compatíveis com o Explorador de Recursos, consulte Tipos de recursos que você pode pesquisar com o Explorador de Recursos. Para obter a lista completa de todas as ações que essa função pode executar, você pode visualizar a `AWSResourceExplorerServiceRolePolicy` política no IAM console.

Um principal é uma IAM entidade, como um usuário, grupo ou função. Se você permitir que o Explorador de Recursos crie o perfil vinculado ao serviço para você quando ele criar o índice na primeira região da conta, a entidade principal que está realizando a tarefa só precisará das permissões requeridas para criar o índice do Explorador de Recursos. Para criar a função vinculada ao serviço manualmente usandoIAM, o diretor que executa a tarefa deve ter permissão para criar uma função vinculada ao serviço. Para obter mais informações, consulte Permissões de funções vinculadas ao serviço no Guia do IAMusuário.

## Criar um perfil vinculado ao serviço para o Explorador de Recursos

Não é necessário criar manualmente uma função vinculada ao serviço. Quando você ativa o Resource Explorer no AWS Management Console, ou executa o primeiro CreateIndex Região da AWS em sua conta usando o AWS CLI ou um AWS API, o Resource Explorer cria a função vinculada ao serviço para você.

Se você excluir esse perfil vinculado ao serviço e precisar criá-lo novamente, poderá usar esse mesmo processo para recriar o perfil na sua conta. Quando você está RegisterResourceExplorerna primeira região da sua conta, o Resource Explorer cria a função vinculada ao serviço para você novamente.

### Editar um perfil vinculado ao serviço para o Explorador de Recursos

O Explorador de Recursos não permite que você edite o perfil vinculado a serviço `AWSServiceRoleForResourceExplorer`. Depois que você criar um perfil vinculado ao serviço, não poderá alterar o nome do perfil, pois várias entidades podem fazer referência ao perfil. No entanto, você pode editar a descrição da função usandoIAM. Para obter mais informações, consulte Edição de uma função vinculada ao serviço no Guia do IAMusuário.

### Excluir um perfil vinculado ao serviço do Explorador de Recursos

Você pode usar o IAM console AWS CLI, o ou o AWS API para excluir manualmente a função vinculada ao serviço. Para fazer isso, primeiro você deve remover os índices do Resource Explorer de cada parte da sua conta e, Região da AWS em seguida, excluir manualmente a função vinculada ao serviço.

> **Note**
>
> Se o serviço do Explorador de Recursos estiver usando o perfil quando você tentar excluir os recursos, poderá ocorrer uma falha na exclusão. Se isso acontecer, certifique-se de que todos os índices de todas as regiões sejam excluídos, espere alguns minutos e tente a operação novamente.

Para excluir manualmente a função vinculada ao serviço usando IAM

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

### Regiões compatíveis com os perfis vinculados ao serviço do Explorador de Recursos

O Explorador de Recursos é compatível com perfis vinculados ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte AWS service (Serviço da AWS) endpoints na Referência geral da Amazon Web Services.

## Solução de problemas de Explorador de recursos da AWS permissões

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o Resource Explorer e AWS Identity and Access Management (IAM).

Tópicos



## Não tenho autorização para realizar uma ação no Explorador de Recursos

Se isso AWS Management Console indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda. O administrador é a pessoa que forneceu as credenciais que você usou para tentar essa operação.

Por exemplo, o erro a seguir ocorre quando alguém assume o perfil do IAM `MyExampleRole` e tenta usar o console para visualizar detalhes, mas não tem a permissão de `resource-explorer-2:GetView`.

```
User: arn:aws:iam::123456789012:role/MyExampleRole is not authorized to perform:
 resource-explorer-2:GetView on resource: arn:aws:resource-explorer-2:us-
east-1:123456789012:view/EC2-Only-View/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111
```

Nesse caso, a pessoa usando o perfil deve solicitar ao administrador que atualize as políticas de permissão do perfil para conceder acesso à visualização usando a ação `resource-explorer-2:GetView`.

## Quero permitir que pessoas fora da minha acessem meus Conta da AWS recursos do Resource Explorer

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem compatibilidade com políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Explorador de Recursos é compatível com esses recursos, consulte Como o Resource Explorer funciona com IAM.

- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

# Proteção de dados em Explorador de recursos da AWS

O modelo de responsabilidade AWS compartilhada modelo se aplica à proteção de dados em Explorador de recursos da AWS. 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 o Resource Explorer ou outro Serviços da AWS usando o consoleAPI, 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.

## Criptografia em repouso

Os dados armazenados pelo Resource Explorer incluem a lista indexada dos recursos e seus associados ARNs que são usados pelo cliente e as visualizações para acessá-los.

Esses dados são criptografados quando em repouso usando AWS Key Management Service (AWS KMS) chaves de criptografia simétricas que implementam o Advanced Encryption Standard (AES) no Galois Counter Mode (GCM) com chaves de 256 bits (AES-256-). GCM

## Criptografia em trânsito

As solicitações do cliente e todos os dados associados são criptografados em trânsito usando o Transport Later Security (TLS) 1.2 ou posterior. Todos os endpoints do Resource Explorer oferecem suporte HTTPS à criptografia de dados em trânsito. Para obter uma lista de endpoints de serviço do Explorador de Recursos, consulte Explorador de recursos da AWS endpoints and quotas na Referência geral da AWS.

# Validação de conformidade do Explorador de recursos da AWS

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas específicos de conformidade, consulte Serviços da Serviços da AWS no escopo por programa de conformidade. Para obter informações gerais, consulteAWS Programas de conformidade.

É possível fazer download de relatórios de auditoria de terceiros usando o AWS Artifact. Para obter mais informações, consulte Downloading reports in AWS Artifact no AWS Artifact User Guide.

Sua responsabilidade em relação à compatibilidade ao usar o Explorador de Recursos é determinada pelo grau de confidencialidade dos dados, pelos objetivos de compatibilidade da sua empresa e pelos regulamentos e leis aplicáveis. A AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido de segurança e compatibilidade: estes guias de implantação abordam as considerações de arquitetura e fornecem etapas para implantação de ambientes de linha de base focados em compatibilidade e segurança na AWS.
- Architecting for HIPAA Security and Compliance on Amazon Web Services: esse artigo técnico descreve como as empresas podem usar o AWS para criar aplicações elegíveis para a HIPAA.

  > **Note**
  >
  > Nem todos os Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- atributos de conformidade da AWS: essa coleção de manuais e guias pode ser aplicada a seu setor e local.
- Avaliação de recursos com regras no AWS ConfigGuia do desenvolvedor – AWS Configavalia a conformidade das configurações de seus recursos com práticas internas, diretrizes do setor e regulamentos.
- AWS Security Hub: esse serviço da AWS fornece uma visão abrangente do estado da segurança na AWS que ajuda verificar a conformidade com os padrões e as práticas recomendadas de segurança do setor.

## Resiliência no Explorador de recursos da AWS

A infraestrutura global da AWS é criada com base em Regiões da AWS e zonas de disponibilidade. As regiões fornecem várias zonas de disponibilidade separadas e isoladas fisicamente, que são conectadas com baixa latência, alta throughput e redes altamente redundantes. Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas 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 Explorador de recursos da AWS

Como serviço gerenciado, Explorador de recursos da AWS 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 o Resource Explorer 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.

Para obter mais informações sobre procedimentos AWS globais de segurança de rede, consulte o whitepaper Amazon Web Services: Visão geral dos processos de segurança.

# Monitorar o Explorador de recursos da AWS

O monitoramento é uma parte importante de manter a confiabilidade, a disponibilidade e a performance do Explorador de recursos da AWS e das outras soluções da AWS. A AWS fornece as ferramentas de monitoramento a seguir para observar o Explorador de Recursos, informar quando algo está errado e realizar ações automaticamente quando apropriado:

- O AWS CloudTrail captura chamadas de API e eventos relacionados feitos por sua conta da Conta da AWS ou em nome dela e entrega os arquivos de log a um bucket do Amazon S3 que você especifica. Você pode identificar quais usuários e contas chamaram a AWS, o endereço IP de origem do qual as chamadas foram feitas e quando elas ocorreram. Para obter mais informações, consulte Registrar em log chamadas de API do Explorador de recursos da AWS usando o AWS CloudTrail e o Manual do usuário do AWS CloudTrail.

# Registrar em log chamadas de API do Explorador de recursos da AWS usando o AWS CloudTrail

O Explorador de recursos da AWS é integrado ao AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, um perfil ou um AWS service (Serviço da AWS) no Explorador de Recursos. O CloudTrail captura todas as chamadas da API do Explorador de Recursos como eventos. As chamadas capturadas incluem as chamadas do console do Explorador de Recursos e as chamadas de código para operações da API do Explorador de Recursos.

Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail a um bucket do Amazon S3, incluindo os eventos para o Explorador de Recursos. Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log a um bucket do Amazon S3 especificado. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Com as informações coletadas pelo CloudTrail, você pode determinar a solicitação que foi feita ao Explorador de Recursos, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

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

## Informações do Explorador de Recursos no CloudTrail

O CloudTrail é habilitado em sua Conta da AWS quando ela é criada. Quando ocorre alguma atividade no Systems Manager, ela é registrada em um evento do CloudTrail junto com outros

eventos do AWS service (Serviço da AWS) no Histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua Conta da AWS. Para obter mais informações, consulte Viewing events with CloudTrail Event history (Como visualizar eventos com o histórico de eventos do CloudTrail).

> **Important**
>
> Você pode encontrar todos os eventos do Explorador de Recursos pesquisando Fonte do evento = resource-explorer-2.amazonaws.com

Para ter um registro contínuo dos eventos na sua Conta da AWS, inclusive os eventos do Explorador de Recursos, 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, você pode 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 os seguintes tópicos no Guia do usuário do AWS CloudTrail:

- Criar uma trilha para a sua Conta da AWS
- Integrações de serviços da AWS com logs do CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail
- Recebimento de arquivos de log do CloudTrail de várias regiões
- Recebimento de arquivos de log do CloudTrail de várias contas

Todas as ações do Explorador de Recursos são registradas pelo CloudTrail e são documentadas na Explorador de recursos da AWS API Reference. Por exemplo, as chamadas para as APIs `CreateIndex`, `DeleteIndex` e `UpdateIndex` geram entradas nos arquivos de log do CloudTrail.

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

- Credenciais da raiz da Conta da AWS
- 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.

> **Important**
>
> Por razões de segurança, todos os valores de `Tags`, `Filters` e `QueryString` são ocultados nas entradas de trilha do CloudTrail.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail.

## Noções básicas sobre entradas de arquivos de log do Explorador de Recursos

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.

Tópicos

- CreateIndex
- DeleteIndex
- UpdateIndexType
- Pesquisar
- CreateView
- DeleteView
- DisassociateDefaultView

### CreateIndex

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação `CreateIndex`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
```

```
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-166EXAMPLE",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-166EXAMPLE",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-23T19:13:59Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "CreateIndex",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.create-index",
    "requestParameters": {
        "ClientToken": "792ee665-58af-423c-bfdb-d7c9aEXAMPLE"
    },
    "responseElements": {
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
        "State": "CREATING",
        "CreatedAt": "2022-08-23T19:13:59.775Z"
    },
    "requestID": "a193afe9-17ff-4f30-ae0a-73bb0EXAMPLE",
    "eventID": "2ec50598-4de6-474d-bd0e-f5c00EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
```

```
}
```

## DeleteIndex

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação `DeleteIndex`.

> **Note**
>
> Essa ação também exclui todas as visualizações da conta nessa região de modo assíncrono, o que gera um evento do `DeleteView` para cada visualização excluída.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:My-Role-Name",
        "arn": "arn:aws:sts::123456789012:assumed-role/My-Admin-Role/My-Delegated-
Role",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/My-Admin-Role",
                "accountId": "123456789012",
                "userName": "My-Admin-Role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T18:33:06Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-23T19:04:06Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "DeleteIndex",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
```

```
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.delete-index",
    "requestParameters": {
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-RequestId,x-amzn-ErrorType,x-amzn-
ErrorMessage,Date",
        "State": "DELETING",
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    },
    "requestID": "d7d80bd2-cd2d-47fb-88d6-5133aEXAMPLE",
    "eventID": "675eab39-c514-4d32-989d-0ea98EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

## UpdateIndexType

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação `UpdateIndexType` para promover um índice do tipo `LOCAL` a `AGGREGATOR`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
```

```
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-23T19:21:18Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "UpdateIndexType",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.update-index-type",
    "requestParameters": {
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
        "Type": "AGGREGATOR"
    },
    "responseElements": {
        "Type": "AGGREGATOR",
        "Arn": "arn:aws:resource-explorer-2:us-
east-1:123456789012:index/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111",
        "LastUpdatedAt": "2022-08-23T19:21:17.924Z",
        "State": "UPDATING"
    },
    "requestID": "a145309d-df14-4c2e-a9f6-8ed45EXAMPLE",
    "eventID": "ed33ab96-f5c6-4a77-a69a-8585aEXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

## Pesquisar

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação `Search`.

> **Note**
>
> Por razões de segurança, todas as referências aos parâmetros `Tag`, `Filters` e `QueryString` são ocultadas nas entradas de trilha do CloudTrail.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-08-03T16:50:11Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "Search",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.search",
    "requestParameters": {
        "QueryString": "***"
    },
    "responseElements": null,
    "requestID": "22320db5-b194-446f-b9f4-e603bEXAMPLE",
```

```
    "eventID": "addb3bca-0c41-46bf-a5e6-42299EXAMPLE",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

## CreateView

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação `CreateView`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-01-20T21:54:48Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "CreateView",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.create-view",
```

```
    "requestParameters": {
        "ViewName": "CTTagsTest",
        "Tags": "***"
    },
    "responseElements": {
        "View": {
            "Filters": "***",
            "IncludedProperties": [],
            "LastUpdatedAt": "2023-01-20T21:54:48.079Z",
            "Owner": "123456789012",
            "Scope": "arn:aws:iam::123456789012:root",
            "ViewArn": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
CTTest/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
        }
    },
    "requestID": "b22d8ced-4905-42c4-b1aa-ef713EXAMPLE",
    "eventID": "f62e339f-1070-41a8-a6ec-12491EXAMPLE",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```


## DeleteView

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra o evento que pode ocorrer quando a ação `DeleteView` é iniciada automaticamente por causa de uma operação `DeleteIndex` na mesma Região da AWS.

> **Note**
>
> Se a visualização excluída for a visualização padrão para a região, essa ação também desassociará a visualização como padrão de modo assíncrono. Isso gera um evento `DisassociateDefaultView`.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAEXAMPLEEXAMPLE:botocore-session-1661282039",
```

```
        "arn": "arn:aws:sts::123456789012:assumed-role/cli-role/botocore-
session-1661282039",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAEXAMPLEEXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/cli-role",
                "accountId": "123456789012",
                "userName": "cli-role"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-08-23T19:13:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-09-16T19:33:27Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "DeleteView",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.delete-view",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "cd174d1e-0a24-4b47-8b67-d024aEXAMPLE",
    "readOnly": false,
    "resources": [{
        "accountId": "334026708824",
        "type": "AWS::ResourceExplorer2::View",
        "ARN": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/
CTTest/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
    }],
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

## DisassociateDefaultView

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra o evento que pode ocorrer quando a ação `DisassociateDefaultView` é iniciada automaticamente por causa de uma operação `DeleteView` na visualização padrão atual.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "resource-explorer-2.amazonaws.com"
    },
    "eventTime": "2022-09-16T19:33:26Z",
    "eventSource": "resource-explorer-2.amazonaws.com",
    "eventName": "DisassociateDefaultView",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "10.24.34.15",
    "userAgent": "aws-cli/2.7.14 Python/3.9.11 Windows/10 exe/AMD64 prompt/off command/
resource-explorer-2.disassociate-default-view",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "d8016cb1-5c23-4ea4-bda2-70b03EXAMPLE",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

# Solução de problemas do Explorador de Recursos

Se você encontrar problemas ao trabalhar com o Explorador de Recursos, consulte os tópicos desta seção. Veja também Solução de problemas de Explorador de recursos da AWS permissões na seção Segurança deste guia.

Tópicos



# Problemas gerais

Tópicos



## Recebi um link para o Explorador de Recursos, mas quando o abro, o console mostra apenas um erro.

Algumas ferramentas de terceiros geram URLs de link para páginas do Explorador de Recursos. Em alguns casos, essas URLs não incluem o parâmetro que direciona o console para uma Região da AWS específica. Se você abrir esse link, o console do Explorador de Recursos não será informado sobre qual região usar e usará, por padrão, a última região na qual o usuário fez login. Se o usuário não tiver permissões para acessar o Explorador de Recursos nessa região, o console tentará usar a região Leste dos EUA (Norte da Virgínia) (`us-east-1`) ou Oeste dos EUA (Oregon) (`us-west-2`) se não puder acessar a região `us-east-1`.

Se o usuário não tiver permissão para acessar o índice em nenhuma dessas regiões, o console do Explorador de Recursos retornará um erro.

Você pode evitar esse problema garantindo que todos os usuários tenham as seguintes permissões:

- `ListIndexes`: nenhum recurso específico; use `*`.
- `GetIndex` para o ARN de cada índice criado na conta. Para evitar ter que refazer as políticas de permissão se excluir e recriar um índice, recomendamos que você use um `*`.

A política mínima para conseguir isso pode ser semelhante a este exemplo:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetIndex",
                "resource-explorer-2:ListIndexes",
            ],
            "Resource": "*"
        }
    ]
}
```

Como alternativa, você pode pensar em anexar a permissão gerenciada pela `AWSAWSResourceExplorerReadOnlyAccess` a todos os usuários que precisem usar o Explorador de Recursos. Isso concede essas permissões requeridas, além das permissões necessárias para ver as visualizações disponíveis na região e pesquisar usando essas visualizações.

## Por que a pesquisa unificada no console causa erros de "acesso negado" nos meus registros do CloudTrail?

A pesquisa unificada do AWS Management Console permite que as entidades principais pesquisem em qualquer página do AWS Management Console. Os resultados podem incluir recursos da conta da entidade principal se o Explorador de Recursos estiver ativado e configurado para possibilitar a pesquisa unificada. Sempre que você começa a digitar na barra de pesquisa unificada, a pesquisa unificada tenta chamar a operação `resource-explorer-2:ListIndexes` para verificar se é possível incluir recursos da conta do usuário nos resultados.

A pesquisa unificada usa as permissões do usuário que está conectado no momento para realizar essa verificação. Se esse usuário não tiver permissão para chamar `resource-explorer-2:ListIndexes`, concedida em uma política de permissão anexada ao AWS Identity

and Access Management (IAM), a verificação falhará. Essa falha é adicionada como uma entrada de `Access denied` nos logs do CloudTrail.

Essa entrada de log do CloudTrail tem as seguintes características:

- Origem do evento: `resource-explorer-2.amazonaws.com`
- Nome do evento: `ListIndexes`
- Código de erro: `403` (acesso negado)

As políticas gerenciadas pela AWS a seguir incluem permissão para chamar `resource-explorer-2:ListIndexes`. Se você atribuir qualquer uma delas à entidade principal, ou qualquer outra política que inclua essa permissão, esse erro não ocorrerá:

- AWSResourceExplorerReadOnlyAccess
- AWSResourceExplorerFullAccess
- ReadOnlyAccess
- ViewOnlyAccess

# Solução de problemas de instalação e configuração do Explorador de Recursos

Use estas informações para ajudá-lo a diagnosticar e corrigir problemas que podem ocorrer quando você instala ou configura inicialmente o Explorador de recursos da AWS.

Tópicos

- Eu recebo uma mensagem de "acesso negado" quando faço uma solicitação ao Explorador de Recursos
- Eu recebo uma mensagem de "acesso negado" quando faço uma solicitação com credenciais de segurança temporárias

# Eu recebo uma mensagem de "acesso negado" quando faço uma solicitação ao Explorador de Recursos

- Verifique se você tem permissões para chamar a ação e o recurso que solicitou. Um administrador pode conceder permissões atribuindo uma política de permissão do AWS Identity and Access Management (IAM) à sua entidade principal do IAM, como um perfil, um grupo ou um usuário.

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

  - Usuários e grupos no AWS IAM Identity Center:

    Crie um conjunto de permissões. Siga as instruções em Create a permission set (Criação de um conjunto de permissões) no Guia do usuário do AWS IAM Identity Center.

  - Usuários gerenciados no IAM usando um provedor de identidades:

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

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

  A política deve permitir a `Action` solicitada no `Resource` que você deseja acessar.

  Se as declarações de política que concedem essas permissões incluírem condições, como horário do dia ou restrições de endereço IP, você também deverá cumprir esses requisitos ao enviar a solicitação. Para obter informações sobre como visualizar ou modificar políticas para uma entidade principal do IAM, consulte Gerenciar políticas do IAM no Guia do usuário do IAM.

- Se você estiver assinando as solicitações de API manualmente (sem usar os SDKs da AWS), verifique se assinou a solicitação corretamente.

## Eu recebo uma mensagem de "acesso negado" quando faço uma solicitação com credenciais de segurança temporárias

- Verifique se a entidade principal do IAM que você está usando para fazer a solicitação tem as permissões corretas. As permissões para credenciais de segurança temporárias são derivadas de uma entidade principal definida no IAM, para que as permissões sejam limitadas às concedidas à entidade principal. Para obter mais informações sobre como as permissões de credenciais de segurança temporárias são determinadas, consulte Controle de permissões para credenciais de segurança temporárias no Guia do usuário do IAM.
- Verifique se suas solicitações estão sendo assinadas corretamente e se a solicitação está bem formulada. Para obter detalhes, consulte a documentação do toolkit para o SDK escolhido ou Uso de credenciais temporárias com recursos da AWS no Guia do usuário do IAM.
- Verifique se suas credenciais de segurança temporárias não expiraram. Para obter mais informações, consulte Solicitação de credenciais de segurança temporárias no Guia do usuário do IAM.

# Solução de problemas de pesquisa do Explorador de Recursos

Use estas informações para ajudar você a diagnosticar e corrigir erros comuns que podem ocorrer quando pesquisa os recursos usando o Explorador de Recursos.

Tópicos



## Por que alguns recursos não aparecem nos meus resultados de pesquisa do Explorador de Recursos?

A lista a seguir fornece os motivos pelos quais alguns recursos podem não aparecer nos resultados da pesquisa como esperado:

A indexação inicial não foi concluída

Depois de ativar inicialmente o Resource Explorer em um Região da AWS, pode levar até 36 horas para que a indexação e a replicação no índice agregador sejam concluídas. Tente pesquisar novamente mais tarde.

O recurso é novo

Pode levar alguns minutos para um novo recurso ser descoberto pelo Explorador de Recursos e adicionado ao índice local. Tente novamente em alguns minutos.

As informações sobre um novo recurso em uma região ainda não foram propagadas para o índice agregador

Pode levar algum tempo para que os detalhes sobre um novo recurso descoberto em uma região sejam indexados em sua própria região e depois replicados no índice agregador da conta. O novo recurso pode aparecer nos resultados da pesquisa inter-regional apenas após a conclusão da replicação. Tente pesquisar novamente mais tarde.

A região com o recurso não tem o Explorador de Recursos ativado

Seu administrador determina em quais recursos Regiões da AWS o Resource Explorer pode operar. A página Configurações mostra quais regiões têm o Explorador de Recursos ativado e contêm um índice. Se a região com seu recurso não estiver ativada, peça ao administrador que ative o Explorador de Recursos nessa região.

O recurso existe em outra região e a região pesquisada não contém o índice agregador

Você só pode pesquisar recursos em todas as regiões da conta usando uma visualização na região que contém o índice agregador. As pesquisas em qualquer outra região só retornam os recursos da região na qual você realiza a pesquisa.

Os filtros na visualização excluem esse recurso

Toda visualização pode incluir filtros na configuração que restrinjam quais resultados podem ser incluídos nos resultados das pesquisas feitas com essa visualização. Verifique se o recurso que você está procurando corresponde aos filtros da visualização usada na pesquisa. Para obter mais informações sobre filtros, consulteFiltros.

O tipo de recurso não é suportado pelo Resource Explorer

Alguns tipos de recurso não são compatíveis com o Explorador de Recursos. Para obter mais informações, consulte Tipos de recursos que você pode pesquisar com o Explorador de Recursos.

Índices ou visualizações não estão configurados na região do console

Se os índices ou visualizações não estiverem configurados nas regiões esperadas pelo console que consome o widget, você não verá os resultados esperados. Para obter mais informações, consulte Ativar a pesquisa inter-regional criando um índice agregador.

Suas visualizações não incluem tags

As tags são exigidas pelo widget Resource Explorer. Se suas visualizações não incluírem tags, os recursos não serão incluídos em seus resultados. Para obter mais informações, consulte Adicionar tags a visualizações.

Sua pesquisa usa a sintaxe de consulta de pesquisa errada

A pesquisa no Resource Explorer é exclusiva desse serviço. Sem a sintaxe correta, você não encontrará os recursos que espera. Para obter mais informações, consulte Referência da sintaxe de consulta de pesquisa do Explorador de Recursos.

Você marcou recentemente seus recursos

Depois de marcar um recurso, há um atraso de 30 segundos antes que ele apareça nos resultados da pesquisa.

O tipo de recurso não é compatível com filtros de tag

Se os filtros de tag não forem compatíveis com o tipo de recurso, eles não serão exibidos no widget Resource Explorer. Os tipos de recursos que não oferecem suporte a filtros de tag são:

- `cloudfront:cache-policy`
- `cloudfront:origin-access-identity`
- `cloudfront:function`
- `cloudfront:origin-request-policy`
- `cloudfront:realtime-log-config`
- `cloudfront:response-headers-policy`
- `cloudwatch:dashboard`
- `docdb:globalcluster`
- `elasticache:globalreplicationgroup`
- `iam:group`
- `lambda:code-signing-config`

- `lambda:event-source-mapping`
- `ssm:windowtarget`
- `ssm:windowtask`
- `rds:auto-backup`
- `rds:global-cluster`
- `s3:accesspoint`

## Por que meus recursos não estão aparecendo nos resultados da pesquisa unificada no console?

Os resultados da pesquisa unificada estão disponíveis na barra de pesquisa na parte superior de toda página do AWS Management Console . Porém, a pesquisa pode retornar os recursos que correspondem à consulta nos resultados da pesquisa apenas após as seguintes opções de configuração serem preenchidas:

- Deve haver um índice agregador em uma das regiões da conta.
- Deve haver uma visualização padrão na região que contém o índice agregador.
- Todos os diretores (IAMfunções e usuários) devem ter permissão para pesquisar usando essa visualização padrão.

## Por que a pesquisa unificada feita no console e feita no Explorador de Recursos às vezes fornecem resultados diferentes?

Os resultados da pesquisa unificada estão disponíveis na barra de pesquisa na parte superior de toda página do AWS Management Console . Quando você usa a pesquisa unificada, o processo de pesquisa unificada insere automaticamente um caractere curinga (*) no final do primeiro termo digitado na string de consulta. Esse caractere curinga não fica visível na caixa de pesquisa unificada, mas afeta os resultados.

> **Important**
>
> A pesquisa unificada insere automaticamente um operador de caractere curinga (*) no final da primeira palavra-chave da string. Isso significa que os resultados da pesquisa unificada incluem os recursos que correspondem a qualquer string que comece com a palavra-chave especificada.

A pesquisa realizada pela caixa de texto Consulta na página Pesquisa de recursos no console do Explorador de Recursos não adiciona automaticamente um caractere curinga. Você pode inserir um * manualmente depois de qualquer termo na string de pesquisa.

## Quais permissões eu preciso ter para poder pesquisar recursos?

Para pesquisar, você deve ter permissão para realizar ambas as operações a seguir em uma visualização que resida na região em que você chamar a operação:

- `resource-explorer-2:GetView`
- `resource-explorer-2:Search`

Isso pode ser feito adicionando uma declaração semelhante ao exemplo a seguir a uma política atribuída ao seu IAM diretor.

```
        {
            "Effect": "Allow",
            "Action": [
                "resource-explorer-2:GetView",
                "resource-explorer-2:Search"
            ],
            "Resource": "arn:aws:resource-explorer-2:us-east-1:123456789012:view/My-
View-Name/1a2b3c4d-5d6e-7f8a-9b0c-abcd11111111"
        }
```

Você pode substituir o Amazon Resource Number (ARN) de uma visualização específica por um ARN que inclua um curinga (*) para conceder permissão a todas as visualizações correspondentes.

Se você não especificar uma visualização na sua solicitação, o Explorador de Recursos usará automaticamente a visualização padrão da região na qual você fez a solicitação. Se você não tiver permissões para usar a visualização padrão, fale com o administrador.

> **Note**
>
> Mesmo que veja um recurso nos resultados de uma consulta de pesquisa do Explorador de Recursos, você precisará de permissões no próprio recurso para poder interagir com ele.

# Cotas do Explorador de Recursos

Sua Conta da AWS tem cotas padrão para cada AWS service (Serviço da AWS). A menos que especificado de outra forma, cada cota é específica da região. Você pode solicitar aumentos para algumas cotas e outras cotas não podem ser aumentadas.

Para visualizar todas as cotas do Explorador de recursos da AWS, abra o console do Service Quotas. No painel de navegação, escolha Serviços da AWS e selecione Explorador de Recursos.

Para solicitar o aumento da cota, consulte Requesting a Quota Increase (Solicitar um aumento de cota) no Guia do usuário do Service Quotas. Se a cota ainda não estiver disponível no Service Quotas, use o formulário de aumento de limite.

As cotas a seguir são os padrões para o Explorador de Recursos.

| Cotas de valor máximo | Valor padrão |
|---|---|
| Número de visualizações em uma Região da AWS | 10 |

| Limites de taxa para operações | Valor padrão |
|---|---|
| Máximo de operações de pesquisa por segundo | 5 |
| Máximo de operações que não são de pesquisa por segundo | 3 |
| Máximo de operações de pesquisa na região de agregação por mês | 10.000 |
| Máximo de operações de pesquisa nas regiões locais por mês | 500 |

# Usando Explorador de recursos da AWS com um AWS SDK

AWS kits de desenvolvimento de software (SDKs) estão disponíveis para muitas linguagens de programação populares. Cada um SDK API fornece exemplos de código e documentação que facilitam aos desenvolvedores a criação de aplicativos em seu idioma preferido.

| SDKdocumentação | Exemplos de código |
| --- | --- |
| AWS SDK for C++ | AWS SDK for C++ exemplos de código |
| AWS CLI | AWS CLI exemplos de código |
| AWS SDK for Go | AWS SDK for Go exemplos de código |
| AWS SDK for Java | AWS SDK for Java exemplos de código |
| AWS SDK for JavaScript | AWS SDK for JavaScript exemplos de código |
| AWS SDK para Kotlin | AWS SDK para Kotlin exemplos de código |
| AWS SDK for .NET | AWS SDK for .NET exemplos de código |
| AWS SDK for PHP | AWS SDK for PHP exemplos de código |
| AWS Tools for PowerShell | Ferramentas para exemplos PowerShell de código |
| AWS SDK for Python (Boto3) | AWS SDK for Python (Boto3) exemplos de código |
| AWS SDK for Ruby | AWS SDK for Ruby exemplos de código |
| AWS SDK para Rust | AWS SDK para Rust exemplos de código |
| SDK da AWS para SAP ABAP | SDK da AWS para SAP ABAP exemplos de código |
| AWS SDK for Swift | AWS SDK for Swift exemplos de código |

Exemplo de disponibilidade

Você não consegue encontrar o que precisa? Solicite um código de exemplo no link Fornecer feedback na parte inferior desta página.

# Histórico de documento para o Guia do usuário do Explorador de Recursos

A tabela a seguir descreve as versões de documentação do Explorador de recursos da AWS. Para receber notificações sobre atualizações desta documentação, você pode assinar um RSS feed.

| Alteração | Descrição | Data |
| --- | --- | --- |
| Novo filtro de pesquisa adicionado | O Resource Explorer adicionou um novo filtro de consulta de `tag:all` pesquisa, permitindo que você pesquise recursos que tenham uma ou mais tags criadas pelo usuário anexadas, mesmo que o tipo de recurso não seja suportado no Resource Explorer. | 6 de setembro de 2024 |
| Melhorias na organização de conteúdo | Títulos de tópicos atualizados e conteúdo reorganizado para melhorar a legibilidade e a capacidade de descoberta. | 29 de agosto de 2024 |
| Aviso para atualizar IAM as políticas para IPv6 | Os clientes que estão usando o endereçamento duplo com ASPEN políticas que contêm `aws:sourceIp` são afetados por essa atualização. O endereçamento duplo significa que a rede oferece suporte tanto para IPv4 quantoIPv6. | 15 de julho de 2024 |
| Suporte descontinuado para três tipos de recursos | O Resource Explorer interrompeu o suporte para | 9 de julho de 2024 |

| | | |
|---|---|---|
| | os três tipos de recursos a seguir: `ecs:taskssm:automation-execution` , e. `ssm:patchbaseline` | |
| Adicionada compatibilidade com novos tipos de recursos | O Resource Explorer adicionou suporte para 65 novos recursos AWS Key Management Service, Serviços da AWS incluindo o Amazon Route 53 e o Amazon Fraud Detector. | 20 de fevereiro de 2024 |
| Política gerenciada atualizada | O Resource Explorer adicionou suporte para visualizar outros tipos de recursos. A política `AWSResourceExplorerServiceRolePolicy` AWS gerenciada foi atualizada para conceder acesso ao Resource Explorer para visualizar tipos de recursos adicionais. | 12 de dezembro de 2023 |
| Novo filtro de pesquisa adicionado | O Explorador de Recursos agora é compatível com a pesquisa de recursos por aplicação. | 16 de novembro de 2023 |
| Adicionada compatibilidade com novos tipos de recursos | O Resource Explorer adicionou suporte para 86 novos recursos AWS CloudFormation, Serviços da AWS incluindo AWS Glue, e Amazon SageMaker. | 15 de novembro de 2023 |

| | | |
|---|---|---|
| O Explorador de Recursos é compatível com a pesquisa em várias contas | Agora você pode usar o Explorador de Recursos para pesquisar e descobrir recursos entre Contas da AWS na sua organização ou unidade organizacional. Para obter mais informações, consulte Ativar a pesquisa em várias contas. | 14 de novembro de 2023 |
| Políticas gerenciadas novas e atualizadas | O Explorador de Recursos passou a ser compatível com o AWS Organizations. As políticas gerenciadas pela AWS foram adicionadas e atualizadas para conceder ao Explorador de Recursos acesso à sua organização, estrutura organizacional, contas e administradores delegados. | 14 de novembro de 2023 |
| Adicionada compatibilidade com novos tipos de recursos | O Explorador de Recursos passou a ser compatível com o AWS Organizations. As políticas gerenciadas pela AWS foram atualizadas para conceder ao Explorador de Recursos acesso à sua organização, estrutura organizacional, contas e administradores delegados. | 14 de novembro de 2023 |

| | | |
|---|---|---|
| Adicionada compatibilidade com novos tipos de recursos | O Explorador de Recursos agora é compatível com 12 novos tipos de recursos dos serviços, incluindo o Amazon Cognito, o AWS Elastic Beanstalk e o Amazon Elastic File System. | 18 de outubro de 2023 |
| Adicionada compatibilidade com novos tipos de recursos | O Explorador de Recursos passou a ser compatível com 164 recursos. As políticas gerenciadas pela AWS que concedem ao Explorador de Recursos acesso aos recursos de índice foram atualizadas para incluir esses novos tipos de recursos. | 17 de outubro de 2023 |
| O Explorador de Recursos agora está disponível em determinadas regiões de adesão | Os clientes estão BAH cadastrados e agora CGK podem se cadastrar no Resource Explorer. | 5 de outubro de 2023 |

| | | |
|---|---|---|
| Adicionada compatibilidade com novos tipos de recursos | O Resource Explorer adicionou suporte para recursos dos seguintes Serviços da AWS: AWS CodeBuild, AWS CodePipeline, Amazon Cognito, Amazon Elastic Container Registry AWS Elastic Beanstalk, Amazon Elastic File System AWS IoT, e. AWS Step Functions As políticas gerenciadas pela AWS que concedem ao Explorador de Recursos acesso aos recursos de índice foram atualizadas para incluir esses novos tipos de recursos. | 1º de agosto de 2023 |
| O Resource Explorer agora suporta a exportação dos resultados da pesquisa para um CSV | Agora você pode exportar os resultados da sua pesquisa na página de pesquisa de recursos para um arquivo CSV formatado. | 4 de abril de 2023 |
| Use AWS Chatbot para pesquisar e descobrir seus AWS recursos | Agora você pode usar AWS Chatbot para pesquisar seus recursos usando perguntas de linguagem natural. Para obter mais informações, consulte Usar o AWS Chatbot para pesquisar recursos. | 30 de março de 2023 |

| | | |
|---|---|---|
| Adicionada compatibilidade com novos tipos de recursos | O Resource Explorer adicionou suporte para recursos dos seguintes Serviços da AWS: Amazon ElastiCache e Amazon Simple Queue Service (AmazonSQS). AWS Lambda As políticas gerenciadas pela AWS que concedem ao Explorador de Recursos acesso aos recursos de índice foram atualizadas para incluir esses novos tipos de recursos. | 7 de março de 2023 |
| IAMatualização de melhores práticas | Guia atualizado para se alinhar às IAM melhores práticas. Para obter mais informações, consulte Melhores práticas de segurança em IAM. | 6 de dezembro de 2022 |
| Novas políticas AWS gerenciadas | O Resource Explorer adiciona AWSResourceExplorerFullAccess AWSResourceExplorerReadOnlyAccess, e AWSResourceExplorerServiceRolePolicy gerencia políticas. | 7 de novembro de 2022 |
| Lançamento inicial | Versão inicial do Guia do usuário do Explorador de Recursos | 7 de novembro de 2022 |

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.