Manual do usuário

# AWS Resource Groups

# AWS Resource Groups: Manual do usuário

# Table of Contents

# O que são grupos de recursos?

Você pode usar grupos de recursos para organizar seus recursos da AWS. O AWS Resource Groups é o serviço que permite gerenciar e automatizar tarefas em um grande número de recursos de uma vez. Este guia mostra como criar e gerenciar grupos de recursos no AWS Resource Groups. As tarefas que você pode realizar em um recurso variam de acordo com o produto da AWS que você está usando. Para obter uma lista dos serviços que oferecem suporte ao AWS Resource Groups e uma breve descrição do que cada serviço permite que você faça com um grupo de recursos, consulte AWS serviços que funcionam com AWS Resource Groups.

Você pode acessar os Grupos de recursos usando qualquer um dos seguintes pontos de entrada.

- Na barra de navegação, no AWS Management Console, escolha Serviços. Em seguida, em Gerenciamento e governança, escolha Grupos de recursos e Tag Editor.

  Link direto: Console do AWS Resource Groups
- Usando a API dos Grupos de recursos, em comandos daAWS CLI ou em linguagens de programação do AWS SDK. Para obter mais informações, consulte a Referência da API AWS Resource Groups.

Para trabalhar com grupos de recursos na página inicial do AWS Management Console

1. Faça login no AWS Management Console.
2. Na barra de navegação, escolha Services (Serviços).
3. Em Gerenciamento e governança, escolha Grupos de recursos e Tag Editor.
4. No painel de navegação à esquerda, escolha Grupos de recursos salvos para trabalhar com um grupo existente ou Criar um grupo para criar um novo.

# O que são grupos de recursos?

Na AWS, um recurso é uma entidade com a qual você pode trabalhar. Os exemplos incluem uma instância do Amazon EC2, uma pilha do AWS CloudFormation ou um bucket do Amazon S3. Se você trabalhar com vários recursos, talvez seja útil gerenciá-los como um grupo, em vez de alternar de um serviço da AWS para outro a cada tarefa. Se você gerenciar grandes números de recursos relacionados, como instâncias do EC2 que compõem uma camada de aplicativo, provavelmente,

precisará executar ações em massa nesses recursos de uma vez. Os exemplos de ações em massa incluem:

- Aplicação de atualizações ou patches de segurança.
- Atualização de aplicativos.
- Abertura ou fechamento de portas para tráfego de rede.
- Coleta de dados específicos de monitoramento e de log em sua frota de instâncias.

Um grupo de recursos é um conjunto de recursos da AWS que estão na mesma Região da AWS e atendem aos critérios especificados na consulta do grupo. Em Grupos de recursos, há dois tipos de consultas que você pode usar para criar um grupo. Os dois tipos de consulta incluem recursos que são especificados no formato `AWS::service::resource`.

- Baseadas em tags

  Um grupo de recursos baseado em tags baseia sua associação em uma consulta que especifica uma lista de tipos de recursos e tags. Tags são chaves que ajudam a identificar e classificar os recursos em sua organização. Opcionalmente, as tags incluem valores para chaves.

  > **Important**
  >
  > Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. Usamos tags para fornecer serviços de cobrança e administração. As tags não devem ser usadas para dados privados ou confidenciais.

- Baseadas em pilha do AWS CloudFormation

  Um grupo de recursos baseado em pilhas do AWS CloudFormation baseia sua associação a uma consulta que especifica uma pilha do AWS CloudFormation em sua conta na região atual. Você também pode escolher os tipos de recurso na pilha que você deseja incluir no grupo. Sua consulta pode ser baseada em apenas uma pilha do AWS CloudFormation.

### Grupos de recursos vinculados a serviços

Alguns Serviços da AWS definem grupos de recursos que você só pode criar e gerenciar usando o console e as APIs desse serviço. O que você pode fazer com esses grupos está limitado no console

Grupos de recursos. Para obter mais informações, consulte Configurações de serviço para Grupos de recursos no Guia de referência da API do AWS Resource Groups.

Os grupos de recursos podem ser aninhados. Um grupo de recursos pode conter grupos de recursos existentes na mesma região.

## Casos de uso para grupos de recursos

Por padrão, o AWS Management Console é organizado por serviço da AWS. Mas com os Grupos de recursos, você pode criar um console personalizado que organiza e consolida informações com base em critérios especificados em tags ou nos recursos em uma pilha do AWS CloudFormation. A lista a seguir descreve alguns dos casos em que o agrupamento de recursos pode ajudar a organizar seus recursos.

- Um aplicativo que contém fases diferentes, como desenvolvimento, preparação e produção.
- Projetos gerenciados por vários departamentos ou indivíduos.
- Um conjunto de recursos da AWS que você usa em conjunto para um projeto comum ou que deseja gerenciar ou monitorar como um grupo.
- Um conjunto de recursos relacionados a aplicativos que são executados em uma plataforma específica, como Android ou iOS.

Por exemplo, digamos que você esteja desenvolvendo um aplicativo web e mantendo conjuntos separados de recursos para os estágios alfa, beta e de lançamento. Cada versão é executada no Amazon EC2 com um volume de armazenamento do Amazon Elastic Block Store. Use o Elastic Load Balancing para gerenciar o tráfego, e o Route 53 para gerenciar seu domínio. Sem os Grupos de recursos, você pode ter que acessar vários consoles apenas para verificar o status de seus serviços ou modificar as configurações de uma versão da sua aplicação.

Com os Grupos de recursos, você usa uma única página para visualizar e gerenciar seus recursos. Por exemplo, digamos que você use a ferramenta para criar um grupo de recursos para cada versão — alfa, beta e de lançamento — de sua aplicação. Para verificar seus recursos na versão alfa do aplicativo, abra o grupo de recursos. Depois, visualize as informações consolidadas em sua página do grupo de recursos. Para modificar um recurso específico, escolha os links do recurso na página do grupo de recursos para acessar o console do serviço com as configurações de que você precisa.

# AWS Resource Groups e permissões

As permissões do atributo Grupos de recursos estão no nível da conta. Desde que as entidades principais do IAM, como perfis e usuários, que estão compartilhando sua conta tiverem as permissões corretas do IAM, elas poderão trabalhar com os grupos de recursos que você criar.

As tags são as propriedades de um recurso, de modo que são compartilhadas por toda a sua conta. Os usuários em um departamento ou grupo especializado podem extrair de um vocabulário comum (tags) para criar grupos de recursos significativos para suas funções e responsabilidades. Ter um grupo comum de tags também significa que quando os usuários compartilham um grupo de recursos, eles não precisam se preocupar com a falta ou conflitos de informações de tags.

## Atributos AWS Resource Groups

Nos Grupos de recursos, o único recurso disponível é um grupo. Os grupos têm um nome de recurso da Amazon (ARN) exclusivo associado a eles. Para obter mais informações sobre ARNs, consulte Nomes de recurso da Amazon (ARN) e namespaces de serviço da AWS no Referência geral da Amazon Web Services.

| Tipo de recurso | Formato de nome do recurso da Amazon (ARN) |
|---|---|
| Grupo de recursos | `arn:aws:resource-groups:` *`region`*`:`*`account`*`:group/`*`group-name`* |

## Como funcionam as tags

As tags são pares de chave e valor que atuam como metadados para organizar seus recursos da AWS. Com a maioria dos recursos da AWS, você tem a opção de adicionar tags ao criar o recurso, seja uma instância do Amazon EC2, um bucket do Amazon S3 ou outros recursos. No entanto, você também pode adicionar tags a vários recursos com suporte de uma vez usando o Tag Editor. Você cria uma consulta de recursos de vários tipos e adiciona, remove ou substitui as tags dos recursos nos resultados da pesquisa. As consultas atribuem um operador AND às tags, de forma que qualquer recurso que corresponda aos tipos de recurso especificados e todas as tags especificadas seja retornado pela consulta.

> **Important**
>
> Não armazene informações de identificação pessoal (PII) nem outras informações confidenciais ou sigilosas em tags. Usamos tags para fornecer serviços de cobrança e administração. As tags não devem ser usadas para dados privados ou confidenciais.

Para obter mais informações sobre marcação, consulte o Guia de usuário do Tag Editor. Você pode marcar recursos com suporte usando o Tag Editor, e alguns recursos adicionais usando a funcionalidade de marcação no console de serviço onde você cria e gerencia o recurso.

# Conceitos básicos do AWS Resource Groups

Na AWS, um recurso é uma entidade com a qual você pode trabalhar. Os exemplos incluem uma instância do Amazon EC2, um bucket do Amazon S3 ou uma zona hospedada do Amazon Route 53. Se você trabalhar com vários recursos, talvez seja útil gerenciá-los como um grupo, em vez de alternar de um serviço da AWS para outro a cada tarefa.

Esta seção mostra como começar a usar o AWS Resource Groups. Primeiro, organize os recursos da AWS marcando-os no Tag Editor. Depois, crie consultas nos Grupos de recursos que incluam os tipos de recurso que você deseja incluir em um grupo, e as tags que você aplicou aos recursos.

Depois de criar grupos de recursos nos Grupos de Recursos, use as ferramentas do AWS Systems Manager como Automação para simplificar as tarefas de gerenciamento em seus Grupos de recursos.

Para obter mais informações sobre os conceitos básicos dos atributos e ferramentas do AWS Systems Manager, consulte o Guia do usuário do AWS Systems Manager.

Tópicos



## Pré-requisitos para trabalhar com AWS Resource Groups

Antes de começar a trabalhar com grupos de recursos, certifique-se de que você tem uma conta ativa da AWS com recursos existentes e direitos apropriados para marcar recursos e criar grupos.

## Inscreva-se para 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 https://portal.aws.amazon.com/billing/signup.
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.

## Criar recursos do

Você pode criar um grupo de recursos vazio, mas não pode executar qualquer tarefa nos membros do grupo de recursos enquanto não existirem recursos no grupo. Para obter mais informações sobre os tipos de recurso com suporte, consulte Tipos de recursos que você pode usar com AWS Resource Groups o Tag Editor.

## Configurar permissões

Para aproveitar ao máximo os Grupos de recursos e o Tag Editor, você talvez precise de permissões adicionais para marcar recursos ou para ver as chaves e valores de tag de um recurso. Essas permissões se encaixam nas seguintes categorias:

- Permissões para serviços individuais, para que você possa marcar recursos desses serviços e incluí-los em grupos de recursos.
- Permissões que são necessárias para usar o console do Tag Editor
- Permissões necessárias para usar o AWS Resource Groups console e a API.

Se você for administrador, poderá fornecer permissões para seus usuários criando políticas por meio do serviço AWS Identity and Access Management (IAM). Primeiro, você cria seus principais, como funções ou usuários do IAM, ou associa identidades externas ao seu AWS ambiente usando um

serviço como. AWS IAM Identity Center Em seguida, você aplica políticas com as permissões de que seus usuários precisam. Para obter informações sobre como criar e anexar políticas do IAM, consulte Como trabalhar com políticas.

Permissões para serviços individuais

> **Important**
>
> Esta seção descreve as permissões necessárias para marcar recursos em outros consoles e APIs de serviço e adicionar esses recursos a grupos de recursos.

Conforme descrito em O que são grupos de recursos?, cada grupo de recursos representa um conjunto de recursos de tipos especificados que compartilham uma ou mais chaves ou valores de tag. Para adicionar tags a um recurso, você precisa das permissões necessárias para o serviço ao qual o recurso pertence. Por exemplo, para marcar instâncias do Amazon EC2, você precisa ter permissões para as ações de marcação na API daquele serviço, como as listadas no Guia do usuário do Amazon EC2.

Para aproveitar as funções do recurso Grupos de recursos ao máximo, você precisa de outras permissões que permitam acessar um console do serviço e interagir com os recursos ali. Para obter exemplos dessas políticas para o Amazon EC2, consulte Exemplos de políticas para trabalhar no console do Amazon EC2 no Guia do usuário do Amazon EC2.

Permissões obrigatórias para Grupos de recursos e Tag Editor

Para usar os Grupos de recursos e o Tag Editor, as seguintes permissões devem ser adicionadas a uma declaração da política do usuário no IAM. Você pode adicionar políticas AWS gerenciadas que são mantidas e mantidas up-to-date por AWS, ou você pode criar e manter sua própria política personalizada.

Usando políticas AWS gerenciadas para permissões de Resource Groups e Tag Editor

AWS Resource Groups e o Tag Editor oferecem suporte às seguintes políticas AWS gerenciadas que você pode usar para fornecer um conjunto predefinido de permissões aos seus usuários. Você pode anexar essas políticas gerenciadas a qualquer usuário, perfil ou grupo da mesma forma que faria com qualquer outra política criada por você.

ResourceGroupsandTagEditorReadOnlyAccess

Essa política concede ao perfil do IAM ou ao usuário anexado permissão para chamar as operações somente de leitura para Grupos de recursos e Tag Editor. Para ler as tags de um recurso, você também deve ter permissões para esse recurso por meio de outra política (consulte a seguinte observação importante).

ResourceGroupsandTagEditorFullAccess

Essa política concede ao perfil do IAM ou ao usuário anexado permissão para chamar qualquer operação de Grupos de recursos e as operações de tag de leitura e gravação no Tag Editor. Para ler ou gravar as tags de um recurso, você também deve ter permissões para esse recurso por meio de outra política (consulte a seguinte observação importante).

**Important**

As duas políticas anteriores concedem permissão para chamar as operações dos Grupos de recursos e do Tag Editor e usar esses consoles. Para operações de Grupos de recursos, essas políticas são suficientes e concedem todas as permissões necessárias para trabalhar com qualquer recurso no console Grupos de recursos.
No entanto, para operações de marcação e o console do Tag Editor, as permissões são mais granulares. Você deve ter permissões não apenas para invocar a operação, mas também permissões apropriadas para o recurso específico cujas tags você está tentando acessar. Para conceder o acesso às tags, você também deve anexar uma das seguintes políticas:

- A política AWS gerenciada ReadOnlyAccessconcede permissões às operações somente de leitura dos recursos de cada serviço. AWS mantém essa política atualizada automaticamente com novos AWS serviços à medida que eles se tornam disponíveis.
- Muitos serviços fornecem políticas AWS gerenciadas somente para leitura específicas que você pode usar para limitar o acesso somente aos recursos fornecidos por esse serviço. Por exemplo, o Amazon EC2 fornece o AmazonEC2. ReadOnlyAccess
- Você pode criar sua própria política que conceda acesso somente às operações de somente leitura muito específicas para os poucos serviços e recursos que você deseja que seus usuários acessem. Essa política usa uma estratégia de “lista de permissões” ou uma estratégia de lista de negação.

Uma estratégia de lista de permissões aproveita o fato de que o acesso é negado por padrão até que você o permita explicitamente em uma política. Você pode usar uma política como neste exemplo:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [ "resource-groups:*" ],
            "Resource": "arn:aws:resource-groups:*:123456789012:group/*"
        }
    ]
}
```

Como alternativa, você pode usar uma estratégia de “lista de negação” que permite acesso a todos os recursos, exceto aqueles que você bloqueia explicitamente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
             "Action": [ "resource-groups:*" ],
            "Resource": "arn:aws:resource-groups:*:123456789012:group/*"
        }
    ]
}
```

Adicionar permissões de Grupos de recursos e Tag Editor manualmente

- `resource-groups:*` Esta permissão permite todas as ações dos Grupos de recursos. Se, em vez disso, quiser restringir as ações que estão disponíveis para um usuário, você pode substituir o asterisco por uma ação específica dos Grupos de recursos ou por uma lista de ações separada por vírgulas
- `cloudformation:DescribeStacks`
- `cloudformation:ListStackResources`

- `tag:GetResources`
- `tag:TagResources`
- `tag:UntagResources`
- `tag:getTagKeys`
- `tag:getTagValues`
- `resource-explorer:*`

> **Note**
>
> A `resource-groups:SearchResources` permissão permite que o Editor de tags liste recursos quando você filtra sua pesquisa usando chaves ou valores de tag.
> A `resource-explorer:ListResources` permissão permite que o Editor de tags liste recursos quando você pesquisa recursos sem definir tags de pesquisa.

Para usar os Grupos de recursos e o Tag Editor no console, você também precisa de permissão para executar a ação `resource-groups:ListGroupResources`. Essa permissão é necessária para listar os tipos de recursos disponíveis na região atual. Atualmente, não há suporte para o uso de condições de política com o `resource-groups:ListGroupResources`.

Conceder permissões para usar um AWS Resource Groups Editor de tags

Para adicionar uma política de uso AWS Resource Groups do Editor de tags a um usuário, faça o seguinte.

1. Abra o console do IAM.
2. No painel de navegação, escolha Users.
3. Encontre o usuário a quem você deseja conceder AWS Resource Groups e as permissões do Editor de tags. Escolha o nome do usuário para abrir a página de propriedades do usuário.
4. Escolha Add permissions (Adicionar permissões).
5. Escolha Anexar políticas existentes diretamente.
6. Escolha Criar política.
7. Na guia JSON, cole a seguinte declaração de política.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "resource-groups:*",
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-explorer:*"
      ],
      "Resource": "*"
    }
  ]
}
```

> **Note**
>
> Esta declaração de política de exemplo concede permissões somente para ações do AWS Resource Groups e do Tag Editor. Ele não permite o acesso às AWS Systems Manager tarefas no AWS Resource Groups console. Por exemplo, essa política não concede permissões para que você use os comandos de Automação do Systems Manager. Para executar tarefas do Systems Manager em grupos de recursos, você deve ter permissões do Systems Manager anexadas à sua política (como `ssm:*`). Para obter mais informações sobre como conceder acesso ao Systems Manager, consulte Configurar acesso ao Systems Manager no Guia do usuário do AWS Systems Manager .

8. Escolha Revisar política.
9. Dê um nome e uma descrição à nova política (por exemplo, `AWSResourceGroupsQueryAPIAccess`).
10. Escolha Criar política.
11. Agora que a política está salva no IAM, você pode vinculá-la a outros usuários. Para obter mais informações sobre como adicionar uma política a um usuário, consulte Adição de permissões anexando políticas diretamente ao usuário no Guia do usuário do IAM.

Saiba mais sobre AWS Resource Groups autorização e controle de acesso

Os Grupos de recursos oferecem suporte ao seguinte.

- Políticas baseadas em ação. Por exemplo, você pode criar uma política que permita que os usuários executem operações ListGroups, mas não outras.
- Permissões em nível de recurso. Os Grupos de recursos oferecem suporte ao uso de ARNs para especificar recursos individuais na política.
- Autorização baseada em tags. Os Grupos de recursos oferecem suporte ao uso de tags de recursos na condição de uma política. Por exemplo, você pode criar uma política que conceda aos usuários dos Grupos de recursos acesso total a um grupo marcado.
- Credenciais temporárias. Os usuários podem assumir uma função com uma política que permite AWS Resource Groups operações.

Os Grupos de recursos não oferecem suporte a políticas baseadas em recurso.

Os Grupos de recursos não usam perfis vinculados a serviços.

Para obter mais informações sobre como o Resource Groups e o Tag Editor se integram ao AWS Identity and Access Management (IAM), consulte os tópicos a seguir no Guia AWS Identity and Access Management do usuário.

- AWS serviços que funcionam com o IAM
- Ações, recursos e chaves de condição para AWS Resource Groups
- Controle de acesso usando políticas

# Criação de grupos baseados em consultas no AWS Resource Groups

Tópicos

- Tipos de consultas de grupos de recursos
- Criar uma consulta baseada em tag e criar um grupo
- Criar um grupo baseado em pilha do AWS CloudFormation

# Tipos de consultas de grupos de recursos

No AWS Resource Groups, uma consulta é a base de um grupo baseado em consultas. Você pode basear um grupo de recursos em um de dois tipos de consulta.

Baseadas em tags

As consultas baseadas em tags incluem listas de tipos de recursos que são especificados no seguinte formato `AWS::service::resource` e tags. As tags são chaves que ajudam a identificar e classificar seus recursos em sua organização. Opcionalmente, as tags incluem valores para chaves.

Para uma consulta baseada em tags, você também especifica as tags que são compartilhadas pelos recursos que deseja que sejam membros do grupo. Por exemplo, para criar um grupo de recursos que tenha todas as instâncias do Amazon EC2 e buckets do Amazon S3 que você está usando para executar o estágio de teste de uma aplicação, e você tem instâncias e buckets que estão marcados dessa forma, escolha os tipos de recurso `AWS::EC2::Instance` e `AWS::S3::Bucket` na lista suspensa e especifique a chave de tag **`Stage`** com um valor de **`Test`**.

A sintaxe do parâmetro `ResourceQuery` de um grupo de recursos baseado em tags contém os seguintes elementos:

- `Type`

  Este elemento indica qual tipo de consulta define este grupo de recursos. Para criar um grupo de recursos baseado em tags, especifique o valor `TAG_FILTERS_1_0` da seguinte maneira:

  ```
  "Type": "TAG_FILTERS_1_0"
  ```

- `Query`

  Este elemento define a consulta real usada para comparar com os recursos. Ele deve conter uma representação de cadeia de caracteres de uma estrutura JSON com os seguintes elementos:

  - `ResourceTypeFilters`

    Este elemento limita os resultados para apenas aqueles tipos de recursos que correspondem ao filtro. Especifique os seguintes valores:

- `"AWS::AllSupported"` — para especificar que os resultados podem incluir recursos de qualquer tipo que correspondam à consulta e que sejam atualmente suportados pelo serviço Grupos de recursos.
- `"AWS::`*`service-id`*`::`*`resource-type`* — uma lista separada por vírgulas de cadeias de caracteres de especificação de tipo de recurso com este formato, como `"AWS::EC2::Instance"`.

- `TagFilters`

  Este elemento especifica pares de cadeias de caracteres de chave/valor que são comparados às tags anexadas aos seus recursos. Aqueles com uma chave de tag e um valor que correspondem ao filtro são incluídos no grupo. Cada filtro consiste nos seguintes elementos:

  - `"Key"` — uma cadeia de caracteres com um nome de chave. Somente os recursos com tags que contenham um nome de chave correspondente podem corresponder ao filtro e serem membros do grupo.
  - `"Values"` — uma cadeia de caracteres com uma lista de valores separados por vírgula para a chave especificada. Somente recursos com uma chave de tag correspondente e um valor que corresponda a outro valor nesta lista são membros do grupo.

Todos esses elementos JSON devem ser combinados em uma representação de cadeia de caracteres de linha única da estrutura JSON. Por exemplo, considere uma `Query` com o exemplo de estrutura JSON a seguir. Esta consulta deve corresponder somente às instâncias do Amazon EC2 que têm a tag “Stage” com o valor “Test”.

```
{
    "ResourceTypeFilters": [ "AWS::EC2::Instance" ],
    "TagFilters": [
        {
            "Key": "Stage",
            "Values": [ "Test" ]
        }
    ]
}
```

Este JSON pode ser representado como a seguinte cadeia de caracteres de linha única e usado como o valor do elemento `Query`. Como o valor de uma estrutura JSON deve ser uma cadeia de caracteres entre aspas duplas, você deve escapar quaisquer caracteres de aspas duplas

ou caracteres de barra invertida incorporados precedendo cada um com uma barra invertida, conforme mostrado aqui:

```
"Query":"{\"ResourceTypeFilters\":[\"AWS::AllSupported\"],\"TagFilters\":[{\"Key\":
\"Stage\",\"Values\":[\"Test\"]}]}"
```

A cadeia de caracteres `ResourceQuery` completa é então representada conforme mostrado aqui, como um parâmetro de comando da CLI:

```
--resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters\":
[\"AWS::AllSupported\"],\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":[\"Test
\"]}]}"}'
```

### AWS CloudFormation baseado em pilhas

Em uma consulta baseada em pilha do AWS CloudFormation, você escolhe uma pilha do AWS CloudFormation em sua conta na região atual e escolhe os tipos de recurso na pilha que você deseja incluir no grupo. Sua consulta pode ser baseada em apenas uma pilha do AWS CloudFormation.

> **Note**
>
> Uma pilha do AWS CloudFormation pode conter outras pilhas “secundárias” do AWS CloudFormation. No entanto, um grupo de recursos baseado em uma pilha “principal” não obtém todos os recursos das pilhas secundárias como membros do grupo. Os grupos de recursos adicionam as pilhas secundárias ao grupo de recursos da pilha principal como membros individuais do grupo e não as expandem.

Os Grupos de recursos oferecem suporte a consultas baseadas em pilhas do AWS CloudFormation que têm um dos seguintes status.

- `CREATE_COMPLETE`
- `CREATE_IN_PROGRESS`
- `DELETE_FAILED`
- `DELETE_IN_PROGRESS`
- `REVIEW_IN_PROGRESS`

> **Important**
>
> Somente os recursos criados diretamente como parte da pilha na consulta são incluídos no grupo de recursos. Recursos criados posteriormente por membros da pilha do AWS CloudFormation não se tornam membros do grupo. Por exemplo, se um grupo de ajuste de escala automático for criado como parte da pilha do AWS CloudFormation, esse grupo de ajuste de escala automático será membro do grupo. No entanto, uma instância do Amazon EC2 criada por esse grupo de ajuste de escala automático como parte de sua operação não. é membro do grupo de recursos baseado em pilha do AWS CloudFormation.

Se você criar um grupo baseado em uma pilha do AWS CloudFormation, e a pilha for alterada para um status que não for mais compatível como uma base para uma consulta de grupo, como `DELETE_COMPLETE`, o grupo de recursos ainda existirá, mas ele não terá recursos de membro.

Depois de criar um grupo de recursos, você pode usar executar tarefas nos recursos do grupo.

A sintaxe do parâmetro `ResourceQuery` de um grupo de recursos baseado em pilhas do CloudFormation contém os seguintes elementos:

- `Type`

  Este elemento indica qual tipo de consulta define este grupo de recursos.

  Para criar um grupo de recursos baseado em pilhas do AWS CloudFormation, especifique o valor `CLOUDFORMATION_STACK_1_0`, da seguinte forma:

  ```
  "Type": "CLOUDFORMATION_STACK_1_0"
  ```

- `Query`

  Este elemento define a consulta real usada para comparar com os recursos. Ele deve conter uma representação de cadeia de caracteres de uma estrutura JSON com os seguintes elementos:

  - `ResourceTypeFilters`

    Este elemento limita os resultados para apenas aqueles tipos de recursos que correspondem ao filtro. Especifique os seguintes valores:

- `"AWS::AllSupported"` — Para especificar que os resultados podem incluir recursos de qualquer tipo que correspondam à consulta.
- `"AWS::`*`service-id`*`::`*`resource-type`* — Uma lista separada por vírgulas de cadeias de caracteres de especificação de tipo de recurso com este formato, como `"AWS::EC2::Instance"`.

- `StackIdentifier`

  Este elemento especifica o nome do recurso da Amazon (ARN) da pilha do AWS CloudFormation cujos recursos você deseja incluir no grupo.

Todos esses elementos JSON devem ser combinados em uma representação de cadeia de caracteres de linha única da estrutura JSON. Por exemplo, considere uma `Query` com o exemplo de estrutura JSON a seguir. Esta consulta deve corresponder somente aos buckets do Amazon S3 que fazem parte da pilha do AWS CloudFormation especificada.

```
{
    "ResourceTypeFilters": [ "AWS::S3::Bucket" ],
    "StackIdentifier": "arn:aws:cloudformation:us-
west-2:123456789012:stack/MyCloudFormationStackName/fb0d5000-aba8-00e8-
aa9e-50d5cEXAMPLE"
}
```

Este JSON pode ser representado como a seguinte cadeia de caracteres de linha única e usado como o valor do elemento `Query`. Como o valor de uma estrutura JSON deve ser uma cadeia de caracteres entre aspas duplas, você deve escapar quaisquer caracteres de aspas duplas ou caracteres de barra invertida incorporados precedendo cada um com uma barra invertida, conforme mostrado aqui:

```
"Query":"{\"ResourceTypeFilters\":[\"AWS::S3::Bucket\"],\"StackIdentifier\":
\"arn:aws:cloudformation:us-west-2:123456789012:stack\/MyCloudFormationStackName\/
fb0d5000-aba8-00e8-aa9e-50d5cEXAMPLE\"
```

A cadeia de caracteres `ResourceQuery` completa é então representada conforme mostrado aqui, como um parâmetro de comando da CLI:

```
--resource-query '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::S3::Bucket\"],\"StackIdentifier\":\"arn:aws:cloudformation:us-
```

```
west-2:123456789012:stack\/MyCloudFormationStackName\/fb0d5000-aba8-00e8-
aa9e-50d5cEXAMPLE\"}'
```

## Criar uma consulta baseada em tag e criar um grupo

Os procedimentos a seguir mostram como criar uma consulta baseada em tag e usar isso para criar um grupo de recursos.

Console

1. Faça login no console do AWS Resource Groups.
2. No painel de navegação, selecione Criar grupo de recursos.
3. Na página Criar grupo baseado em consulta, em Tipo de grupo, escolha o tipo de grupo Baseado em tags.
4. Em Critérios de agrupamento, escolha os tipos de recurso que você deseja incluir no grupo de recursos. Você pode ter no máximo 20 tipos de recurso em uma consulta. Para esta demonstração, escolha AWS::EC2::Instance e AWS::S3::Bucket.
5. Ainda em Critérios de agrupamento, para Tags, especifique uma chave de tag, ou um par de chave e valor de tag, a fim de limitar os recursos correspondentes para incluir somente aqueles que estão marcados com seus valores especificados. Escolha Add (Adicionar) ou pressione Enter quando tiver concluído a tag. Neste exemplo, filtramos os recursos que têm uma chave de tag Stage (Estágio). O valor da tag é opcional, mas restringe ainda mais os resultados da consulta. Você pode adicionar vários valores para uma chave de tag adicionando um operador `OR` entre os valores de tag. Para adicionar mais tags, escolha Add (Adicionar). As consultas atribuem um operador `AND` às tags, de forma que qualquer recurso que corresponda aos tipos de recurso especificados e todas as tags especificadas seja retornado pela consulta.
6. Ainda em Critérios de agrupamento, escolha Visualizar recursos do grupo para retornar a lista de instâncias do EC2 e buckets do S3 na sua conta que correspondam às chaves de tag especificadas.
7. Depois de obter os resultados desejados, crie um grupo com base nessa consulta.

    a. Na página Detalhes do grupo, digite um nome para seu grupo de recursos em Nome do grupo.

    Um nome de grupo de recursos pode ter no máximo 128 caracteres, incluindo letras, números, pontos, hifens e sublinhados. O nome não pode iniciar com `AWS` ou `aws`.

Esses são reservados. Um nome de grupo de recursos deve ser exclusivo na região atual em sua conta.

b. (Opcional) Em Group description (Descrição do grupo), digite uma descrição para o grupo.

c. (Opcional) Na área Group tags (Tags do grupo), adicione pares de chave e valor de tags que se aplicam somente ao grupo de recursos, e não a recursos de membro no grupo.

   As tags de grupo são úteis se você desejar que esse grupo faça parte de um grupo maior. Como é necessário especificar pelo menos uma chave de tag para criar um grupo, certifique-se de adicionar pelo menos uma chave de tag em Group tags (Tags do grupo) nos grupos que você pretende aninhar em grupos maiores.

8. Ao concluir, escolha Criar grupo.

AWS CLI & AWS SDKs

Um grupo baseado em tag é baseado em uma consulta do tipo `TAG_FILTERS_1_0`.

1. Em uma sessão da AWS CLI, digite o seguinte e pressione Enter, substituindo os valores de nome do grupo, descrição, tipos de recurso, chaves de tags e valores de tags por seus próprios. As descrições podem ter um máximo de 512 caracteres, incluindo letras, números, sublinhados, hifens, pontuação e espaços. Você pode ter no máximo 20 tipos de recurso em uma consulta. Um nome de grupo de recursos pode ter no máximo 128 caracteres, incluindo letras, números, pontos, hifens e sublinhados. O nome não pode iniciar com `AWS` ou `aws`. Esses são reservados. Um nome de grupo de recursos deve ser exclusivo em sua conta.

   Pelo menos um valor para `ResourceTypeFilters` é necessário. Para especificar todos os tipos de recurso, use `AWS::AllSupported` como o valor de `ResourceTypeFilters`.

```
$ aws resource-groups create-group \
    --name resource-group-name \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"resource_type1\",\"resource_type2\"],\"TagFilters\":[{\"Key\":\"Key1\",
\"Values\":[\"Value1\",\"Value2\"]},{\"Key\":\"Key2\",\"Values\":[\"Value1\",
\"Value2\"]}]}"}'
```

   O comando a seguir é um exemplo.

```
$ aws resource-groups create-group \
```

```
    --name my-resource-group \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::EC2::Instance\"],\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":
[\"Test\"]}]}"}'
```

O comando a seguir é um exemplo que inclui todos os tipos de recurso compatíveis.

```
$ aws resource-groups create-group \
    --name my-resource-group \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::AllSupported\"],\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":[\"Test
\"]}]}"}'
```

2. Veja a seguir o que é retornado na resposta ao comando.

   - Uma descrição completa do grupo que você criou.
   - A consulta de recursos que você usou para criar o grupo.
   - As tags associadas ao grupo.

## Criar um grupo baseado em pilha do AWS CloudFormation

Os procedimentos a seguir mostram como criar uma consulta baseada em pilha e usar isso para criar um grupo de recursos.

Console

1. Faça login no console do AWS Resource Groups.
2. No painel de navegação, selecione Criar grupo de recursos.
3. Em Criar grupo baseado em consulta, em Tipo de grupo, escolha o tipo de grupo Baseado em pilha do CloudFormation.
4. Escolha a pilha que você deseja usar como a base do grupo. Um grupo de recursos pode ser baseado em apenas uma pilha. Para filtrar a lista de pilhas, comece digitando o nome da pilha. Somente pilhas com status compatíveis são exibidas na lista.
5. Escolha os tipos de recurso na pilha que você deseja incluir no grupo. Para esta demonstração, mantenha o padrão, All supported resource types (Todos os tipos de recurso compatíveis). Para obter mais informações sobre quais tipos de recurso são compatíveis e podem estar no grupo, consulte Tipos de recursos que você pode usar com AWS Resource Groups o Tag Editor.

6. Escolha View group resources (Visualizar recursos do grupo) para retornar à lista de recursos na pilha do AWS CloudFormation que correspondem aos tipos de recurso selecionados.
7. Depois de obter os resultados desejados, crie um grupo com base nessa consulta.

   a. Na página Detalhes do grupo, digite um nome para seu grupo de recursos em Nome do grupo.

      Um nome de grupo de recursos pode ter no máximo 128 caracteres, incluindo letras, números, pontos, hifens e sublinhados. O nome não pode iniciar com `AWS` ou `aws`. Esses são reservados. Um nome de grupo de recursos deve ser exclusivo na região atual em sua conta.

   b. (Opcional) Em Group description (Descrição do grupo), digite uma descrição para o grupo.

   c. (Opcional) Na área Group tags (Tags do grupo), adicione pares de chave e valor de tags que se aplicam somente ao grupo de recursos, e não a recursos de membro no grupo.

      As tags de grupo são úteis se você desejar que esse grupo faça parte de um grupo maior. Como é necessário especificar pelo menos uma chave de tag para criar um grupo, certifique-se de adicionar pelo menos uma chave de tag em Group tags (Tags do grupo) nos grupos que você pretende aninhar em grupos maiores.
8. Ao concluir, escolha Criar grupo.

### AWS CLI & AWS SDKs

Um grupo baseado em pilha do AWS CloudFormation é baseado em uma consulta do tipo `CLOUDFORMATION_STACK_1_0`.

1. Execute o comando a seguir, substituindo os valores pelo nome do grupo e descrição, identificador de pilha e tipos de recurso de sua escolha. As descrições podem ter um máximo de 512 caracteres, incluindo letras, números, sublinhados, hifens, pontuação e espaços.

   Se você não especificar tipos de recurso, os Grupos de recursos incluirão todos os tipos de recurso compatíveis na pilha. Você pode ter no máximo 20 tipos de recurso em uma consulta. Um nome de grupo de recursos pode ter no máximo 128 caracteres, incluindo letras, números, pontos, hifens e sublinhados. O nome não pode iniciar com `AWS` ou `aws`. Esses são reservados. Um nome de grupo de recursos deve ser exclusivo em sua conta.

O *stack_identifier* é o ARN da pilha, conforme mostrado no comando de exemplo.

```
$ aws resource-groups create-group \
    --name group_name \
    --description "description" \
    --resource-query
 '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
\"stack_identifier\",\"ResourceTypeFilters\":[\"resource_type1\",
\"resource_type2\"]}"}'
```

O comando a seguir é um exemplo.

```
$ aws resource-groups create-group \
    --name My-CFN-stack-group \
    --description "My first CloudFormation stack-based group" \
    --resource-query
 '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
\"arn:aws:cloudformation:us-west-2:123456789012:stack\/AWStestuseraccount\/
fb0d5000-aba8-00e8-aa9e-50d5cEXAMPLE\",\"ResourceTypeFilters\":
[\"AWS::EC2::Instance\",\"AWS::S3::Bucket\"]}"}'
```

2. Veja a seguir o que é retornado na resposta ao comando.

   - Uma descrição completa do grupo que você criou.
   - A consulta de recursos que você usou para criar o grupo.

# Atualizar grupos no AWS Resource Groups

Para atualizar um grupo de recursos baseado em tags nos Grupos de recursos, você pode editar a consulta e as tags que são a base do grupo. Você pode adicionar e remover recursos do grupo somente aplicando alterações na consulta ou nas tags. Você não pode selecionar recursos específicos para adicionar ou remover do grupo. A melhor maneira de adicionar ou remover um recurso específico de um grupo é editar as tags do recurso. Em seguida, verifique se sua consulta de tag de grupo de recursos inclui ou omite a tag, dependendo se você quer o recurso em seu grupo.

Para atualizar um grupo de recursos baseado em pilhas do AWS CloudFormation, você pode escolher uma pilha diferente. Você também pode adicionar ou remover tipos de recursos da pilha que deseja que façam parte do grupo. Para alterar os recursos que estão disponíveis na pilha, atualize o modelo do AWS CloudFormation usado para criar a pilha e atualize a pilha no

AWS CloudFormation. Para obter mais informações sobre como atualizar uma pilha do AWS CloudFormation, consulte Atualizações de pilhas do AWS CloudFormation no Guia do usuário do AWS CloudFormation.

Na AWS CLI, você pode atualizar grupos em dois comandos.

- `update-group`, executado para atualizar uma descrição do grupo.
- `update-group-query`, executado para atualizar a consulta e as tags do recurso que determinam os recursos de membro do grupo.

No console, você não pode alterar um grupo baseado em pilha do AWS CloudFormation para um grupo baseado em consultas ou vice-versa. No entanto, você pode fazer isso usando a API dos Grupos de recursos, incluindo na AWS CLI.

## Atualizar grupos de consultas baseados em tags

Console

Atualize um grupo baseado em tags alterando os tipos de recurso ou tags na consulta em que o grupo é baseado. Você também pode adicionar ou alterar a descrição do grupo.

1. Faça login no console do AWS Resource Groups.
2. No painel de navegação, em Grupos de recursos salvos, escolha um grupo e escolha Editar.

> **Note**
>
> Você pode atualizar apenas grupos de recursos de sua propriedade. A coluna Proprietário mostra a propriedade da conta para cada grupo de recursos. Todos os grupos com um proprietário de conta diferente daquele em que você está conectado foram criados no AWS License Manager. Para obter mais informações, consulte Grupos de recursos de host no AWS License Manager no Guia do usuário do License Manager.

3. Na página Editar grupo, em Critérios de agrupamento, adicione ou remova tipos de recurso. Você pode ter no máximo 20 tipos de recurso em uma consulta. Para remover um tipo de recurso, escolha X no rótulo do tipo de recurso. Escolha View group resources (Visualizar recursos do grupo) para ver como as alterações afetam os membros de recursos do grupo. Nesta demonstração, adicionamos o tipo de recurso AWS::RDS::DBInstance à consulta.

4. Ainda em Critérios de agrupamento, edite as tags conforme necessário. Neste exemplo, filtramos recursos que têm uma chave de tag de Stage (Estágio) e adicionamos um valor de tag de Test (Teste). O valor da tag é opcional, mas restringe ainda mais os resultados da consulta. Para remover uma tag, escolha X no rótulo da tag.
5. Na área Additional information (Informações adicionais), você pode editar a descrição do grupo. Você não pode editar o nome de um grupo depois que o grupo foi criado.
6. (Opcional) Em Tags de grupo, você pode adicionar ou remover tags. As tags de grupos são metadados sobre seu grupo de recursos. Elas não afetam os recursos de membro. Para alterar os recursos que são retornados pela consulta do grupo de recursos, edite as tags em Critérios de agrupamento.

   As tags de grupo são úteis se você desejar que esse grupo faça parte de um grupo maior. É necessário especificar pelo menos uma chave de tag para criar um grupo. Portanto, adicione pelo menos uma chave de tag em Tags de grupo aos grupos que você planeja aninhar em grupos maiores.
7. Escolha Visualizar resultados da consulta para retornar a lista atualizada de instâncias do EC2, buckets do S3 e instâncias de banco de dados do Amazon RDS em sua conta que correspondem às chaves de tag especificadas. Se você não vir os recursos que esperava na lista, certifique-se de que os recursos estejam marcados com as tags que você especificou na área Grouping criteria (Critérios de agrupamento).
8. Ao concluir, escolha Save changes (Salvar alterações).

### AWS CLI & AWS SDKs

Na AWS CLI, você atualiza uma consulta do grupo e atualiza uma descrição do grupo de recursos usando dois comandos diferentes. Não é possível editar o nome de um grupo existente. Na AWS CLI, você pode alterar um grupo baseado em tags para um grupo baseado em pilha do CloudFormation ou vice-versa.

1. Se não desejar alterar a descrição do grupo, ignore esta etapa e vá para a próxima. Em uma sessão da AWS CLI, digite o seguinte e pressione Enter, substituindo os valores de nome e descrição do grupo por seus próprios.

```
$ aws resource-groups update-group \
    --group-name resource-group-name \
    --description "description_text"
```

O comando a seguir é um exemplo.

```
$ aws resource-groups update-group \
    --group-name my-resource-group \
    --description "EC2 instances, S3 buckets, and RDS DBs that we are using for
 the test stage."
```

O comando retorna uma descrição completa e atualizada do grupo.

2. Para atualizar a consulta e as tags de um grupo, digite o comando a seguir. Substitua os valores de nome do grupo, tipos de recursos, chaves de tag e valores de tag por valores de sua escolha. Em seguida, pressione Enter. Você pode ter no máximo 20 tipos de recurso em uma consulta.

```
$ aws resource-groups update-group-query \
    --group-name resource-group-name \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"resource_type1\",\"resource_type2\"],\"TagFilters\":[{\"Key\":\"Key1\",
\"Values\":[\"Value1\",\"Value2\"]},{\"Key\":\"Key2\",\"Values\":[\"Value1\",
\"Value2\"]}]}"}'
```

O comando a seguir é um exemplo.

```
$ aws resource-groups update-group-query \
    --group-name my-resource-group \
    --resource-query '{"Type":"TAG_FILTERS_1_0","Query":"{\"ResourceTypeFilters
\":[\"AWS::EC2::Instance\",\"AWS::S3::Bucket\",\"AWS::RDS::DBInstance\"],
\"TagFilters\":[{\"Key\":\"Stage\",\"Values\":[\"Test\"]}]}"}'
```

O comando retorna a consulta atualizada como resultado.

## Atualizar um grupo baseado em pilha do AWS CloudFormation

Console

Você não pode alterar um grupo baseado em pilha do AWS CloudFormation para um grupo baseado em tags no AWS Management Console. No entanto, você pode alterar a pilha na qual o grupo é baseado, ou alterar tipos de recurso da pilha que você deseja incluir no grupo. Você também pode adicionar ou alterar a descrição do grupo.

1. Faça login no console do AWS Resource Groups.
2. No painel de navegação, em Grupos de recursos salvos, escolha o nome do grupo e escolha Editar.
3. 
> **Note**
>
> Você pode atualizar apenas Grupos de recursos de sua propriedade. A coluna Proprietário mostra a propriedade da conta para cada grupo de recursos. Todos os grupos com um proprietário de conta diferente daquele em que você está conectado foram criados no AWS License Manager. Para obter mais informações, consulte Grupos de recursos de host no AWS License Manager no Guia do usuário do License Manager.

4. Na página Editar grupo, em Critérios de agrupamento, para alterar a pilha em que o grupo é baseado, escolha a pilha na lista suspensa. Um grupo de recursos pode ser baseado em apenas uma pilha. Para filtrar a lista de pilhas, comece digitando o nome da pilha. Somente pilhas com status compatíveis são exibidas na lista. Para obter uma lista de status compatíveis, consulte Criação de grupos baseados em consultas no AWS Resource Groups neste guia.
5. Adicione ou remova tipos de recurso. Somente tipos de recurso que estão disponíveis na pilha são mostrados na lista suspensa. O padrão é All supported resource types (Todos os tipos de recurso compatíveis). Você pode ter no máximo 20 tipos de recurso em uma consulta. Para remover um tipo de recurso, escolha X no rótulo do tipo de recurso. Para obter mais informações sobre quais tipos de recurso são compatíveis e podem estar no grupo, consulte Tipos de recursos que você pode usar com AWS Resource Groups o Tag Editor.
6. Escolha Visualizar recursos do grupo para retornar à lista de recursos na pilha do AWS CloudFormation que correspondem aos tipos de recurso selecionados.
7. Na área Additional information (Informações adicionais), você pode editar a descrição do grupo. Você não pode editar o nome de um grupo depois que o grupo foi criado.
8. Em Group tags (Tags do grupo), adicione ou remova tags. As tags de grupos são metadados sobre seu grupo de recursos. Elas não afetam os recursos de membro. Para alterar os recursos que são retornados pela consulta do grupo de recursos, edite as tags na área Grouping criteria (Critérios de agrupamento).

   As tags de grupo são úteis se você desejar que esse grupo faça parte de um grupo maior. É necessário especificar pelo menos uma chave de tag para criar um grupo. Portanto, adicione

pelo menos uma chave de tag em Tags de grupo aos grupos que você planeja aninhar em grupos maiores.

9. Ao concluir, escolha Save changes (Salvar alterações).

### AWS CLI & AWS SDKs

Na AWS CLI, você atualiza uma consulta do grupo e atualiza uma descrição do grupo de recursos usando dois comandos diferentes. Não é possível editar o nome de um grupo existente. Na AWS CLI, você pode alterar um grupo baseado em tags para um grupo baseado em pilha do CloudFormation ou vice-versa.

1. Se não desejar alterar a descrição do grupo, ignore esta etapa e vá para a próxima. Execute o comando a seguir, substituindo os valores pelo nome do grupo e descrição de sua escolha.

```
$ aws resource-groups update-group \
    --group-name "resource-group-name" \
    --description "description_text"
```

O comando a seguir é um exemplo.

```
$ aws resource-groups update-group \
    --group-name "My-CFN-stack-group" \
    --description "EC2 instances, S3 buckets, and RDS DBs that we are using for
 the test stage."
```

O comando retorna uma descrição completa e atualizada do grupo.

2. Para atualizar a consulta e as tags de um grupo, execute o seguinte comando. Substitua os valores do nome do grupo, identificador da pilha e tipos de recursos de sua escolha. Para adicionar tipos de recurso, forneça a lista completa dos tipos de recurso no comando, não apenas os tipos de recurso que você está adicionando. Você pode ter no máximo 20 tipos de recurso em uma consulta.

O *stack_identifier* é o ARN da pilha, conforme mostrado no comando de exemplo.

```
$ aws resource-groups update-group-query \
    --group-name resource-group-name \
    --description "description" \
    --resource-query
 '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
```

```
\"stack_identifier\",\"ResourceTypeFilters\":[\"resource_type1\",
\"resource_type2\"]}"}'
```

O comando a seguir é um exemplo.

```
$ aws resource-groups update-group-query \
    --group-name "my-resource-group" \
    --description "Updated CloudFormation stack-based group" \
    --resource-query
 '{"Type":"CLOUDFORMATION_STACK_1_0","Query":"{\"StackIdentifier\":
\"arn:aws:cloudformation:us-west-2:810000000000:stack\/AWStestuseraccount
\/fb0d5000-aba8-00e8-aa9e-50d5cEXAMPLE\",\"ResourceTypeFilters\":
[\"AWS::EC2::Instance\",\"AWS::S3::Bucket\"]}"}'
```

O comando retorna a consulta atualizada como resultado.

# Eventos do ciclo de vida do grupo: monitorar Grupos de recursos em busca de mudanças

Depois de usar o AWS Resource Groups para organizar seus recursos em grupos, você pode monitorar esses grupos em busca de alterações que são expostas a você como eventos. Você pode receber uma notificação sobre um evento de grupo como um sinal para realizar algum tipo de ação. Por exemplo, você pode configurar uma notificação que é enviada sempre que a associação de um grupo muda. Você pode usar um evento da adição de um novo membro do grupo para acionar uma função do Lambda que analisa programaticamente a alteração para garantir que os novos membros do grupo atendam aos requisitos de conformidade definidos pela sua organização. Essa função do Lambda pode realizar a remediação automática para qualquer novo membro do grupo que não atenda a esses requisitos. Um evento causado pela remoção de um membro do grupo pode acionar uma função do Lambda que executa qualquer limpeza necessária, como excluir recursos vinculados.

Ao ativar eventos de ciclo de vida de grupos para seus grupos de recursos, você permite que eventos sobre alterações em seus grupos sejam capturados pelo Amazon EventBridge e disponibilizados para todos os vários serviços de destino compatíveis com o EventBridge. Em seguida, você pode configurar esses serviços de destino para realizar automaticamente quaisquer ações que seu cenário exija. Esses destinos incluem uma variedade de produtos da AWS, como o Amazon Simple Notification Service (Amazon SNS), o Amazon Simple Queue Service (Amazon SQS) e o AWS Lambda. Com serviços como o Lambda, seus eventos podem acionar respostas

programáticas que usam código para realizar as ações necessárias. Para obter uma lista dos produtos da AWS que você pode segmentar com o EventBridge, consulte os Destinos do Amazon EventBridge no Guia do usuário do Amazon EventBridge.

Quando você ativa os eventos do ciclo de vida do grupo, o AWS Resource Groups cria os seguintes itens:

- Uma perfil vinculado ao serviço (IAM) do AWS Identity and Access Management que tem permissão para monitorar seus recursos em busca de quaisquer alterações em suas tags e suas pilhas do AWS CloudFormation em busca de quaisquer alterações nos recursos que fazem parte de uma pilha.
- Uma regra do EventBridge gerenciada pelos Grupos de recursos que captura os detalhes de qualquer alteração de tag ou pilha em seus recursos. O EventBridge usa essa regra para notificar os Grupos de recursos sobre essas mudanças. Em seguida, os Grupos de recursos gerem eventos de associação para enviar ao EventBridge para que suas regras personalizadas sejam processadas.

O perfil vinculado ao serviço pode ser presumido somente pelo serviço Grupos de recursos. Para obter mais informações sobre o perfil vinculado ao serviço usado pelos Grupos de recursos para esse atributo, consulte Usar perfis vinculados a serviços para Grupos de recursos.

Quando este atributo é ativado, os Grupos de recursos geram um evento quando você faz qualquer uma das seguintes alterações em um grupo de recursos:

- Criar um grupo de recursos.
- Atualizar a consulta que define a associação ao grupo de recursos baseado em consultas.
- Atualizar a configuração de um grupo de recursos vinculado ao serviço.
- Atualizar a descrição de um grupo de recursos.
- Excluir um grupo de recursos.
- Alterar a associação de um grupo de recursos adicionando ou removendo um recurso do grupo. Uma mudança de associação também pode acontecer quando as tags mudam ou quando uma pilha do AWS CloudFormation é alterada.

**Important**

- Para receber e responder com sucesso aos eventos do grupo, você deve fazer alterações nos Grupos de recursos e no EventBridge. Você pode realizar as alterações em qualquer ordem, mas nenhum evento de grupo é publicado nos destinos do EventBridge até que você faça alterações nos dois serviços.

- As alterações do grupo de recursos não incluem alterações em nenhuma tag anexada ao próprio grupo de recursos. Para gerar eventos com base nas alterações de tag em seus grupos, você deve usar uma regra do EventBridge que use a fonte do `aws.tag`, em vez da fonte do `aws.resource-groups`. Para obter mais informações, consulte Marcar eventos de alterações em Recursos do AWS no Guia do usuário do Amazon EventBridge.

Tópicos



## Ativar eventos do ciclo de vida do grupo em Grupos de recursos

Para receber notificações sobre mudanças no ciclo de vida de seus grupos de recursos, você pode nos eventos do ciclo de vida do grupo. Em seguida, o Resource Groups fornece informações sobre as mudanças de seus grupos na Amazon. EventBridge Em EventBridge, você pode avaliar e agir de acordo com as mudanças usando as regras definidas no EventBridge serviço.

**Permissões mínimas**

Para ativar os eventos do ciclo de vida do grupo em seu Conta da AWS, você deve entrar como diretor AWS Identity and Access Management (IAM) com as seguintes permissões:

- `resource-groups:UpdateAccountSettings`
- `iam:CreateServiceLinkedRole`

- `events:PutRule`
- `events:PutTargets`
- `events:DescribeRule`
- `events:ListTargetsByRule`
- `cloudformation:DescribeStacks`
- `cloudformation:ListStackResources`
- `tag:GetResources`

Quando você ativa inicialmente os eventos do ciclo de vida do grupo em um Conta da AWS, o Resource Groups cria uma função vinculada ao serviço chamada. `AWSServiceRoleForResourceGroups` Essa função gerenciada tem permissão para usar uma EventBridge regra gerenciada do Resource Groups. A regra monitora as tags anexadas aos seus recursos e as pilhas do AWS CloudFormation em sua conta para detectar quaisquer alterações. Em seguida, o Resource Groups publica essas alterações no barramento de eventos padrão na Amazon EventBridge. O serviço também cria uma regra EventBridge gerenciada chamada`Managed.ResourceGroups.TagChangeEvents`. Essa regra captura os detalhes das alterações de tag de seus recursos. Isso permite que os Resource Groups gerem eventos de associação EventBridge para serem enviados para processamento de suas regras personalizadas. Suas EventBridge regras podem então responder aos eventos enviando notificações para os alvos configurados das regras.

Depois de concluir essas etapas, as regras que buscam esses eventos devem começar a recebê-los em alguns minutos.

Você pode ativar os eventos do ciclo de vida do grupo usando ou usando um comando da AWS Management Console ou de uma das AWS CLI APIs do SDK.

> **Note**
>
> Você não pode ativar os eventos do ciclo de vida do grupo se a cota de grupos de recursos for muito alta. Para obter mais informações, consulte Exibir cotas de serviço.

AWS Management Console

Para ativar os eventos do ciclo de vida do grupo no console Grupos de recursos

1. Abra a página Configurações no console Grupos de recursos.
2. Na seção Eventos do ciclo de vida do grupo, escolha a opção ao lado de Notificações estão desativadas.
3. Na caixa de diálogo de confirmação, escolha Ativar notificações.

   O botão de atributo exibe Notificações ativadas.

Isso completa a primeira parte do processo. Depois de ativar as notificações de eventos, você pode criar regras na Amazon EventBridge que capturam os eventos e os enviam para pessoas específicas Serviços da AWS para processamento.

AWS CLI

Para ativar eventos do ciclo de vida do grupo usando o AWS CLI ou os SDKs AWS

O exemplo a seguir mostra como usar o AWS CLI para ativar eventos do ciclo de vida do grupo em Resource Groups. Insira o comando com o parâmetro da entidade principal do serviço exatamente como mostrado. A saída mostra o status atual e o status desejado do atributo.

```
$ aws resource-groups update-account-settings \
    --group-lifecycle-events-desired-status ACTIVE
{
    "AccountSettings": {
        "GroupLifecycleEventsDesiredStatus": "ACTIVE",
        "GroupLifecycleEventsStatus": "IN_PROGRESS"
    }
}
```

Você pode confirmar se o atributo está ativado executando o comando de exemplo a seguir. Quando os dois campos de status mostrarem o mesmo valor, a operação estará concluída.

```
$ aws resource-groups get-account-settings
{
    "AccountSettings": {
        "GroupLifecycleEventsDesiredStatus": "ACTIVE",
        "GroupLifecycleEventsStatus": "ACTIVE"
    }
```

```
}
```

Para obter mais informações, consulte os seguintes recursos do :

- AWS CLI — grupos de recursos da AWS e grupos de recursos da update-account-settings AWS get-account-settings
- API — UpdateAccountSettingse GetAccountSettings

## Criação de uma EventBridge regra para capturar eventos do ciclo de vida do grupo e publicar notificações

Você pode ativar eventos de ciclo de vida de grupos para seus grupos de recursos AWS Resource Groups para publicar eventos na Amazon. EventBridge Em seguida, você pode criar EventBridge regras que respondam a esses eventos enviando-os para outros Serviços da AWS para processamento posterior.

AWS CLI

O processo para criar uma regra EventBridge que capture eventos e os envie para o serviço de destino desejado usa dois comandos CLI separados:

1. Crie a EventBridge regra para capturar os eventos que você deseja
2. Anexe um alvo que possa processar os eventos à EventBridge regra

Etapa 1: criar a EventBridge regra para capturar os eventos

O comando de AWS CLI `put-rule` exemplo a seguir cria uma EventBridge regra que captura todas as alterações de eventos do ciclo de vida do Resource Groups.

```
$ aws events put-rule \
    --name "CatchAllResourceGroupEvents" \
    --event-pattern '{"source":["aws.resource-groups"]}'
{
    "RuleArn": "arn:aws:events:us-east-1:123456789012:rule/
CatchAllResourceGroupEvents"
}
```

O resultado inclui o nome do recurso da Amazon (ARN) para a nova política.

> **Note**
>
> Valores de parâmetros que incluem cadeias de caracteres entre aspas têm regras de formatação diferentes com base no sistema operacional e no shell em uso. Para os exemplos deste guia, mostramos comandos que funcionam em um shell Linux BASH. Para obter instruções sobre a formatação de cadeias de caracteres com aspas incorporadas para outros sistemas operacionais, como o prompt de comando do Windows, consulte Usando aspas dentro de cadeias de caracteres no Guia do usuário do AWS Command Line Interface.
> À medida que as cadeias de caracteres de parâmetros se tornam mais complexas, pode ser mais fácil e menos propenso a erros aceitar um valor de parâmetro de um arquivo de texto em vez de digitá-lo diretamente na linha de comando.

O padrão de eventos a seguir restringe os eventos somente àqueles relacionados ao grupo especificado, identificados por seu ARN. Esse padrão de evento é uma cadeia de caracteres JSON complexa que é muito menos legível quando compactada em uma cadeia de caracteres JSON de linha única com escape adequado. Em vez disso, você pode armazená-la em um arquivo.

Armazene a cadeia de caracteres JSON do padrão de evento em um arquivo. No exemplo de código a seguir, o arquivo é`eventpattern.txt`.

```
{
    "source": [ "aws.resource-groups" ],
    "detail": {
        "group": {
            "arn": [ "my-resource-group-arn" ]
        }
    }
}
```

Em seguida, execute o seguinte comando para criar a regra, recuperando o padrão de evento personalizado do arquivo.

```
$ aws events put-rule \
    --name "CatchResourceGroupEventsForMyGroup" \
    --event-pattern file://eventpattern.txt
{
```

```
    "RuleArn": "arn:aws:events:us-east-1:123456789012:rule/
CatchResourceGroupEventsForMyGroup"
}
```

Para capturar outros tipos de eventos dos Grupos de recursos, substitua a cadeia de caracteres `--event-pattern` por filtros como os apresentados na seção Exemplo de padrões de eventos EventBridge personalizados para diferentes casos de uso.

Etapa 2: anexar um alvo que possa processar os eventos à EventBridge regra

Agora que você tem uma regra que captura os eventos de seu interesse, é possível anexar um ou mais destinos para fazer algum tipo de processamento nos eventos.

O seguinte comando da AWS CLI, `put-targets`, anexa um tópico do Amazon Simple Notification Service (Amazon SNS) nomeado `my-sns-topic` à regra criada no exemplo anterior. Todos os assinantes do tópico recebem uma notificação quando ocorre uma alteração no grupo especificado na regra.

```
$ aws events put-targets \
    --rule CatchResourceGroupEventsForMyGroup \
    --targets Id=1,Arn=arn:aws:sns:us-east-1:123456789012:my-sns-topic
{
    "FailedEntryCount": 0,
    "FailedEntries": []
}
```

Nesse ponto, todas as alterações de grupo que correspondam ao padrão de evento em sua regra são enviadas automaticamente para o destino ou destinos configurados. Se, como no exemplo anterior, o destino for um tópico do Amazon SNS, todos os assinantes do tópico receberão uma mensagem contendo o evento conforme descrito em Estrutura e sintaxe dos eventos do ciclo de vida dos Grupos de recursos.

Para mais informações, consulte os seguintes recursos:

- AWS CLI — aws events put-rule e aws events put-targets
- API — PutRulee PutTargets

### Criação de uma regra para capturar somente tipos específicos de eventos do ciclo de vida do grupo

É possível criar uma regra com um padrão de evento personalizado que capture somente os eventos pelos quais você se interessa. Para obter detalhes completos sobre como filtrar eventos recebidos usando um padrão de evento personalizado, consulte EventBridge Eventos da Amazon no Guia do EventBridge usuário da Amazon.

Por exemplo, suponha que você queira que uma regra processe somente as notificações de Grupos de recursos que indicam a criação de um novo grupo de recursos. Você pode usar um padrão de evento personalizado semelhante ao exemplo a seguir.

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group State Change" ],
    "detail": {
        "state-change": "create"
    }
}
```

Esse filtro captura somente os eventos que têm esses valores exatos nos campos especificados. Para obter uma lista completa dos campos do disponíveis para você corresponder, consulte Estrutura e sintaxe dos eventos do ciclo de vida dos Grupos de recursos.

## Desativar eventos do ciclo de vida do grupo

Você pode desativar os eventos do ciclo de vida do grupo para impedir o AWS Resource Groups de emitir eventos para o Amazon EventBridge. É possível fazer isso usando o AWS Management Console ou usando um comando da AWS CLI ou uma das APIs do SDK.

> **Note**
>
> A desativação dos eventos do ciclo de vida do grupo exclui a regra gerenciada do EventBridge dos Grupos de recursos usada para verificar se há alterações nas tags e pilhas de recursos do AWS CloudFormation. Os Grupos de recursos não podem mais passar essas alterações para o EventBridge. Todas as regras que você definiu no EventBridge que procuram eventos dos Grupos de recursos param de receber eventos para serem processadas. Se você pretende ativar os eventos do ciclo de vida do grupo novamente no futuro, você pode desativar suas regras. Se você não pretende usar essas regras

novamente, é possível excluí-las. Para obter mais informações, consulte Desativar ou excluir uma regra para o EventBridge no Guia do usuário do Amazon EventBridge.
A desativação dos eventos do ciclo de vida do grupo não exclui o perfil vinculado a serviços. É possível excluir manualmente ao perfil vinculado a serviços usando o IAM. Se, posteriormente, você precisar ativar novamente os eventos do ciclo de vida do grupo e o perfil vinculado a serviços não existir, os Grupos de recursos a recriarão automaticamente.

Permissões mínimas

Para desativar os eventos do ciclo de vida do grupo na sua Conta da AWS atual, você deve entrar como entidade principal (IAM) do AWS Identity and Access Management com as seguintes permissões:

- `resource-groups:UpdateAccountSettings`
- `events:DeleteRule`
- `events:RemoveTargets`
- `events:DescribeRule`
- `events:ListTargetsByRule`

AWS Management Console

Para desativar as notificações de eventos do ciclo de vida do grupo no EventBridge

1. Abra a página Configurações no console Grupos de recursos.
2. Na seção Eventos do ciclo de vida do grupo, escolha a opção ao lado de Notificações estão ativadas.
3. Na caixa de diálogo de confirmação, escolha Desativar notificações.

   A opção de atributos é exibida: As notificações de eventos estão desativadas.

Nesse momento, os Grupos de recursos não enviam mais eventos para o barramento de eventos padrão do EventBridge e nenhuma regra que você tenha recebe eventos de notificação de grupo para processar. Opcionalmente, você pode excluir essas regras para concluir a limpeza.

AWS CLI

Para desativar as notificações de eventos do ciclo de vida do grupo no EventBridge

O exemplo a seguir mostra como usar a AWS CLI para desativar eventos do ciclo de vida do grupo em Grupos de recursos.

```
$ aws resource-groups update-account-settings \
    ----group-lifecycle-events-desired-status INACTIVE
{
    "AccountSettings": {
        "GroupLifecycleEventsDesiredStatus": "INACTIVE",
        "GroupLifecycleEventsStatus": "INACTIVE"
    }
}
```

Para mais informações, consulte os seguintes recursos do :

- AWS CLI – aws resource-groups update-account-settings e aws resource-groups get-account-settings
- API — UpdateAccountSettings e getAccountSettings

## Estrutura e sintaxe dos eventos do ciclo de vida dos Grupos de recursos

Os eventos do ciclo de vida do AWS Resource Groups assumem a forma de cadeias de caracteres de objetos JSON no seguinte formato geral.

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group ... Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/MyGroupName"
    ],
    "detail": {
        ...
```

```
    }
}
```

Para obter detalhes sobre os campos comuns a todos os EventBridge eventos da Amazon, consulte EventBridge Eventos da Amazon no Guia EventBridge do usuário da Amazon. Os detalhes específicos de Grupos de recursos são explicados na tabela a seguir.

| Nome do campo | Tipo | Descrição |
| --- | --- | --- |
| `detail-type` | Cadeia de caracteres | Para Grupos de recursos, o campo `detail-type` é sempre um dos seguintes valores:<br>• `ResourceGroups Group State Change`: representa mudanças no estado geral do grupo e em suas propriedades.<br>• `ResourceGroups Group Membership Change`: representa mudanças na associação ao grupo. |
| `source` | String | Para Grupos de recursos, esse valor é always `"aws.resource-groups"` . |
| `resources` | Uma matriz de nomes do recurso da Amazon (ARNs) | Este campo sempre inclui o nome do recurso da Amazon (ARN) do grupo com a alteração que acionou esse evento.<br>Este campo também pode incluir os ARNs de quaisquer recursos adicionados ou removidos do grupo, se aplicável. |
| `detail` | Cadeia de caracteres de objetos JSON | Esta é a carga útil do evento. O conteúdo do campo `detail` varia com base no valor do `detail-type` . Consulte a próxima seção para obter mais informações. |

## Estrutura do campo **`detail`**

O campo `detail` inclui todos os detalhes específicos do serviço Grupos de recursos sobre uma alteração específica. O campo `detail` pode assumir uma das duas formas, uma mudança de estado de grupo ou alteração de associação, com base no valor do campo `detail-type` descrito na seção anterior.

> **Important**
>
> Os Grupos de recursos nestes eventos são identificados por uma combinação do ARN do grupo e um campo `"unique-id"` que contém um UUID. Ao incluir um UUID como parte da identidade de um grupo de recursos, você pode distinguir entre um grupo excluído e um grupo diferente criado posteriormente com o mesmo nome. Recomendamos que você trate uma concatenação do ARN e do ID exclusivo como a chave para o grupo em seus programas que interagem com esses eventos.

Alteração de estado de grupo

```
"detail-type": "ResourceGroups Group State Change"
```

Este valor `detail-type` indica que o estado do próprio grupo, incluindo seus metadados, foi alterado. Esta alteração ocorre quando um grupo é criado, atualizado ou excluído, conforme indicado pelo campo `"change"` no `detail`.

As informações incluídas na seção `details` quando este `detail-type` é especificado incluem os campos descritos na tabela a seguir.

| Nome do campo | Tipo | Descrição |
|---|---|---|
| `event-sequence` | Double | Um número monotonicamente crescente que especifica a sequência de eventos para um grupo específico. O número é redefinido quando você exclui o grupo e cria outro com o mesmo nome. |
| `group` | Objeto JSON `Group` | O objeto de grupo associado ao evento por seu ARN, nome e ID exclusivo. |

| Nome do campo | Tipo | Descrição |
| --- | --- | --- |
| `state-change` | String | O tipo de mudança de estado que ocorreu. Pode ser qualquer um dos valores a seguir:<br>• `create`<br>• `update`<br>• `delete` |
| `old-state` | Objeto JSON `GroupState` | O estado do grupo antes da mudança. O objeto inclui somente os valores das propriedades que foram alteradas. |
| `new-state` | Objeto JSON `GroupState` | O estado do grupo após a mudança. O objeto inclui somente os valores das propriedades que foram alteradas. |

O objeto JSON `group` contém os elementos descritos na tabela a seguir.

| Nome do campo | Tipo | Descrição |
| --- | --- | --- |
| `arn` | Cadeia de caracteres | O ARN do grupo. |
| `name` | String | O nome amigável do grupo. |
| `unique-id` | GUID | Um valor de GUID exclusivo que distingue entre um grupo que foi excluído e um grupo diferente que foi criado posteriormente com o mesmo nome e ARN. Use a concatenação do ARN e esse valor como uma chave exclusiva para o grupo ao consumir esses eventos em seu código. |

Os objetos JSON `GroupState` contêm os elementos descritos na tabela a seguir.

| Nome do campo | Tipo | Descrição |
| --- | --- | --- |
| `description` | Cadeia de caracteres | A descrição fornecida pelo cliente do grupo de recursos. |
| `resource-query` | Objeto JSON `ResourceQuery` | Uma representação JSON da consulta que define os membros do grupo. Este campo está presente somente para grupos baseados em uma consulta. A sintaxe desse campo é definida pelo tipo de dados da ResourceQuery API. Exemplos disso estão incluídos nos eventos de exemplo de Criar e Atualizar. |
| `group-configuration` | Objeto JSON `Configuration` | Uma representação JSON dos parâmetros de configuração associados a um grupo vinculado ao serviço. Para obter mais informações, consulte Configurações de serviço para grupos de recursos na Referência da API do AWS Resource Groups. |

Cada um dos exemplos de código a seguir ilustra o conteúdo do campo `detail` para cada tipo `state-change`.

Criar

`"state-change": "create"`

O evento indica que um novo grupo foi criado. O evento carrega todas as propriedades de metadados do grupo definidas durante a criação do grupo. Este evento geralmente é seguido por um ou mais eventos de associação ao grupo, a menos que o grupo esteja vazio. As propriedades que têm um valor nulo não são exibidas no corpo do evento.

O exemplo de evento a seguir indica um grupo de recursos recém-criado chamado `my-service-group`. Neste exemplo, o grupo usa uma consulta com tag que corresponde somente instâncias do Amazon Elastic Compute Cloud (Amazon EC2) que têm a tag `"project"="my-service"`.

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
```

```
    "detail-type": "ResourceGroups Group State Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-group"
    ],
    "detail": {
        "event-sequence": 1.0,
        "state-change": "create",
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-
group",
            "name": "my-service-group",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        },
        "new-state": {
            "resource-query": {
                "type": "TAG_FILTERS_1_0",
                "query": "{
                    \"ResourceTypeFilters\": [\"AWS::EC2::Instance\"],
                    \"TagFilters\": [{\"Key\":\"project\", \"Values\":[\"my-service\"}]
                }"
            }
        }
    }
}
```

Atualizar

`"state-change": "update"`

O evento indica que um grupo existente foi modificado de alguma forma. O evento carrega somente as propriedades que foram alteradas em relação ao estado anterior. As propriedades que não foram alteradas não são exibidas no corpo do evento.

O evento de exemplo a seguir indica que a consulta baseada em tags no grupo de recursos do exemplo anterior foi modificada para incluir também recursos de volume do Amazon EC2 no grupo.

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
```

```
    "detail-type": "ResourceGroups Group State Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-group"
    ],
    "detail": {
        "event-sequence": 3.0,
        "state-change": "update",
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service-
group",
            "name": "my-service",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        },
        "new-state": {
            "resource-query": {
                "type": "TAG_FILTERS_1_0",
                "query": "{
                    \"ResourceTypeFilters\": [\"AWS::EC2::Instance\",
 \"AWS::EC2::Volume\"],
                    \"TagFilters\": [{\"Key\":\"project\", \"Values\":[\"my-service\"}]
                }"
            }
        },
        "old-state": {
            "resource-query": {
                "type": "TAG_FILTERS_1_0",
                "query": "{
                    \"ResourceTypeFilters\": [\"AWS::EC2::Instance\"],
                    \"TagFilters\": [{\"Key\":\"Project\", \"Values\":[\"my-service\"}]
                }"
            }
        }
    }
}
```

### Delete

`"state-change": "delete"`

O evento indica que um grupo existente foi excluído. O campo de detalhes não inclui metadados sobre o grupo além de sua identificação. O campo `event-sequence` é redefinido após esse evento, pois é, por definição, o último evento deste `arn` e `unique-id`.

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group State Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service"
    ],
    "detail": {
        "event-sequence": 4.0,
        "state-change": "delete",
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service",
            "name": "my-service",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        }
    }
}
```

Alteração de associação de grupo

`"detail-type": "ResourceGroups Group Membership Change"`

Este valor `detail-type` indica que a associação do grupo foi alterada pela adição ou remoção de um recurso do grupo. Quando este `detail-type` é especificado, o campo `resources` de nível superior inclui o ARN do grupo cuja associação foi alterada e os ARNs de todos os recursos que foram adicionados ou removidos do grupo.

As informações incluídas na seção `details` quando este `detail-type` é especificado incluem os campos descritos na tabela a seguir.

| Nome do campo | Tipo | Descrição |
| --- | --- | --- |
| `event-sequence` | Double | Um número monotonicamente crescente que indica a sequência de eventos para um grupo |

| Nome do campo | Tipo | Descrição |
| --- | --- | --- |
| | | específico. O número é redefinido quando o grupo é excluído e sua ID exclusiva é alterada. |
| `group` | Objeto JSON `Group` | Identifica o objeto de grupo associado ao evento por seu ARN, nome e ID exclusivo. |
| `resources` | Matriz de objetos JSON de `ResourceChange` | Uma matriz de recursos cuja associação ao grupo foi alterada.<br><br>Este objeto `ResourceChange` contém os campos a seguir para cada recurso:<br><br>• `membership-change` — O valor é `"add"` ou `"remove"`.<br>• `arn` — O ARN do recurso adicionado ou removido.<br>• `resource-type` — O tipo do recurso adicionado ou removido. |

O exemplo de código a seguir ilustra o conteúdo do evento para um tipo típico de alteração de associação. Este exemplo mostra um recurso sendo adicionado ao grupo e um recurso sendo removido do grupo.

```
{
    "version": "0",
    "id": "08f00e24-2e30-ec44-b824-8acddf1ac868",
    "detail-type": "ResourceGroups Group Membership Change",
    "source": "aws.resource-groups",
    "account": "123456789012",
    "time": "2020-09-29T09:59:01Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:resource-groups:us-east-1:123456789012:group/my-service",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111",
        "arn:aws:ec2:us-east-1:123456789012:instance/i-efef2222"
    ],
    "detail": {
        "event-sequence": 2.0,
```

```
        "group": {
            "arn": "arn:aws:resource-groups:us-east-1:123456789012:group/my-service",
            "name": "my-service",
            "unique-id": "3dd07ab7-3228-4410-8cdc-6c4a10fcceea"
        },
        "resources": [
            {
                "membership-change": "add",
                "arn": "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111",
                "resource-type": "AWS::EC2::Instance"
            },
            {
                "membership-change": "remove",
                "arn": "arn:aws:ec2:us-east-1:123456789012:instance/i-efef2222",
                "resource-type": "AWS::EC2::Instance"
            }
        ]
    }
}
```

## Exemplo de padrões de eventos EventBridge personalizados para diferentes casos de uso

O exemplo de padrões de eventos EventBridge personalizados a seguir filtra os eventos gerados pelo Resource Groups para somente aqueles nos quais você está interessado para uma regra e um destino de evento específicos.

Nos exemplos de código a seguir, se um grupo ou recurso específico for necessário, substitua cada *espaço reservado de entrada do usuário* por suas próprias informações.

Todos os eventos dos Grupos de recursos

```
{
    "source": [ "aws.resource-groups" ]
}
```

Eventos de mudança de estado ou associação do grupo

O exemplo de código a seguir é para todas as alterações de estado do grupo.

```
{
```

```
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group State Change " ]
}
```

O exemplo de código a seguir é para todas as alterações de associação do grupo.

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ]
}
```

Eventos para um grupo específico

```
{
    "source": [ "aws.resource-groups" ],
    "detail": {
        "group": {
            "arn": [ "my-group-arn" ]
        }
    }
}
```

O exemplo anterior captura as alterações no grupo especificado. O exemplo a seguir faz o mesmo e também captura as alterações quando o grupo é um recurso membro de outro grupo.

```
{
    "source": [ "aws.resource-groups" ],
    "resources": [ "my-group-arn" ]
}
```

Eventos para um recurso específico

Você pode filtrar somente eventos de alteração de associação de grupos para recursos específicos de membros.

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change " ],
    "resources": [ "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f" ]
}
```

Eventos para um tipo de recurso específico

Você pode usar a correspondência de prefixos com ARNs para combinar eventos de um tipo de recurso específico.

```
{
    "source": [ "aws.resource-groups" ],
    "resources": [
        { "prefix": "arn:aws:ec2:us-east-1:123456789012:instance" }
    ]
}
```

Como alternativa, você pode usar a correspondência exata usando identificadores `resource-type`, potencialmente correspondendo em mais de um tipo de forma concisa. Diferentemente do exemplo anterior, o exemplo a seguir corresponde somente aos eventos de alteração da associação ao grupo porque os eventos de mudança de estado do grupo não incluem um campo `resources` em seu campo `detail`.

```
{
    "source": [ "aws.resource-groups" ],
    "detail": {
        "resources": {
                "resource-type": [ "AWS::EC2::Instance", "AWS::EC2::Volume" ]
         }
    }
}
```

Todos os eventos de remoção de recurso

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ],
    "detail": {
        "resources": {
                "membership-change": [ "remove" ]
        }
    }
}
```

Todos os eventos de remoção de recursos para um recurso específico

```
 {
```

```
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ],
    "detail": {
        "resources": {
                "membership-change": [ "remove" ],
                "arn": [ "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f" ]
         }
    }
}
```

Você não pode usar a matriz `resources` de nível superior usada no primeiro exemplo desta seção para esse tipo de filtragem de eventos. Isso porque um recurso no elemento `resources` de nível superior pode ser um recurso que está sendo adicionado a um grupo e o evento ainda corresponderia. Em outras palavras, o exemplo de código a seguir pode retornar eventos inesperados. Em vez disso, use a sintaxe mostrada no exemplo anterior.

```
{
    "source": [ "aws.resource-groups" ],
    "detail-type": [ "ResourceGroups Group Membership Change" ],
    "resources": [ "arn:aws:ec2:us-east-1:123456789012:instance/i-b188560f" ],
    "detail": {
        "resources": {
                "membership-change": [ "remove" ]
         }
     }
}
```

# Excluir grupos de recursos do AWS Resource Groups

Você pode usar o console do AWS Resource Groups ou a AWS CLI para excluir grupos de recursos do AWS Resource Groups. A exclusão de um grupo de recursos não exclui os recursos que são membros do grupo ou das tags nos recursos de membro. Ela exclui apenas a estrutura do grupo e todas as tags em nível do grupo.

Console

Para excluir grupos de recursos

1. Faça login no console do AWS Resource Groups.
2. No painel de navegação, selecione Grupos de recursos salvos.

3. Escolha o nome do grupo de recursos que deseja excluir e depois selecione Visualizar detalhes.
4. Na página de detalhes do grupo, escolha Excluior no canto direito superior.
5. Quando solicitado a confirmar a exclusão, escolha Delete (Excluir).

AWS CLI & AWS SDKs

Para excluir grupos de recursos

1. Digite o comando a seguir, substituindo *resource_group_name* pelo nome de seu grupo.

```
$ aws resource-groups delete-group \
    --group-name resource_group_name
```

2. Quando solicitado a confirmar a exclusão, digite `yes` e pressione Enter.

# AWS serviços que funcionam com AWS Resource Groups

Você pode usar os seguintes AWS serviços com AWS Resource Groups.

| AWS serviço | Usar Grupos de recursos |
| --- | --- |
| AWS CloudFormation— Crie grupos de recursos AWS CloudFormation usando um modelo de pilha. | Provisione e organize AWS recursos ao mesmo tempo. Organize os recursos por tags. Organize recursos de outra pilha. Reúna insights sobre seus AWS recursos em grupos de recursos usando a Amazon CloudWatch ou realize ações operacionais usando AWS Systems Manager.<br><br>Para obter mais informações, consulte a referência do tipo de ResourceGroups recurso no Guia AWS CloudFormation do usuário. |
| CloudTrail— Capture todas as ações do grupo de recursos usando AWS CloudTrail. | Capture informações sobre ações realizadas em seus grupos de recursos, incluindo detalhes como quem realizou a ação (principal do |

| AWS serviço | Usar Grupos de recursos |
| --- | --- |
| | IAM, como uma função, usuário ou um AWS service (Serviço da AWS)), quando a ação foi realizada, onde a ação ocorreu (o endereço IP de origem) e muito mais. Esses registros podem então ser usados para análise ou para acionar ações de acompanhamento.<br><br>Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos. |
| Amazon CloudWatch — Permita o monitoram ento em tempo real de seus AWS recursos e dos aplicativos em que você executa AWS. | Concentre a exibição para mostrar métricas e alarmes em um único grupo de recursos.<br><br>Para obter mais informações, consulte Foco em métricas e alarmes em um grupo de recursos no Guia do CloudWatch usuário da Amazon. |
| Amazon CloudWatch Application Insights — Detecte problemas comuns com seus aplicativ os baseados em .NET e SQL Server. | Monitore os recursos de aplicações .NET e SQL Server que pertencem a um grupo de recursos.<br><br>Para obter mais informações, consulte Componentes de aplicativos compatíveis no Guia CloudWatch do usuário da Amazon. |
| Grupos de tabelas do Amazon DynamoDB — Organize suas tabelas do DynamoDB em agrupamentos lógicos para que você possa gerenciar seus recursos com mais facilidade. | Crie, edite e exclua grupos de tabelas do DynamoDB no menu Ação do DynamoDB.<br><br>Para obter mais informações, consulte o Guia do desenvolvedor do Amazon DynamoDB. |

| AWS serviço | Usar Grupos de recursos |
| --- | --- |
| Hosts dedicados do Amazon EC2 — Use suas licenças de software existentes por soquete, por núcleo ou por VM, incluindo o Windows Server, o Microsoft SQL Server, o SUSE e o Linux Enterprise Server. | Inicie instâncias do Amazon EC2 em grupos de recursos do host para ajudar a maximizar a utilização de hosts dedicados.<br><br>Para obter mais informações, consulte Como trabalhar com hosts dedicados no Guia do usuário do Amazon EC2. |
| Reservas de capacidade do Amazon EC2 — Reserve capacidade para que suas instância s do Amazon EC2 sejam usadas quando você precisar. Você pode especificar atributos para a reserva de capacidade para que ela funcione somente com instâncias do Amazon EC2 que sejam executadas com atributos correspon dentes. | Inicie suas instâncias do Amazon EC2 em grupos de recursos que contenham uma ou mais reservas de capacidade. Se o grupo não tiver uma reserva de capacidade com atributos correspondentes e capacidade disponível para uma instância solicitada, a instância será executada como uma instância sob demanda. Se você adicionar uma reserva de capacidad e correspondente ao grupo de destino, a correspondência da instância será automátic a e ela será movida para sua capacidade reservada.<br><br>Para obter mais informações, consulte Trabalhar com grupos de reserva de capacidad e no Guia do usuário do Amazon EC2. |
| AWS License Manager — Simplifica o processo de transferir as licenças de fornecedo r de software para a nuvem. | Configure um grupo de recursos de host para permitir que o License Manager gerencie seus hosts dedicados.<br><br>Para obter mais informações, consulte Grupos de recursos de host no License Manager no Guia do usuário do License Manager. |

| AWS serviço | Usar Grupos de recursos |
| --- | --- |
| AWS Resilience Hub — prepare e proteja seus aplicativos contra interrupções. | Descubra suas aplicações que são definidas usando Grupos de recursos.<br><br>Para obter mais informações, consulte Measure and Improve Your Application Resilience with AWS Resilience Hub no Blog de notícias da AWS . |
| AWS Resource Access Manager— Compartilhe AWS recursos específicos que você possui com outras contas. | Compartilhe grupos de recursos do host usando AWS RAM.<br><br>Para obter mais informações, consulte Recursos compartilháveis no Guia do usuário do AWS RAM . |
| AWS Service Catalog AppRegistry — Defina e gerencie suas aplicações e seus metadados. | Quando você cria um aplicativo em AppRegistry, esse serviço cria automaticamente um grupo de recursos para esse aplicativo. O grupo de recursos da aplicação é uma coleção de todos os recursos da sua aplicação. O serviço também cria um grupo de recursos AWS CloudFormation baseado em pilhas para cada pilha associada ao aplicativo.<br><br>Para obter mais informações, consulte Usando AppRegistry no Guia do AWS Service Catalog Administrador. |

| AWS serviço | Usar Grupos de recursos |
| --- | --- |
| AWS Systems Manager— Permita a visibilidade e o controle de seus AWS recursos. | Reúna insights operacionais e realize ações em massa em suas aplicações com base em grupos de recursos. No AWS Systems Manager console, a página Aplicativos personalizados do Application Manager importa e exibe automaticamente os dados de operações dos aplicativos baseados em grupos de recursos. Você pode usar as informações no Application Manager para ajudar a determinar quais recursos em um grupo estão em conformidade e funcionando corretamente, e quais recursos exigem ação.<br><br>Para obter mais informações, consulte Trabalhar com aplicações no Application Manager no Guia do usuário do AWS Systems Manager . |
| Analisador de Acesso à Rede do Amazon VPC — Identifique o acesso à rede indesejado aos seus recursos na AWS. | Você pode especificar as fontes e os destinos para seus requisitos de acesso à rede usando AWS Resource Groups. Isso permite que você controle o acesso à rede em seu AWS ambiente, independentemente de como você configura sua rede.<br><br>Para obter mais informações, consulte Usar os Grupos de recursos com escopos de acesso à rede no Guia do usuário do Amazon Virtual Private Cloud. |

## Configurações de serviço para grupos de recursos

Os grupos de recursos permitem que você gerencie coleções de seus AWS recursos como uma unidade. Alguns produtos da AWS oferecem suporte a isso executando as operações solicitadas em todos os membros do grupo. Esses serviços podem armazenar as configurações a serem aplicadas

aos membros do grupo como uma configuração na forma de uma estrutura de dados JSON anexada ao grupo.

Este tópico descreve as definições de configuração disponíveis para os produtos da AWS compatíveis.

Tópicos

- Como acessar a configuração do serviço anexada a um grupo de recursos
- Sintaxe JSON de uma configuração de serviço
- Tipos e parâmetros de configuração compatíveis

## Como acessar a configuração do serviço anexada a um grupo de recursos

Os serviços que oferecem suporte a grupos vinculados a serviços geralmente definem a configuração para você quando você usa as ferramentas fornecidas por esse serviço, como o console de gerenciamento desse serviço ou suas operações AWS CLI e do AWS SDK. Alguns serviços gerenciam totalmente seus grupos vinculados a serviços e você não pode modificá-los de nenhuma forma, exceto conforme permitido pelo console ou pelos comandos fornecidos pelo serviço proprietário AWS . No entanto, em alguns casos, você pode interagir com a configuração do serviço usando as seguintes operações de API nos AWS SDKs ou em seus AWS CLI equivalentes:

- Você pode anexar sua própria configuração a um grupo ao criar o grupo usando a CreateGroupoperação.
- Você pode modificar a configuração atual anexada a um grupo usando a PutGroupConfigurationoperação.
- Você pode ver a configuração atual de um grupo de recursos chamando a GetGroupConfigurationoperação.

## Sintaxe JSON de uma configuração de serviço

Um grupo de recursos pode conter uma configuração que define configurações específicas do serviço que se aplicam aos recursos que são membros desse grupo.

Uma configuração é expressa como um objeto JSON. No nível mais alto, uma configuração é uma matriz de itens de configuração de grupo. Cada item de configuração de grupo contém dois elementos: um `Type` para a configuração e um conjunto de `Parameters` definidos por esse tipo.

Cada parâmetro contém um `Name` e uma matriz de um ou mais `Values`. O exemplo a seguir com *`espaços reservados`* mostra a sintaxe básica de uma configuração para um único tipo de recurso de amostra. Este exemplo mostra um tipo com dois parâmetros e cada parâmetro com dois valores. Os tipos, parâmetros e valores reais válidos são discutidos na próxima seção.

```
{
    "Configuration": [
        {
            "Type": "configuration-type",
            "Parameters": [
                {
                    "Name": "parameter1-name",
                    "Values": [
                        "value1",
                        "value2"
                    ]
                },
                {
                    "Name": "parameter2-name",
                    "Values": [
                        "value3",
                        "value4"
                    ]
                }
            ]
        }
    ]
}
```

## Tipos e parâmetros de configuração compatíveis

Os Grupos de recursos são compatíveis usando estes tipos de configuração. Cada tipo de configuração tem um conjunto de parâmetros que são válidos para esse tipo.

Tópicos

- AWS::ResourceGroups::Generic
- AWS::AppRegistry::Application
- AWS::CloudFormation::Stack
- AWS::EC2::CapacityReservationPool
- AWS::EC2::HostManagement

- AWS::NetworkFirewall::RuleGroup

## AWS::ResourceGroups::Generic

Esse tipo de configuração especifica as configurações que impõem os requisitos de associação ao grupo de recursos, em vez de definir o comportamento de um tipo de recurso específico para um serviço. AWS Este tipo de configuração é adicionado automaticamente pelos grupos vinculados ao serviço que precisam dele, como os tipos `AWS::EC2::CapacityReservationPool` e `AWS::EC2::HostManagment`.

Os `Parameters` a seguir são válidos para o grupo vinculado ao serviço `AWS::ResourceGroups::Generic` `Type`.

- **`allowed-resource-types`**

  Este parâmetro especifica que o grupo de recursos pode consistir somente em recursos do tipo ou tipos especificados.

  Tipo de dados dos valores: cadeia de caracteres

  Valores permitidos:

  - `AWS::EC2::Host` — Um `Configuration` com esse parâmetro e valor é necessário quando a configuração do serviço também contém uma `Configuration` do tipo `AWS::EC2::HostManagement`. Isso garante que o grupo `HostManagement` possa conter somente hosts dedicados do Amazon EC2.
  - `AWS::EC2::CapacityReservation` — Um `Configuration` com esse parâmetro e valor é necessário quando a configuração do serviço também contém um item `Configuration` do tipo `AWS::EC2::CapacityReservationPool`. Isso garante que um grupo `CapacityReservation` possa conter somente a capacidade de reserva de capacidade do Amazon EC2.

  Obrigatório: condicional, com base em outros elementos de `Configuration` anexados ao grupo de recursos. Consulte a entrada anterior a respeito de Valores permitidos.

  O exemplo a seguir restringe os membros do grupo somente às instâncias de host do Amazon EC2.

```
{
    "Configuration": [
```

```
        {
            "Type": "AWS::ResourceGroups::Generic",
            "Parameters": [
                {
                    "Name": "allowed-resource-types",
                    "Values": ["AWS::EC2::Host"]
                }
            ]
        }
    ]
}
```

- **`deletion-protection`**

  Esse parâmetro especifica que o grupo de recursos não pode ser excluído a menos que não contenha membros. Para obter mais informações, consulte Excluir um grupo de recursos de host no Guia do usuário do License Manager

  Tipo de dados dos valores: matriz de cadeia de caracteres

  Valores permitidos: o único valor permitido é `[ "UNLESS_EMPTY" ]` (o valor deve estar em maiúsculas).

  Obrigatório: condicional, com base em outros elementos de `Configuration` anexados ao grupo de recursos. Esse parâmetro é necessário somente quando o grupo de recursos também tem outro elemento `Configuration` com o `Type` de `AWS::EC2::HostManagement`.

  O exemplo a seguir permite a proteção contra exclusão do grupo, a menos que o grupo não tenha membros.

```
{
    "Configuration": [
        {
            "Type": "AWS::ResourceGroups::Generic",
            "Parameters": [
                {
                    "Name": "deletion-protection",
                    "Values": [ "UNLESS_EMPTY" ]
                }
            ]
        }
    ]
```

```
}
```

### AWS::AppRegistry::Application

Esse `Configuration` tipo especifica que o grupo de recursos representa um aplicativo criado por AWS Service Catalog AppRegistry.

Grupos de recursos desse tipo são totalmente gerenciados pelo AppRegistry serviço e não podem ser criados, atualizados ou excluídos por usuários, exceto usando as ferramentas fornecidas pelo AppRegistry.

> **Note**
>
> Como os grupos de recursos desse tipo são criados e mantidos automaticamente pelo usuário AWS e não são gerenciados pelo usuário, esses grupos de recursos não contam no limite de cota para o número máximo de grupos de recursos que você pode criar no seu Conta da AWS.

Para obter mais informações, consulte Using AppRegistry in the Service Catalog User Guide.

Ao AppRegistry criar um grupo de recursos vinculado a serviços desse tipo, ele também cria automaticamente um grupo AWS CloudFormation vinculado a serviços adicional separado para cada AWS CloudFormation pilha associada ao aplicativo.

AppRegistry nomeia automaticamente os grupos vinculados a serviços desse tipo que ele cria com o prefixo `AWS_AppRegistry_Application-` seguido pelo nome do aplicativo: `AWS_AppRegistry_Application-`*`MyAppName`*

Os parâmetros a seguir são compatíveis com o tipo de grupo vinculado ao serviço de `AWS::AppRegistry::Application`.

- **`Name`**

  Esse parâmetro especifica o nome amigável do aplicativo que foi atribuído pelo usuário quando ele foi criado no AppRegistry.

  Tipo de dados dos valores: cadeia de caracteres

Valores permitidos: qualquer sequência de texto permitida pelo AppRegistry serviço para o nome de um aplicativo.

Obrigatório: Sim

- **`Arn`**

  Esse parâmetro especifica o caminho do Amazon Resource Name (ARN) do aplicativo atribuído por. AppRegistry

  Tipo de dados dos valores: cadeia de caracteres

  Valores permitidos: um ARN válido.

  Obrigatório: Sim

> **Note**
>
> Para alterar qualquer um desses elementos, você deve modificar o aplicativo usando o AppRegistry console ou o AWS SDK e AWS CLI as operações desse serviço.

Esse grupo de recursos do aplicativo inclui automaticamente como membros do grupo os grupos de recursos criados para as AWS CloudFormation pilhas associadas ao AppRegistry aplicativo. Você pode usar a ListGroupResourcesoperação para ver esses grupos de filhos.

O exemplo a seguir mostra a aparência da seção de configuração de um grupo vinculado a serviços do `AWS::AppRegistry::Application`.

```
{
    "Configuration": [
        {
            "Type": "AWS::AppRegistry::Application",
            "Parameters":[
                {
                    "Name": "Name",
                    "Values": [
                        "MyApplication"
                    ]
```

```
                },
                {
                    "Name": "Arn",
                    "Values": [
                        "arn:aws:servicecatalog:us-east-1:123456789012:/
applications/<application-id>"
                    ]
                }
            ]
        }
    ]
}
```

### `AWS::CloudFormation::Stack`

Esse `Configuration` tipo especifica que o grupo representa uma AWS CloudFormation pilha e seus membros são os AWS recursos criados por essa pilha.

Grupos de recursos desse tipo são criados automaticamente para você quando você associa uma AWS CloudFormation pilha ao AppRegistry serviço. Você não pode criar, atualizar ou excluir esses grupos, exceto usando as ferramentas fornecidas pelo AppRegistry.

AppRegistry nomeia automaticamente os grupos vinculados a serviços desse tipo que ele cria com o prefixo `AWS_CloudFormation_Stack-` seguido pelo nome da pilha: `AWS_CloudFormation_Stack-`*`MyStackName`*

> **Note**
>
> Como os grupos de recursos desse tipo são criados e mantidos automaticamente pelo usuário AWS e não são gerenciados pelo usuário, esses grupos de recursos não contam no limite de cota para o número máximo de grupos de recursos que você pode criar no seu Conta da AWS.

Para obter mais informações, consulte Using AppRegistry in the Service Catalog User Guide.

AppRegistry cria automaticamente um grupo de recursos vinculado a serviços desse tipo para cada AWS CloudFormation pilha que você associa ao aplicativo. AppRegistry Esses grupos de recursos se tornam membros secundários do grupo de recursos principal do AppRegistry aplicativo.

Os membros desse grupo de AWS CloudFormation recursos são os AWS recursos criados como parte da pilha.

Os parâmetros a seguir são compatíveis com o tipo de grupo vinculado ao serviço de `AWS::CloudFormation::Stack`.

- **`Name`**

  Esse parâmetro especifica o nome amigável da AWS CloudFormation pilha atribuída pelo usuário quando a pilha foi criada.

  Tipo de dados dos valores: cadeia de caracteres

  Valores permitidos: qualquer sequência de texto permitida pelo AWS CloudFormation serviço para o nome de uma pilha.

  Obrigatório: Sim

- **`Arn`**

  Esse parâmetro especifica o caminho do Amazon Resource Name (ARN) da AWS CloudFormation pilha anexada ao aplicativo em. AppRegistry

  Tipo de dados dos valores: cadeia de caracteres

  Valores permitidos: um ARN válido.

  Obrigatório: Sim

> **Note**
>
> Para alterar qualquer um desses elementos, você deve modificar o aplicativo usando o AppRegistry console ou o AWS SDK e AWS CLI as operações equivalentes.

O exemplo a seguir mostra a aparência da seção de configuração de um grupo vinculado a serviços do `AWS::CloudFormation::Stack`.

```
{
    "Configuration": [
```

```
        {
            "Type": "AWS::CloudFormation::Stack",
            "Parameters":[
                {
                    "Name": "Name",
                    "Values": [
                        "MyStack"
                    ]
                },
                {
                    "Name": "Arn",
                    "Values": [
                        "arn:aws:cloudformation:us-
east-1:123456789012:stack/MyStack/<stack-id>"
                    ]
                }
            ]
        }
    ]
}
```

## `AWS::EC2::CapacityReservationPool`

Esse tipo `Configuration` especifica que o grupo de recursos representa um pool comum de capacidade fornecido pelos membros do grupo. Os membros desse grupo de recursos devem ser reservas de capacidade do Amazon EC2. Um grupo de recursos pode incluir reservas de capacidade que você possui em sua conta e reservas de capacidade que são compartilhadas com você de outras contas usando AWS Resource Access Manager. Isso permite que você execute uma instância do Amazon EC2 usando esse grupo de recursos como o valor do parâmetro de reserva de capacidade. Quando você faz isso, a instância usa a capacidade reservada disponível no grupo. Se o grupo de recursos não tiver capacidade disponível, a instância será executada como uma instância autônoma sob demanda fora do pool. Para obter mais informações, consulte Como trabalhar com grupos de reserva de capacidade no Guia do usuário do Amazon EC2.

Se você configurar um grupo de recursos vinculado ao serviço com um item de `Configuration` deste tipo, também deverá especificar itens diferentes de `Configuration` com os seguintes valores:

- Um tipo `AWS::ResourceGroups::Generic` com um parâmetro:

- O parâmetro `allowed-resource-types` e um valor único de `AWS::EC2::CapacityReservation`. Isso garante que somente as reservas de capacidade do Amazon EC2 possam ser membros do grupo de recursos.

O item `AWS::EC2::CapacityReservationPool` em uma configuração de grupo não oferece suporte a nenhum parâmetro.

O exemplo a seguir mostra a aparência da seção `Configuration` de um grupo como esse.

```
{
    "Configuration": [
        {
            "Type": "AWS::EC2::CapacityReservationPool"
        },
        {
            "Type": "AWS::ResourceGroups::Generic",
            "Parameters": [
                {
                    "Name": "allowed-resource-types",
                    "Values": [ "AWS::EC2::CapacityReservation" ]
                }
            ]
        }
    ]
}
```

### `AWS::EC2::HostManagement`

Esse identificador especifica as configurações para o gerenciamento de host do Amazon EC2 AWS License Manager e que são aplicadas aos membros do grupo. Para obter mais informações, consulte Hospedar grupos de recursos em AWS License Manager.

Se você configurar um grupo de recursos vinculado ao serviço com um item de `Configuration` deste tipo, também deverá especificar itens diferentes de `Configuration` com os seguintes valores:

- Um tipo `AWS::ResourceGroups::Generic`, com um parâmetro de `allowed-resource-types` e um valor único de `AWS::EC2::Host`. Isso garante que somente hosts dedicados do Amazon EC2 possam ser membros do grupo.

- Um tipo `AWS::ResourceGroups::Generic`, com um parâmetro de `deletion-protection` e um valor único de `UNLESS_EMPTY`. Isso garante que o grupo não possa ser excluído, a menos que esteja vazio.

Os parâmetros a seguir são compatíveis com o tipo de grupo vinculado ao serviço de `AWS::EC2::HostManagement`.

- **`auto-allocate-host`**

  Esse parâmetro permite que você gerencie se as instâncias são executadas em um host dedicado específico ou em qualquer host disponível com as configurações correspondentes. Para obter mais informações, consulte Noções básicas sobre posicionamento automático e afinidade no Guia do usuário do Amazon EC2.

  Tipo de dados dos valores: booleano

  Valores permitidos: "true" or "false" (devem estar em minúsculas).

  Obrigatório: não

```
{
    "Configuration": [
        {
            "Type": "AWS::EC2::HostManagement",
            "Parameters": [
                {
                    "Name": "auto-allocate-host",
                    "Values": [ "true" ]
                }
            ]
        },
        {
            "Type": "AWS::ResourceGroups::Generic",
            "Parameters": [
                {
                    "Name": "allowed-resource-types",
                    "Values": [ "AWS::EC2::Host" ]
                },
                {
                    "Name": "deletion-protection",
                    "Values": [ "UNLESS_EMPTY" ]
```

```
                }
            ]
        }
    ]
}
```

- **`auto-release-host`**

  Esse parâmetro especifica se um host dedicado no grupo é liberado automaticamente após o encerramento da última instância em execução. Para obter mais informações, consulte Lançamento de hosts dedicados no Guia do usuário do Amazon EC2.

  Tipo de dados dos valores: booleano

  Valores permitidos: "true" or "false" (devem estar em minúsculas).

  Obrigatório: não

```
{
    "Configuration": [
        {
            "Type": "AWS::EC2::HostManagement",
            "Parameters": [
                {
                    "Name": "auto-release-host",
                    "Values": [ "false" ]
                }
            ]
        },
        {
            "Type": "AWS::ResourceGroups::Generic",
            "Parameters": [
                {
                    "Name": "allowed-resource-types",
                    "Values": [ "AWS::EC2::Host" ]
                },
                {
                    "Name": "deletion-protection",
                    "Values": [ "UNLESS_EMPTY" ]
                }
            ]
        }
    ]
```

```
}
```

- **`allowed-host-families`**

  Esse parâmetro especifica quais famílias de tipos de instância podem ser usadas por instâncias que são membros desse grupo.

  Tipo de dados dos valores: matriz de cadeia de caracteres.

  Valores permitidos: cada um deve ser um identificador válido da família do tipo de instância do Amazon EC2, como `C4`, `M5`, `P3dn` ou `R5d`.

  Obrigatório: não

  O exemplo de item de configuração a seguir especifica que as instâncias executadas só podem ser membros das famílias de tipos de instância C5 ou M5.

```
{
    "Configuration": [
        {
            "Type": "AWS::EC2::HostManagement",
            "Parameters": [
                {
                    "Name": "allowed-host-families",
                    "Values": ["c5", "m5"]
                }
            ]
        },
        {
            "Type": "AWS::ResourceGroups::Generic",
            "Parameters": [
                {
                    "Name": "allowed-resource-types",
                    "Values": ["AWS::EC2::Host"]
                },
                {
                    "Name": "deletion-protection",
                    "Values": ["UNLESS_EMPTY"]
                }
            ]
        }
    ]
```

```
}
```

- **`allowed-host-based-license-configurations`**

  Esse parâmetro especifica os caminhos do nome do recurso da Amazon (ARN) de uma ou mais configurações de licença baseadas em core/soquete que você deseja aplicar aos membros do grupo.

  Tipo de dados dos valores: matriz de ARNs.

  Valores permitidos: cada um deve ser um ARN válido de configuração do License Manager.

  Obrigatório: condicional. Você deve especificar este parâmetro ou `any-host-based-license-configuration`, mas não ambos. Os parâmetros são mutuamente exclusivos.

  O exemplo de item de configuração a seguir especifica que os membros do grupo podem usar as duas configurações especificadas do License Manager.

```
{
    "Configuration": [
        {
            "Type": "AWS::EC2::HostManagement",
            "Parameters": [
                {
                    "Name": "allowed-host-based-license-configurations",
                    "Values": [
                        "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-6eb6586f508a786a2ba41EXAMPLE1111",
                        "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-8a786a26f50ba416eb658EXAMPLE2222"
                    ]
                }
            ]
        },
        {
            "Type": "AWS::ResourceGroups::Generic",
            "Parameters": [
                {
                    "Name": "allowed-resource-types",
                    "Values": [ "AWS::EC2::Host" ]
                },
                {
                    "Name": "deletion-protection",
```

```
                    "Values": [ "UNLESS_EMPTY" ]
                }
            ]
        }
    ]
}
```

- **`any-host-based-license-configuration`**

  Esse parâmetro especifica que você não deseja associar uma configuração de licença específica ao seu grupo. Nesse caso, todas as configurações de licença baseadas em core/soquete estão disponíveis para os membros do seu grupo de recursos do host. Use essa configuração se você tiver um número ilimitado de licenças e quiser otimizar a utilização do host.

  Tipo de dados dos valores: booleano

  Valores permitidos: "true" or "false" (devem estar em minúsculas).

  Obrigatório: condicional. Você deve especificar este parâmetro ou `allowed-host-based-license-configurations`, mas não ambos. Os parâmetros são mutuamente exclusivos.

  O exemplo de item de configuração a seguir especifica que os membros do grupo podem usar qualquer configuração de licença baseada em core/soquete.

```
{
    "Configuration": [
        {
            "Type": "AWS::EC2::HostManagement",
            "Parameters": [
                {
                    "Name": "any-host-based-license-configuration",
                    "Values": ["true"]
                }
            ]
        },
        {
            "Type": "AWS::ResourceGroups::Generic",
            "Parameters": [
                {
                    "Name": "allowed-resource-types",
                    "Values": ["AWS::EC2::Host"]
                },
                {
```

```
                    "Name": "deletion-protection",
                    "Values": ["UNLESS_EMPTY"]
                }
            ]
        }
    ]
}
```

O exemplo a seguir ilustra como incluir todas as configurações de gerenciamento do host em uma única configuração.

```
{
    "Configuration": [
        {
            "Type": "AWS::EC2::HostManagement",
            "Parameters": [
                {
                    "Name": "auto-allocate-host",
                    "Values": ["true"]
                },
                {
                    "Name": "auto-release-host",
                    "Values": ["false"]
                },
                {
                    "Name": "allowed-host-families",
                    "Values": ["c5", "m5"]
                },
                {
                    "Name": "allowed-host-based-license-configurations",
                    "Values": [
                        "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-6eb6586f508a786a2ba41EXAMPLE1111",
                        "arn:aws:license-manager:us-west-2:123456789012:license-
configuration:lic-8a786a26f50ba416eb658EXAMPLE2222"
                    ]
                }
            ]
        },
        {
            "Type": "AWS::ResourceGroups::Generic",
            "Parameters": [
```

```
                {
                    "Name": "allowed-resource-types",
                    "Values": ["AWS::EC2::Host"]
                },
                {
                    "Name": "deletion-protection",
                    "Values": ["UNLESS_EMPTY"]
                }
            ]
        }
    ]
}
```

### `AWS::NetworkFirewall::RuleGroup`

Esse identificador especifica configurações para grupos de AWS Network Firewall regras que são aplicadas aos membros do grupo. Os administradores de firewall podem especificar o ARN de um grupo de recursos desse tipo para resolver automaticamente os endereços IP dos membros do grupo para uma regra de firewall, em vez de precisar listar cada endereço manualmente. Para obter mais informações, consulte Usar grupos de recursos baseados em tags no AWS Network Firewall.

Você pode criar grupos de recursos desse tipo de configuração usando o console do Network Firewall ou executando um AWS CLI comando ou uma operação do AWS SDK.

Grupos de recursos desse tipo de configuração têm as seguintes restrições:

- Os membros do grupo consistem somente em recursos dos tipos suportados pelo Network Firewall.
- O grupo deve conter uma consulta baseada em tags para gerenciar a associação do grupo; quaisquer recursos de tipos compatíveis com tags que correspondam à consulta são automaticamente membros do grupo.
- Não há suporte a `Parameters` para esse tipo de configuração.
- Para excluir um grupo de recursos desse tipo de configuração, ele não pode ser referenciado por nenhum grupo de regras do Network Firewall.

O exemplo a seguir ilustra as seções `ResourceQuery` e `Configuration` e de um grupo desse tipo.

```
{
```

```
    "Configuration": [
        {
            "Type": "AWS::NetworkFirewall::RuleGroup",
            "Parameters": []
        }
    ],
    "ResourceQuery": {
        "Query": "{\"ResourceTypeFilters\":[\"AWS::EC2::Instance\"],\"TagFilters\":
[{\"Key\":\"environment\",\"Values\":[\"production\"]}]}",
        "Type": "TAG_FILTERS_1_0"
    }
}
```

O AWS CLI comando de exemplo a seguir cria um grupo de recursos com a configuração e a consulta anteriores.

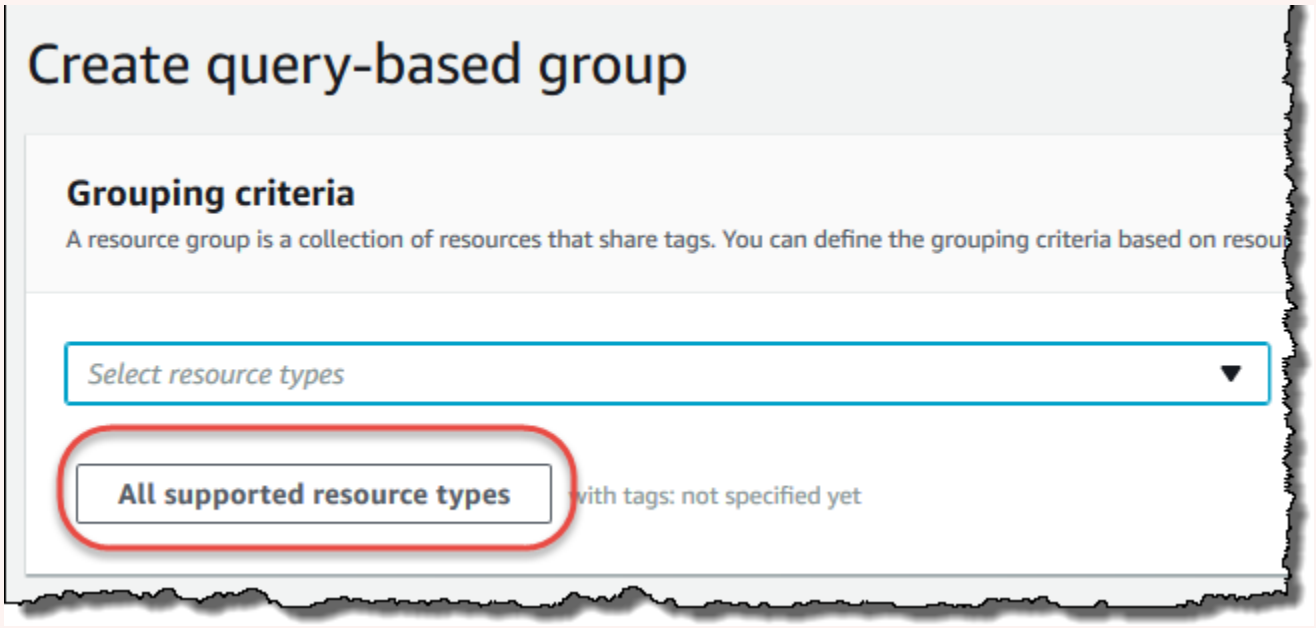
```
$ aws resource-groups create-group \
    --name test-group \
    --resource-query '{"Type": "TAG_FILTERS_1_0", "Query": "{\"ResourceTypeFilters\":
 [\"AWS::EC2::Instance\"], \"TagFilters\": [{\"Key\": \"environment\", \"Values\":
 [\"production\"]}]}"}' \
    --configuration '[{"Type": "AWS::NetworkFirewall::RuleGroup", "Parameters": []}]'
{
    "Group":{
        "GroupArn":"arn:aws:resource-groups:us-west-2:123456789012:group/test-group",
        "Name":"test-group",
        "OwnerId":"123456789012"
    },
    "Configuration": [
        {
            "Type": "AWS::NetworkFirewall::RuleGroup",
            "Parameters": []
        }
    ],
    "ResourceQuery": {
        "Query": "{\"ResourceTypeFilters\":[\"AWS::EC2::Instance\"],\"TagFilters\":
[{\"Key\":\"environment\",\"Values\":[\"production\"]}]}",
        "Type": "TAG_FILTERS_1_0"
    }
}
```

# Tipos de recursos que você pode usar com AWS Resource Groups o Tag Editor

Você pode usar o AWS Management Console ou o AWS CLI para criar grupos de recursos e depois interagir com os recursos dos membros por meio desses grupos. Você pode adicionar tags a vários AWS recursos e depois usar essas tags para gerenciar a associação ao grupo. Este tópico descreve os tipos de AWS recursos que você pode incluir em grupos de recursos usando AWS Resource Groups e os tipos de recursos que você pode marcar usando o Editor de tags.

**Important**

Um grupo de recursos baseado em uma consulta de All supported resource types (Todos os tipos de recurso compatíveis) pode adicionar membros automaticamente ao longo do tempo, à medida que novos recursos passam a ser compatíveis com os Grupos de recursos. Ao executar automações ou outras tarefas em massa em um grupo de recursos existente baseado em All supported resource types (Todos os tipos de recurso compatíveis), lembre-se de que as ações podem ser executadas em muito mais recursos do que os que estavam no grupo quando você criou o grupo. Isso também pode significar que as automações ou tarefas que você criou para outros recursos são aplicadas a recursos possivelmente não intencionais ou a recursos nos quais as tarefas não podem ser concluídas com êxito. Nesses casos, você pode adicionar um filtro de tipo de recurso para especificar que somente recursos dos tipos especificados podem fazer parte do grupo.



As tabelas a seguir listam quais tipos de recursos são compatíveis com a marcação no Editor de tags, a participação em grupos baseados em consultas de tags e a participação em grupos baseados em AWS CloudFormation pilhas.

Definições de coluna

- Marcação do Tag Editor — Você pode marcar recursos desse tipo usando o console do Tag Editor. Caso contrário, você deverá usar os serviços de marcação ou AWS Resource Groups Tagging API compatíveis de forma nativa com o serviço proprietário desse recurso.
- Grupos baseados em tags — Você pode incluir recursos desse tipo em grupos de recursos cuja associação seja determinada pelas tags anexadas aos recursos. O grupo especifica os nomes e valores das chaves da tag, e todos os recursos com tags correspondentes são automaticamente parte do grupo
- AWS CloudFormation Grupos baseados em pilhas — Você pode incluir recursos desse tipo em grupos de recursos cuja associação consiste nos recursos criados como parte de uma CloudFormation pilha. O grupo especifica o ARN da pilha e todos os seus recursos são automaticamente membros do grupo. Adicionar tags a uma AWS CloudFormation pilha causa uma atualização da pilha.

Para obter uma lista dos tipos de recursos que estão obsoletos e não são mais compatíveis com Grupos de recursos, consulte a seção Tipos de recursos descontinuados no final deste tópico.

> **Note**
>
> Os Resource Groups e o Tag Editor são compatíveis com os tipos de recursos na tabela a seguir, mas alguns tipos de recursos podem não estar disponíveis no seu Região da AWS.

# Amazon API Gateway

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::ApiGateway::Account` | ✗ Não | ✗ Não | ✓ Sim |
| `AWS::ApiGateway::ApiKey` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::ApiGateway::ClientCertificate` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::ApiGateway::DomainName` | ✗ Não | ✗ Não | ✓ Sim |
| `AWS::ApiGateway::RestApi` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::ApiGateway::Stage` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::ApiGateway::UsagePlan` | ✗ Não | ✓ Sim | ✓ Sim |

# Amazon API Gateway V2

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::ApiGatewayV2::Api` | ✗ Não | ✓ Sim | ✗ Não |

# IAM Access Analyzer

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::AccessAnalyzer::Analyzer` | ✗ Não | ✓ Sim | ✗ Não |

# AWS Amplify

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Amplify::App` | ✗ Não | ✓ Sim | ✗ Não |

# AWS App Mesh

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::AppMesh::Mesh` | ✗ Não | ✓ Sim | ✗ Não |

# Amazon AppStream

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::AppStream::AppBlock` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::AppStream::Application` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::AppStream::Fleet` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::AppStream::ImageBuilder` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::AppStream::Stack` | ✓ Sim | ✓ Sim | ✓ Sim |

# AWS AppSync

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::AppSync::DataSource` | ✗ Não | ✗ Não | ✓ Sim |
| `AWS::AppSync::GraphQLApi` | ✗ Não | ✗ Não | ✓ Sim |

# Amazon Athena

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Athena::DataCatalog` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::Athena::WorkGroup` | ✗ Não | ✓ Sim | ✗ Não |

# AWS Backup

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Backup::BackupPlan` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::Backup::BackupVault` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::Backup::ReportPlan` | ✗ Não | ✓ Sim | ✗ Não |

# AWS Batch

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Batch::ComputeEnvironment` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::Batch::JobQueue` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::Batch::SchedulingPolicy` | ✗ Não | ✓ Sim | ✗ Não |

# AWS Billing Conductor

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::BillingConductor::BillingGroup` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::BillingConductor::CustomLineItem` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::BillingConductor::PricingPlan` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::BillingConductor::PricingRule` | ✗ Não | ✓ Sim | ✓ Sim |

## Amazon Braket

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Braket::Job` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::Braket::QuantumTask` | ✓ Sim | ✓ Sim | ✗ Não |

## AWS Certificate Manager

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::CertificateManager::Certificate` | ✓ Sim | ✓ Sim | ✓ Sim |

## AWS Certificate Manager Autoridade de certificação privada

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::ACMPCA::CertificateAuthority` | ✗ Não | ✓ Sim | ✗ Não |

# AWS Cloud9

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Cloud9::Environment` | ✓ Sim | ✓ Sim | ✗ Não |

# AWS CloudFormation

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::CloudFormation::Stack` | ✓ Sim | ✓ Sim | ✓ Sim |

# Amazon CloudFront

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::CloudFront::Distribution` | ✓ Sim[1] | ✓ Sim[2] | ✓ Sim[2] |

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::CloudFront::StreamingDistribution` | ✓ Sim[1] | ✓ Sim[2] | ✓ Sim[2] |

[1] Este é um recurso para um serviço global que está hospedado na região Leste dos EUA (Norte da Virgínia). Para usar o Tag Editor para criar ou modificar tags para esse tipo de recurso, você deve incluir `us-east-1` na lista Selecionar regiões em Encontrar recursos para marcar no console do Tag Editor.

[2] Este é um recurso para um serviço global que está hospedado na região Leste dos EUA (Norte da Virgínia). Como os Resource Groups são mantidos separadamente para cada região, você deve mudar o seu AWS Management Console para Região da AWS aquele que contém os recursos que você deseja incluir no grupo. Para criar um grupo de recursos que contenha um recurso global, você deve configurar seu us-east-1 AWS Management Console para o Leste dos EUA (Norte da Virgínia) usando o seletor de região no canto superior direito do. AWS Management Console

# AWS Cloud Map

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::ServiceDiscovery::Service` | X Não | ✓ Sim | X Não |

# AWS CloudTrail

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::CloudTrail::Channel` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::CloudTrail::EventDataStore` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::CloudTrail::Trail` | ✓ Sim | ✓ Sim | ✓ Sim |

# Amazon CloudWatch

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::CloudWatch::Alarm` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::CloudWatch::Dashboard` | ✗ Não | ✗ Não | ✓ Sim |
| `AWS::CloudWatch::InsightRule` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::CloudWatch::MetricStream` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::CloudWatch::ServiceLevelObjective` | ✗ Não | ✓ Sim | ✗ Não |

## CloudWatch Registros da Amazon

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Logs::Destination` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::Logs::LogGroup` | ✗ Não | ✓ Sim | ✓ Sim |

## Amazon CloudWatch Synthetics

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Synthetics::Canary` | ✗ Não | ✓ Sim | ✓ Sim |

## AWS CodeArtifact

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::CodeArtifact::Domain` | ✓ Sim | ✓ Sim | ✓ Sim |

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::CodeArtifact::Repository` | ✓ Sim | ✓ Sim | ✓ Sim |

## AWS CodeBuild

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::CodeBuild::Project` | ✓ Sim | ✓ Sim | X Não |

## AWS CodeCommit

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::CodeCommit::Repository` | ✓ Sim | ✓ Sim | X Não |

# AWS CodeDeploy

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::CodeDeploy::Application` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::CodeDeploy::DeploymentConfig` | ✗ Não | ✗ Não | ✓ Sim |

# CodeGuru Revisor da Amazon

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::CodeGuruReviewer::RepositoryAssociation` | ✓ Sim | ✓ Sim | ✓ Sim |

# Amazon CodeGuru Profiler

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::CodeGuruProfiler::ProfilingGroup` | ✗ Não | ✓ Sim | ✗ Não |

# AWS CodePipeline

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::CodePipeline::CustomActionType` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::CodePipeline::Pipeline` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::CodePipeline::Webhook` | ✓ Sim | ✓ Sim | ✓ Sim |

# Conexões de código da AWS

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::CodeStarConnections::Connection` | ✗ Não | ✓ Sim | ✗ Não |

# Amazon Cognito

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Cognito::IdentityPool` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::Cognito::UserPool` | ✓ Sim | ✓ Sim | ✓ Sim |

# Amazon Comprehend

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Comprehend::DocumentClassifier` | ✓ Sim | ✓ Sim | ✗ Não |

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Comprehend::EntityRecognizer` | ✓ Sim | ✓ Sim | ✗ Não |

# AWS Config

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Config::AggregationAuthorization` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::Config::ConfigRule` | ✓ Sim | ✓ Sim | ✗ Não |
| `AWS::Config::ConfigurationAggregator` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::Config::StoredQuery` | ✗ Não | ✓ Sim | ✗ Não |

# Amazon Connect

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Connect::Instance` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::Connect::PhoneNumber` | ✗ Não | ✓ Sim | ✗ Não |

# Amazon Connect Wisdom

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Wisdom::Assistant` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::Wisdom::AssistantAssociation` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::Wisdom::Content` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::Wisdom::KnowledgeBase` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::Wisdom::Session` | ✗ Não | ✓ Sim | ✗ Não |

# AWS Data Exchange

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::DataExchange::DataSet` | ✓ Sim | ✓ Sim | ✗ Não |
| `AWS::DataExchange::Revision` | ✗ Não | ✓ Sim | ✗ Não |

# AWS Data Pipeline

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::DataPipeline::Pipeline` | ✓ Sim | ✓ Sim | ✓ Sim |

# AWS DataSync

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::DataSync::Task` | ✗ Não | ✓ Sim | ✗ Não |

# AWS Database Migration Service

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| AWS::DMS::Certificate | ✓ Sim | ✓ Sim | × Não |
| AWS::DMS::Endpoint | ✓ Sim | ✓ Sim | ✓ Sim |
| AWS::DMS::EventSubscription | ✓ Sim | ✓ Sim | × Não |
| AWS::DMS::ReplicationInstance | ✓ Sim | ✓ Sim | ✓ Sim |
| AWS::DMS::ReplicationSubnetGroup | ✓ Sim | ✓ Sim | × Não |
| AWS::DMS::ReplicationTask | ✓ Sim | ✓ Sim | × Não |

# AWS Device Farm

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| AWS::DeviceFarm::InstanceProfile | × Não | ✓ Sim | × Não |
| AWS::DeviceFarm::Project | × Não | ✓ Sim | × Não |
| AWS::DeviceFarm::TestGridProject | × Não | ✓ Sim | × Não |

# Amazon DynamoDB

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::DynamoDB::Table` | ✓ Sim | ✓ Sim | ✓ Sim |

# Amazon EMR

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::EMR::Cluster` | ✓ Sim | ✓ Sim | ✓ Sim |

# Contêineres do Amazon EMR

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::EMRContainers::JobRun` | X Não | ✓ Sim | X Não |
| `AWS::EMRContainers::VirtualCluster` | ✓ Sim | ✓ Sim | ✓ Sim |

# Amazon EMR Serverless

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::EMRServerless::Application` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::EMRServerless::JobRun` | ✗ Não | ✓ Sim | ✗ Não |

# Amazon ElastiCache

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::ElastiCache::CacheCluster` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::ElastiCache::ParameterGroup` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::ElastiCache::SecurityGroup` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::ElastiCache::Snapshot` | ✓ Sim | ✓ Sim | ✗ Não |
| `AWS::ElastiCache::SubnetGroup` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::ElastiCache::User` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::ElastiCache::UserGroup` | ✗ Não | ✓ Sim | ✗ Não |

# AWS Elastic Beanstalk

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::ElasticBeanstalk::Application` | ✓ Sim | ✓ Sim | × Não |
| `AWS::ElasticBeanstalk::ApplicationVersion` | × Não | ✓ Sim | × Não |
| `AWS::ElasticBeanstalk::ConfigurationTemplate` | × Não | ✓ Sim | × Não |
| `AWS::ElasticBeanstalk::Environment` | × Não | ✓ Sim | × Não |

# Amazon Elastic Compute Cloud (Amazon EC2)

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::EC2::CapacityReservation` | × Não | ✓ Sim | × Não |
| `AWS::EC2::CapacityReservationFleet` | × Não | ✓ Sim | × Não |
| `AWS::EC2::CarrierGateway` | × Não | ✓ Sim | × Não |
| `AWS::EC2::ClientVpnEndpoint` | × Não | ✓ Sim | × Não |
| `AWS::EC2::CoipPool` | × Não | ✓ Sim | × Não |

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| AWS::EC2::CustomerGateway | ✓ Sim | ✓ Sim | ✓ Sim |
| AWS::EC2::DHCPOptions | ✓ Sim | ✓ Sim | ✓ Sim |
| AWS::EC2::EC2Fleet | × Não | ✓ Sim | × Não |
| AWS::EC2::EgressOnlyInternetGateway | × Não | ✓ Sim | × Não |
| AWS::EC2::EIP | ✓ Sim | ✓ Sim | × Não |
| AWS::EC2::ExportImageTask | × Não | ✓ Sim | × Não |
| AWS::EC2::ExportInstanceTask | × Não | ✓ Sim | × Não |
| AWS::EC2::FlowLog | × Não | ✓ Sim | × Não |
| AWS::EC2::FpgaImage | × Não | ✓ Sim | × Não |
| AWS::EC2::Host | × Não | ✓ Sim | × Não |
| AWS::EC2::HostReservation | × Não | ✓ Sim | × Não |
| AWS::EC2::Image | ✓ Sim | ✓ Sim | × Não |
| AWS::EC2::ImportImageTask | × Não | ✓ Sim | × Não |
| AWS::EC2::ImportSnapshotTask | × Não | ✓ Sim | × Não |
| AWS::EC2::Instance | ✓ Sim | ✓ Sim | ✓ Sim |
| AWS::EC2::InstanceEventWindow | × Não | ✓ Sim | × Não |
| AWS::EC2::InternetGateway | ✓ Sim | ✓ Sim | ✓ Sim |

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| AWS::EC2::IPv4Pool | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::IPv6Pool | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::KeyPair | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::LaunchTemplate | ✗ Não | ✓ Sim | ✓ Sim |
| AWS::EC2::LocalGateway | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::LocalGatewayRouteTable | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::LocalGatewayRouteTableVirtualInterfaceGroupAssociation | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::LocalGatewayRouteTableVPCAssociation | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::LocalGatewayVirtualInterface | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::LocalGatewayVirtualInterfaceGroup | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::NatGateway | ✓ Sim | ✓ Sim | ✓ Sim |
| AWS::EC2::NetworkAcl | ✓ Sim | ✓ Sim | ✓ Sim |
| AWS::EC2::NetworkInsightsAccessScope | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::NetworkInsightsAccessScopeAnalysis | ✗ Não | ✓ Sim | ✗ Não |

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| AWS::EC2::NetworkInsightsAnalysis | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::NetworkInsightsPath | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::NetworkInterface | ✓ Sim | ✓ Sim | ✓ Sim |
| AWS::EC2::PlacementGroup | ✗ Não | ✓ Sim | ✓ Sim |
| AWS::EC2::PrefixList | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::ReplaceRootVolumeTask | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::ReservedInstance | ✓ Sim | ✓ Sim | ✗ Não |
| AWS::EC2::RouteTable | ✓ Sim | ✓ Sim | ✓ Sim |
| AWS::EC2::SecurityGroup | ✓ Sim | ✓ Sim | ✓ Sim |
| AWS::EC2::Snapshot | ✓ Sim | ✓ Sim | ✗ Não |
| AWS::EC2::SpotFleet | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::SpotInstanceRequest | ✓ Sim | ✓ Sim | ✗ Não |
| AWS::EC2::Subnet | ✓ Sim | ✓ Sim | ✓ Sim |
| AWS::EC2::SubnetCidrReservation | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::TrafficMirrorFilter | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::TrafficMirrorSession | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::TrafficMirrorTarget | ✗ Não | ✓ Sim | ✗ Não |

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| AWS::EC2::TransitGateway | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::TransitGatewayAttachment | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::TransitGatewayConnectPeer | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::TransitGatewayMulticastDomain | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::TransitGatewayPolicyTable | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::TransitGatewayRouteTable | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::TransitGatewayRouteTableAnnouncement | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::VerifiedAccessEndpoint | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::VerifiedAccessGroup | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::VerifiedAccessInstance | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::VerifiedAccessTrustProvider | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::Volume | ✓ Sim | ✓ Sim | ✓ Sim |
| AWS::EC2::VPC | ✓ Sim | ✓ Sim | ✓ Sim |
| AWS::EC2::VPCEndpoint | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::VPCEndpointConnection | ✗ Não | ✓ Sim | ✗ Não |
| AWS::EC2::VPCEndpointService | ✗ Não | ✓ Sim | ✗ Não |

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::EC2::VPCEndpointServicePermissions` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::EC2::VPCPeeringConnection` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::EC2::VPNConnection` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::EC2::VPNGateway` | ✓ Sim | ✓ Sim | ✓ Sim |

## Amazon Elastic Container Registry

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::ECR::Repository` | ✗ Não | ✓ Sim | ✗ Não |

# Amazon Elastic Container Service

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::ECS::CapacityProvider` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::ECS::Cluster` | ✓ Sim | ✓ Sim | ✗ Não |
| `AWS::ECS::ContainerInstance` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::ECS::Service` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::ECS::Task` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::ECS::TaskDefinition` | ✓ Sim | ✓ Sim | ✗ Não |
| `AWS::ECS::TaskSet` | ✗ Não | ✓ Sim | ✗ Não |

# Amazon Elastic File System

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::EFS::FileSystem` | ✓ Sim | ✓ Sim | ✓ Sim |

# Amazon Elastic Inference

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::ElasticInference::ElasticInferenceAccelerator` | ✓ Sim | ✓ Sim | ✗ Não |

# Amazon Elastic Kubernetes Service (Amazon EKS)

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::EKS::Addon` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::EKS::Cluster` | ✓ Sim | ✓ Sim | ✓ Sim |

# Elastic Load Balancing

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::ElasticLoadBalancing::LoadBalancer` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::ElasticLoadBalancingV2::Listener` | X Não | ✓ Sim | ✓ Sim |
| `AWS::ElasticLoadBalancingV2::ListenerRule` | X Não | ✓ Sim | ✓ Sim |
| `AWS::ElasticLoadBalancingV2::LoadBalancer` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::ElasticLoadBalancingV2::TargetGroup` | ✓ Sim | ✓ Sim | ✓ Sim |

# OpenSearch Serviço Amazon

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Elasticsearch::Domain` | ✓ Sim | ✓ Sim | ✓ Sim |

# CloudWatch Eventos da Amazon

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Events::EventBus` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::Events::Rule` | ✓ Sim | ✓ Sim | ✓ Sim |

> **Note**
>
> As regras em barramentos de eventos personalizados não são suportadas no Tag Editor.

# EventBridge Esquemas da Amazon

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::EventSchemas::Discoverer` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::EventSchemas::Registry` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::EventSchemas::Schema` | ✗ Não | ✓ Sim | ✗ Não |

# Amazon FSx

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::FSx::FileSystem` | ✓ Sim | ✓ Sim | × Não |
| `AWS::FSx::StorageVirtualMachine` | × Não | ✓ Sim | × Não |
| `AWS::FSx::Volume` | × Não | ✓ Sim | × Não |

# Amazon Forecast

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Forecast::Dataset` | ✓ Sim | ✓ Sim | × Não |
| `AWS::Forecast::DatasetGroup` | ✓ Sim | ✓ Sim | × Não |
| `AWS::Forecast::DatasetImportJob` | ✓ Sim | ✓ Sim | × Não |
| `AWS::Forecast::Forecast` | ✓ Sim | ✓ Sim | × Não |
| `AWS::Forecast::ForecastExportJob` | ✓ Sim | ✓ Sim | × Não |
| `AWS::Forecast::Predictor` | ✓ Sim | ✓ Sim | × Não |

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Forecast::PredictorBacktestExportJob` | ✓ Sim | ✓ Sim | X Não |

## Amazon Fraud Detector

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::FraudDetector::Detector` | ✓ Sim | ✓ Sim | X Não |
| `AWS::FraudDetector::DetectorVersion` | X Não | ✓ Sim | X Não |
| `AWS::FraudDetector::EntityType` | ✓ Sim | ✓ Sim | X Não |
| `AWS::FraudDetector::EventType` | ✓ Sim | ✓ Sim | X Não |
| `AWS::FraudDetector::ExternalModel` | ✓ Sim | ✓ Sim | X Não |
| `AWS::FraudDetector::Label` | ✓ Sim | ✓ Sim | X Não |
| `AWS::FraudDetector::Model` | ✓ Sim | ✓ Sim | X Não |
| `AWS::FraudDetector::ModelVersion` | X Não | ✓ Sim | X Não |
| `AWS::FraudDetector::Outcome` | ✓ Sim | ✓ Sim | X Não |
| `AWS::FraudDetector::Rule` | X Não | ✓ Sim | X Não |

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::FraudDetector::Variable` | ✓ Sim | ✓ Sim | X Não |

## Amazon GameLift

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::GameLift::Alias` | X Não | ✓ Sim | X Não |
| `AWS::GameLift::GameSessionQueue` | X Não | ✓ Sim | X Não |
| `AWS::GameLift::Location` | X Não | ✓ Sim | X Não |
| `AWS::GameLift::MatchmakingConfiguration` | X Não | ✓ Sim | X Não |
| `AWS::GameLift::MatchmakingRuleSet` | X Não | ✓ Sim | X Não |

# AWS Global Accelerator

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::GlobalAccelerator::Accelerator` | ✗ Não | ✓ Sim | ✗ Não |

# AWS Glue

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Glue::Crawler` | ✓ Sim | ✓ Sim | ✗ Não |
| `AWS::Glue::Database` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::Glue::Job` | ✓ Sim | ✓ Sim | ✗ Não |
| `AWS::Glue::MLTransform` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::Glue::Registry` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::Glue::Trigger` | ✓ Sim | ✓ Sim | ✗ Não |
| `AWS::Glue::Workflow` | ✗ Não | ✓ Sim | ✗ Não |

# AWS Glue DataBrew

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::DataBrew::Dataset` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::DataBrew::Job` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::DataBrew::Project` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::DataBrew::Recipe` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::DataBrew::Schedule` | ✓ Sim | ✓ Sim | ✓ Sim |

# AWS Ground Station

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::GroundStation::Config` | X Não | ✓ Sim | X Não |
| `AWS::GroundStation::DataflowEndpointGroup` | X Não | ✓ Sim | X Não |
| `AWS::GroundStation::MissionProfile` | X Não | ✓ Sim | X Não |

# Amazon GuardDuty

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::GuardDuty::Detector` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::GuardDuty::Filter` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::GuardDuty::IPSet` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::GuardDuty::ThreatIntelSet` | ✗ Não | ✓ Sim | ✗ Não |

# Amazon Interactive Video Service

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::IVS::Channel` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::IVS::RecordingConfiguration` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::IVS::StreamKey` | ✗ Não | ✓ Sim | ✗ Não |

# AWS Identity and Access Management

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::IAM::InstanceProfile` | ✓ Sim[1] | ✓ Sim[2] | ✗ Não |
| `AWS::IAM::ManagedPolicy` | ✓ Sim[1] | ✓ Sim[2] | ✗ Não |
| `AWS::IAM::OpenIDConnectProvider` | ✓ Sim[1] | ✓ Sim[2] | ✗ Não |
| `AWS::IAM::Role` | ✗ Não | ✗ Não | ✓ Sim[2] |
| `AWS::IAM::SAMLProvider` | ✓ Sim[1] | ✓ Sim[2] | ✗ Não |
| `AWS::IAM::ServerCertificate` | ✓ Sim[1] | ✓ Sim[2] | ✗ Não |
| `AWS::IAM::VirtualMFADevice` | ✓ Sim[1] | ✓ Sim[2] | ✗ Não |

[1] Este é um recurso para um serviço global que está hospedado na região Leste dos EUA (Norte da Virgínia). Para usar o Tag Editor para criar ou modificar tags para esse tipo de recurso, você deve incluir `us-east-1` na lista Selecionar regiões em Encontrar recursos para marcar no console do Tag Editor.

[2] Este é um recurso para um serviço global que está hospedado na região Leste dos EUA (Norte da Virgínia). Como os Resource Groups são mantidos separadamente para cada região, você deve mudar o seu AWS Management Console para Região da AWS aquele que contém os recursos que você deseja incluir no grupo. Para criar um grupo de recursos que contenha um recurso global, você deve configurar seu us-east-1 AWS Management Console para o Leste dos EUA (Norte da Virgínia) usando o seletor de região no canto superior direito do. AWS Management Console

# EC2 Image Builder

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::ImageBuilder::Component` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::ImageBuilder::ContainerRecipe` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::ImageBuilder::DistributionConfiguration` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::ImageBuilder::Image` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::ImageBuilder::ImagePipeline` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::ImageBuilder::ImageRecipe` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::ImageBuilder::InfrastructureConfiguration` | ✗ Não | ✓ Sim | ✗ Não |

# Amazon Inspector

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Inspector::AssessmentTemplate` | ✗ Não | ✓ Sim | ✓ Sim |

# AWS IoT

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| AWS::IoT::Authorizer | ✗ Não | ✓ Sim | ✗ Não |
| AWS::IoT::BillingGroup | ✗ Não | ✓ Sim | ✗ Não |
| AWS::IoT::CACertificate | ✗ Não | ✓ Sim | ✗ Não |
| AWS::IoT::CustomMetric | ✗ Não | ✓ Sim | ✗ Não |
| AWS::IoT::Dimension | ✗ Não | ✓ Sim | ✗ Não |
| AWS::IoT::JobTemplate | ✗ Não | ✓ Sim | ✗ Não |
| AWS::IoT::MitigationAction | ✗ Não | ✓ Sim | ✗ Não |
| AWS::IoT::Policy | ✗ Não | ✓ Sim | ✗ Não |
| AWS::IoT::RoleAlias | ✗ Não | ✓ Sim | ✗ Não |
| AWS::IoT::ScheduledAudit | ✗ Não | ✓ Sim | ✗ Não |
| AWS::IoT::SecurityProfile | ✗ Não | ✓ Sim | ✗ Não |
| AWS::IoT::ThingGroup | ✗ Não | ✓ Sim | ✗ Não |
| AWS::IoT::ThingType | ✗ Não | ✓ Sim | ✗ Não |
| AWS::IoT::TopicRule | ✗ Não | ✓ Sim | ✓ Sim |

# AWS IoT Analytics

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::IoTAnalytics::Channel` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::IoTAnalytics::Dataset` | ✓ Sim | ✓ Sim | ✗ Não |
| `AWS::IoTAnalytics::Datastore` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::IoTAnalytics::Pipeline` | ✗ Não | ✓ Sim | ✗ Não |

# AWS IoT Events

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::IoTEvents::AlarmModel` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::IoTEvents::DetectorModel` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::IoTEvents::Input` | ✓ Sim | ✓ Sim | ✓ Sim |

# AWS IoT FleetWise

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::IoTFleetWise::Campaign` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::IoTFleetWise::DecoderManifest` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::IoTFleetWise::Fleet` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::IoTFleetWise::ModelManifest` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::IoTFleetWise::SignalCatalog` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::IoTFleetWise::Vehicle` | ✗ Não | ✓ Sim | ✓ Sim |

# AWS IoT Greengrass

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Greengrass::ConnectorDefinition` | ✓ Sim | ✓ Sim | ✗ Não |
| `AWS::Greengrass::CoreDefinition` | ✓ Sim | ✓ Sim | ✗ Não |
| `AWS::Greengrass::DeviceDefinition` | ✓ Sim | ✓ Sim | ✗ Não |
| `AWS::Greengrass::FunctionDefinition` | ✓ Sim | ✓ Sim | ✗ Não |

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Greengrass::Group` | ✓ Sim | ✓ Sim | X Não |
| `AWS::Greengrass::LoggerDefinition` | ✓ Sim | ✓ Sim | X Não |
| `AWS::Greengrass::ResourceDefinition` | ✓ Sim | ✓ Sim | X Não |
| `AWS::Greengrass::SubscriptionDefinition` | ✓ Sim | ✓ Sim | X Não |

# AWS IoT Greengrass Version 2

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::GreengrassV2::ComponentVersion` | X Não | ✓ Sim | X Não |

# Console do AWS IoT SiteWise

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::IoTSiteWise::Asset` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::IoTSiteWise::AssetModel` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::IoTSiteWise::Dashboard` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::IoTSiteWise::Gateway` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::IoTSiteWise::Portal` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::IoTSiteWise::Project` | ✗ Não | ✓ Sim | ✗ Não |

# AWS IoT Wireless

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::IoTWireless::Destination` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::IoTWireless::DeviceProfile` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::IoTWireless::FuotaTask` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::IoTWireless::MulticastGroup` | ✗ Não | ✓ Sim | ✗ Não |

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::IoTWireless::NetworkAnalyzerConfiguration` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::IoTWireless::ServiceProfile` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::IoTWireless::TaskDefinition` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::IoTWireless::WirelessDevice` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::IoTWireless::WirelessGateway` | ✗ Não | ✓ Sim | ✗ Não |

## AWS Key Management Service

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::KMS::Alias` | ✗ Não | ✗ Não | ✓ Sim |
| `AWS::KMS::Key` | ✓ Sim | ✓ Sim | ✓ Sim |

# Amazon Keyspaces (para Apache Cassandra)

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Cassandra::Keyspace` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::Cassandra::Table` | ✗ Não | ✓ Sim | ✗ Não |

# Amazon Kinesis

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Kinesis::Stream` | ✓ Sim | ✓ Sim | ✓ Sim |

# Amazon Managed Service for Apache Flink

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::KinesisAnalytics::Application` | ✓ Sim | ✓ Sim | ✓ Sim |

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::KinesisAnalyticsV2::Application` | ✗ Não | ✗ Não | ✓ Sim |

## Amazon Data Firehose

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::KinesisFirehose::DeliveryStream` | ✗ Não | ✓ Sim | ✓ Sim |

## AWS Lambda

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Lambda::Alias` | ✗ Não | ✗ Não | ✓ Sim |
| `AWS::Lambda::EventSourceMapping` | ✗ Não | ✗ Não | ✓ Sim |
| `AWS::Lambda::Function` | ✓ Sim | ✓ Sim | ✓ Sim |

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| AWS::Lambda::LayerVersion | ✗ Não | ✗ Não | ✓ Sim |
| AWS::Lambda::Version | ✗ Não | ✗ Não | ✓ Sim |

## Amazon Lightsail

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| AWS::Lightsail::Bucket | ✗ Não | ✓ Sim | ✗ Não |
| AWS::Lightsail::Certificate | ✗ Não | ✓ Sim | ✗ Não |
| AWS::Lightsail::Container | ✗ Não | ✓ Sim | ✗ Não |
| AWS::Lightsail::Disk | ✗ Não | ✓ Sim | ✗ Não |
| AWS::Lightsail::Distribution | ✗ Não | ✓ Sim | ✗ Não |
| AWS::Lightsail::Instance | ✗ Não | ✓ Sim | ✗ Não |
| AWS::Lightsail::StaticIp | ✗ Não | ✓ Sim | ✗ Não |

# Amazon MQ

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::AmazonMQ::Broker` | ✓ Sim | ✓ Sim | ✗ Não |
| `AWS::AmazonMQ::Configuration` | ✓ Sim | ✓ Sim | ✗ Não |

# Amazon Macie

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Macie::ClassificationJob` | ✓ Sim | ✓ Sim | ✗ Não |
| `AWS::Macie::CustomDataIdentifier` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::Macie::FindingsFilter` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::Macie::Member` | ✓ Sim | ✓ Sim | ✗ Não |

# Amazon Managed Blockchain

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::ManagedBlockchain::Accessor` | ✗ Não | ✓ Sim | ✗ Não |

# Amazon Managed Streaming for Apache Kafka

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Kafka::Cluster` | ✓ Sim | ✓ Sim | ✗ Não |

# AWS Elemental MediaConnect

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::MediaConnect::Flow` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::MediaConnect::FlowEntitlement` | ✗ Não | ✓ Sim | ✗ Não |

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::MediaConnect::FlowOutput` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::MediaConnect::FlowSource` | ✗ Não | ✓ Sim | ✗ Não |

## AWS Elemental MediaPackage

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::MediaPackage::Channel` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::MediaPackage::PackagingConfiguration` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::MediaPackage::PackagingGroup` | ✗ Não | ✓ Sim | ✗ Não |

# AWS Network Manager

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::NetworkManager::CoreNetwork` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::NetworkManager::Device` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::NetworkManager::GlobalNetwork` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::NetworkManager::Link` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::NetworkManager::Site` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::NetworkManager::VpcAttachment` | ✗ Não | ✓ Sim | ✗ Não |

# OpenSearch Serviço Amazon OpenSearch

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::OpenSearchService::Domain` | ✓ Sim | ✓ Sim | ✓ Sim |

# AWS OpsWorks

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::OpsWorks::Instance` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::OpsWorks::Layer` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::OpsWorks::Stack` | ✗ Não | ✓ Sim | ✓ Sim |

# AWS Organizations

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Organizations::Account` | ✓ Sim | ✓ Sim | ✗ Não |
| `AWS::Organizations::OrganizationalUnit` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::Organizations::Policy` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::Organizations::Root` | ✓ Sim | ✓ Sim | ✗ Não |

# Amazon Pinpoint

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Pinpoint::App` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::Pinpoint::EmailTemplate` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::Pinpoint::PushTemplate` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::Pinpoint::SmsTemplate` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::Pinpoint::VoiceTemplate` | ✗ Não | ✓ Sim | ✗ Não |

# API de SMS e voz do Amazon Pinpoint

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::PinpointSMSVoiceV2::Pool` | ✗ Não | ✓ Sim | ✗ Não |

# Amazon Quantum Ledger Database (Amazon QLDB)

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::QLDB::Ledger` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::QLDB::Stream` | × Não | ✓ Sim | ✓ Sim |

# Amazon Redshift

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Redshift::Cluster` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::Redshift::ClusterParameterGroup` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::Redshift::ClusterSecurityGroup` | × Não | ✓ Sim | ✓ Sim |
| `AWS::Redshift::ClusterSubnetGroup` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::Redshift::DBGroup` | × Não | ✓ Sim | × Não |
| `AWS::Redshift::DBName` | × Não | ✓ Sim | × Não |
| `AWS::Redshift::DBUser` | × Não | ✓ Sim | × Não |
| `AWS::Redshift::EventSubscription` | × Não | ✓ Sim | × Não |

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| AWS::Redshift::HSMClientCertificate | ✓ Sim | ✓ Sim | ✗ Não |
| AWS::Redshift::HSMConfiguration | ✗ Não | ✓ Sim | ✗ Não |
| AWS::Redshift::Namespace | ✗ Não | ✓ Sim | ✗ Não |
| AWS::Redshift::Snapshot | ✗ Não | ✓ Sim | ✗ Não |
| AWS::Redshift::SnapshotCopyGrant | ✗ Não | ✓ Sim | ✗ Não |
| AWS::Redshift::SnapshotSchedule | ✗ Não | ✓ Sim | ✗ Não |
| AWS::Redshift::UsageLimit | ✗ Não | ✓ Sim | ✗ Não |

## Amazon Relational Database Service (Amazon RDS)

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| AWS::RDS::CustomDBEngineVersion | ✗ Não | ✓ Sim | ✗ Não |
| AWS::RDS::DBCluster | ✓ Sim | ✓ Sim | ✓ Sim |
| AWS::RDS::DBClusterEndpoint | ✗ Não | ✓ Sim | ✗ Não |
| AWS::RDS::DBClusterParameterGroup | ✓ Sim | ✓ Sim | ✓ Sim |

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| AWS::RDS::DBClusterSnapshot | ✓ Sim | ✓ Sim | × Não |
| AWS::RDS::DBInstance | ✓ Sim | ✓ Sim | ✓ Sim |
| AWS::RDS::DBParameterGroup | ✓ Sim | ✓ Sim | ✓ Sim |
| AWS::RDS::DBProxy | × Não | ✓ Sim | × Não |
| AWS::RDS::DBProxyEndpoint | × Não | ✓ Sim | × Não |
| AWS::RDS::DBProxyTargetGroup | × Não | ✓ Sim | × Não |
| AWS::RDS::DBSecurityGroup | ✓ Sim | ✓ Sim | ✓ Sim |
| AWS::RDS::DBSnapshot | ✓ Sim | ✓ Sim | × Não |
| AWS::RDS::DBSubnetGroup | ✓ Sim | ✓ Sim | ✓ Sim |
| AWS::RDS::Deployment | × Não | ✓ Sim | × Não |
| AWS::RDS::EventSubscription | ✓ Sim | ✓ Sim | × Não |
| AWS::RDS::OptionGroup | ✓ Sim | ✓ Sim | × Não |
| AWS::RDS::ReservedDBInstance | ✓ Sim | ✓ Sim | × Não |

# AWS Resource Access Manager

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::RAM::ResourceShare` | ✓ Sim | ✓ Sim | ✗ Não |

# AWS Resource Groups

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::ResourceGroups::Group` | ✓ Sim | ✓ Sim | ✓ Sim |

# AWS Robomaker

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::RoboMaker::DeploymentJob` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::RoboMaker::Fleet` | ✗ Não | ✓ Sim | ✗ Não |

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::RoboMaker::Robot` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::RoboMaker::RobotApplication` | ✓ Sim | ✓ Sim | ✗ Não |
| `AWS::RoboMaker::SimulationApplication` | ✓ Sim | ✓ Sim | ✗ Não |
| `AWS::RoboMaker::SimulationJob` | ✓ Sim | ✓ Sim | ✗ Não |

## Amazon Route 53

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Route53::Domain` | ✓ Sim[1] | ✓ Sim[2] | ✗ Não |
| `AWS::Route53::HealthCheck` | ✓ Sim[1] | ✓ Sim[2] | ✓ Sim[2] |
| `AWS::Route53::HostedZone` | ✓ Sim[1] | ✓ Sim[2] | ✓ Sim[2] |

[1] Este é um recurso para um serviço global que está hospedado na região Leste dos EUA (Norte da Virgínia). Para usar o Tag Editor para criar ou modificar tags para esse tipo de recurso, você deve incluir `us-east-1` na lista Selecionar regiões em Encontrar recursos para marcar no console do Tag Editor.

² Este é um recurso para um serviço global que está hospedado na região Leste dos EUA (Norte da Virgínia). Como os Resource Groups são mantidos separadamente para cada região, você deve mudar o seu AWS Management Console para Região da AWS aquele que contém os recursos que você deseja incluir no grupo. Para criar um grupo de recursos que contenha um recurso global, você deve configurar seu us-east-1 AWS Management Console para o Leste dos EUA (Norte da Virgínia) usando o seletor de região no canto superior direito do. AWS Management Console

## Amazon Route 53 Resolver

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Route53Resolver::FirewallDomainList` | ✗ Não | ✓ Sim² | ✗ Não |
| `AWS::Route53Resolver::FirewallRuleGroup` | ✗ Não | ✓ Sim² | ✗ Não |
| `AWS::Route53Resolver::FirewallRuleGroupAssociation` | ✗ Não | ✓ Sim² | ✗ Não |
| `AWS::Route53Resolver::ResolverEndpoint` | ✓ Sim¹ | ✓ Sim² | ✗ Não |
| `AWS::Route53Resolver::ResolverQueryLoggingConfig` | ✗ Não | ✓ Sim² | ✗ Não |
| `AWS::Route53Resolver::ResolverRule` | ✓ Sim¹ | ✓ Sim² | ✗ Não |

¹ Este é um recurso para um serviço global que está hospedado na região Leste dos EUA (Norte da Virgínia). Para usar o Tag Editor para criar ou modificar tags para esse tipo de recurso, você deve incluir `us-east-1` na lista Selecionar regiões em Encontrar recursos para marcar no console do Tag Editor.

² Este é um recurso para um serviço global que está hospedado na região Leste dos EUA (Norte da Virgínia). Como os Resource Groups são mantidos separadamente para cada região, você deve mudar o seu AWS Management Console para Região da AWS aquele que contém os recursos que você deseja incluir no grupo. Para criar um grupo de recursos que contenha um recurso global, você deve configurar seu us-east-1 AWS Management Console para o Leste dos EUA (Norte da Virgínia) usando o seletor de região no canto superior direito do. AWS Management Console

## Amazon S3 Glacier

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Glacier::Vault` | ✓ Sim | ✓ Sim | ✗ Não |

## Amazon SageMaker

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::SageMaker::AppImageConfig` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::SageMaker::CodeRepository` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::SageMaker::Endpoint` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::SageMaker::EndpointConfig` | ✗ Não | ✓ Sim | ✓ Sim |

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::SageMaker::HyperParameterTuningJob` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::SageMaker::Image` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::SageMaker::LabelingJob` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::SageMaker::Model` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::SageMaker::ModelPackageGroup` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::SageMaker::NotebookInstance` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::SageMaker::Pipeline` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::SageMaker::Project` | ✗ Não | ✓ Sim | ✓ Sim |
| `AWS::SageMaker::TrainingJob` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::SageMaker::TransformJob` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::SageMaker::Workteam` | ✗ Não | ✓ Sim | ✗ Não |

# AWS Secrets Manager

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::SecretsManager::Secret` | ✓ Sim | ✓ Sim | ✓ Sim |

# AWS Service Catalog

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::ServiceCatalog::CloudFormationProduct` | × Não | ✓ Sim | ✓ Sim |
| `AWS::ServiceCatalog::Portfolio` | × Não | ✓ Sim | ✓ Sim |

# AWS Service Catalog AppRegistry

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::ServiceCatalogAppRegistry::Application` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::ServiceCatalogAppRegistry::AttributeGroup` | ✗ Não | ✓ Sim | ✗ Não |

# Service Quotas

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::ServiceQuotas::Quota` | ✗ Não | ✓ Sim | ✗ Não |

# Amazon Simple Email Service

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::SES::ConfigurationSet` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::SES::ContactList` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::SES::DedicatedIpPool` | ✓ Sim | ✓ Sim | ✗ Não |
| `AWS::SES::Identity` | ✓ Sim | ✓ Sim | ✗ Não |

# Amazon Simple Notification Service

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::SNS::Topic` | ✓ Sim | ✓ Sim | ✓ Sim |

# Amazon Simple Queue Service

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::SQS::Queue` | ✓ Sim | ✓ Sim | ✓ Sim |

# Amazon Simple Storage Service (Amazon S3)

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::S3::Bucket` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::S3::Job` | X Não | ✓ Sim | X Não |
| `AWS::S3::StorageLens` | X Não | ✓ Sim | X Não |

# AWS Step Functions

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::StepFunctions::Activity` | ✓ Sim | ✓ Sim | ✓ Sim |
| `AWS::StepFunctions::StateMachine` | ✓ Sim | ✓ Sim | ✓ Sim |

# Storage Gateway

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::StorageGateway::Gateway` | ✓ Sim | ✓ Sim | X Não |
| `AWS::StorageGateway::Volume` | X Não | ✓ Sim | X Não |

# AWS Systems Manager

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| AWS::SSM::Association | ✗ Não | ✓ Sim | ✗ Não |
| AWS::SSM::AutomationExecution | ✗ Não | ✓ Sim | ✗ Não |
| AWS::SSM::Document | ✗ Não | ✓ Sim | ✓ Sim |
| AWS::SSM::MaintenanceWindow | ✗ Não | ✓ Sim | ✗ Não |
| AWS::SSM::ManagedInstance | ✗ Não | ✓ Sim | ✗ Não |
| AWS::SSM::OpsItem | ✗ Não | ✓ Sim | ✗ Não |
| AWS::SSM::OpsMetadata | ✗ Não | ✓ Sim | ✗ Não |
| AWS::SSM::Parameter | ✓ Sim | ✓ Sim | ✓ Sim |
| AWS::SSM::PatchBaseline | ✗ Não | ✓ Sim | ✓ Sim |

# AWS Systems Manager para SAP

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| AWS::SystemsManagerSAP::Application | ✗ Não | ✓ Sim | ✓ Sim |

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::SystemsManagerSAP::Database` | ✗ Não | ✓ Sim | ✗ Não |

## Amazon Timestream

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Timestream::ScheduledQuery` | ✗ Não | ✓ Sim | ✓ Sim |

## AWS Transfer Family

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Transfer::Certificate` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::Transfer::Connector` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::Transfer::Profile` | ✗ Não | ✓ Sim | ✗ Não |

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::Transfer::Workflow` | ✗ Não | ✓ Sim | ✗ Não |

## AWS WAF

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::WAF::Rule` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::WAF::WebACL` | ✗ Não | ✓ Sim | ✗ Não |

## Amazon WorkSpaces

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::WorkSpaces::Workspace` | ✓ Sim | ✓ Sim | ✓ Sim |

# AWS X-Ray

| Recursos | Marcação do Tag Editor | Grupos baseados em tags | AWS CloudFormation Grupos baseados em pilhas |
|---|---|---|---|
| `AWS::XRay::Group` | ✗ Não | ✓ Sim | ✗ Não |
| `AWS::XRay::SamplingRule` | ✗ Não | ✓ Sim | ✗ Não |

## Tipos de recursos descontinuados

Os seguintes tipos de recursos não são mais compatíveis com a funcionalidade especificada.

| Serviço | Tipo de atributo | Mudança de compatibilidade | Data |
|---|---|---|---|
| AWS RoboMaker | `AWS::RoboMaker::Robot` | Não é mais compatível com o Tag Editor. | 2 de maio de 2022 |
| AWS RoboMaker | `AWS::RoboMaker::Fleet` | Não é mais compatível com o Tag Editor. | 2 de maio de 2022 |
| AWS RoboMaker | `AWS::RoboMaker::DeploymentJob` | Não é mais compatível com o Tag Editor. | 2 de maio de 2022 |

# Criar grupos de recursos com o AWS CloudFormation

O AWS Resource Groups está integrado ao AWS CloudFormation, um serviço que ajuda você a modelar e configurar seus recursos da AWS para que você possa gastar menos tempo criando e gerenciando seus recursos e infraestrutura. Você cria um modelo que descreve todos os recursos da AWS desejados (como os grupos de recursos), e o AWS CloudFormation provisiona e configura esses recursos para você.

Quando você usa o AWS CloudFormation, é possível reutilizar seu modelo para configurar seus grupos de recursos repetidamente e de forma consistente. Descreva seus grupos de recursos uma vez e depois provisione os mesmos grupos de recursos repetidamente em várias regiões e Contas da AWS.

## Grupos de recursos e modelos do AWS CloudFormation

Para provisionar e configurar recursos para os Grupos 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 suas pilhas do AWS 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 AWS 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.

Os Grupos de recursos oferecem suporte à criação de grupos de recursos no AWS CloudFormation. Para obter mais informações, incluindo exemplos de modelos JSON e YAML para grupos de recursos, consulte a Referência de tipo de recurso do AWS Resource Groups no Manual do usuário do AWS CloudFormation.

## Saiba mais sobre o AWS CloudFormation

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

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

# Segurança em AWS Resource Groups

A segurança para com a nuvem na AWS é a nossa maior prioridade. Como cliente da AWS, você se contará com um datacenter e uma arquitetura de rede criados para atender aos requisitos das organizações com as maiores exigências de segurança.

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

- Segurança da nuvem: a AWS é responsável pela proteção da infraestrutura que executa produtos da AWS na Nuvem AWS. A AWS também fornece serviços que podem ser usados com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos programas de conformidade da AWS. Para saber mais sobre os programas de conformidade que se aplicam ao AWS Resource Groups, consulte Serviços da AWS no escopo pelo programa de conformidade.
- Segurança na nuvem: sua responsabilidade é determinada pelo serviço da AWS que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da sua empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda a entender como aplicar o modelo de responsabilidade compartilhada ao usar os Grupos de recursos. Os tópicos a seguir mostram como configurar os Grupos de recursos para atender aos seus objetivos de segurança e conformidade. Saiba também como usar outros produtos da AWS que ajudam a monitorar e proteger os recursos dos Grupos de recursos.

Tópicos

# Proteção de dados no AWS Resource Groups

O modelo de responsabilidade compartilhada da AWS se aplica à proteção de dados no AWS Resource Groups. Conforme descrito nesse modelo, a AWS é responsável por proteger a infraestrutura global que executa toda a 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 ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS.

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

- Use uma autenticação multifator (MFA [multi-factor authentication]) com cada conta.
- Use SSL/TLS para se comunicar com os recursos da AWS. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure o registro em log das atividades da API e do usuário com o AWS CloudTrail.
- Use as soluções de criptografia da AWS, juntamente com todos os controles de segurança padrão dos 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 módulos criptográficos validados pelo FIPS 140-2 ao acessar a AWS por meio de uma interface de linha de comando ou uma API, use um endpoint do FIPS. Para ter mais informações sobre endpoints do FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de email dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso se aplica inclusive quando você trabalha com os Grupos de recursos e outros Serviços da AWS usando o console, a API, a AWS CLI ou os SDKs da AWS. 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,

recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

## Criptografia de dados

Em comparação com outros produtos da AWS, o AWS Resource Groups tem uma superfície de ataque mínima, pois não fornece uma maneira de alterar, adicionar ou excluir recursos da AWS, exceto para grupos. Os Grupos de recursos coletam as seguintes informações específicas de serviço de você.

- Nomes de grupos (não criptografados, não privados)
- Descrições de grupos (não criptografadas, mas privadas)
- Recursos de membros em grupos (eles são armazenados em registros, que não são criptografados)

### Criptografia em repouso

Não há outras formas de isolar o tráfego de serviços ou de rede específicos para Grupos de recursos. Se aplicável, use isolamento específico da AWS. Você pode usar a API e o console dos grupos de recursos em uma VPC para ajudar a maximizar a privacidade e a segurança da infraestrutura.

### Criptografia em trânsito

Os dados do AWS Resource Groups são criptografados em trânsito para o banco de dados interno do serviço para backup. Isso não é configurável pelo usuário.

### Gerenciamento de chaves

O AWS Resource Groups atualmente não está integrado ao AWS Key Management Service e não oferece suporte a AWS KMS keys.

## Privacidade do tráfego entre redes

O AWS Resource Groups usa HTTPS para todas as transmissões entre usuários dos Grupos de recursos e AWS. Os Grupos de recursos usam o Transport Layer Security (TLS) 1.2, mas também são compatíveis com o TLS 1.0 e 1.1.

# Gerenciamento de identidade e acesso para AWS Resource Groups

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. Os administradores do IAM controlam quem pode ser autenticado (fazer login) e autorizado (ter permissões) para usar os recursos dos Grupos de recursos. O IAM é 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 em Resource Groups.

Usuário do serviço — Se você usa o serviço Grupos de recursos para fazer o trabalho, o administrador fornece as credenciais e as permissões necessárias. À medida que usar mais recursos dos Grupos de recursos para fazer seu trabalho, você poderá precisar 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 nos Grupos de recursos, consulte Solução de problemas AWS Resource Groups de identidade e acesso.

Administrador do serviço — Se você for o responsável pelos recursos dos Grupos de recursos na sua empresa, provavelmente terá acesso total aos recursos dos Grupos de recursos. Cabe a você determinar quais recursos e funcionalidades dos Grupos de recursos os usuários do serviço devem

acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com os Grupos de recursos, consulte Como os Grupos de recursos funcionam com o IAM.

Administrador do IAM: se você for um administrador do IAM, talvez queira saber detalhes sobre como é possível criar políticas para gerenciar o acesso aos Grupos de recursos. Para visualizar exemplos das políticas baseadas em identidades dos Grupos de recursos que podem ser usadas no IAM, consulte Exemplos de políticas baseadas em identidade do AWS Resource Groups.

## Autenticando com identidades

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

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (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 faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. 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 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 assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

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 do Usuário do AWS IAM Identity Center . Usar a autenticação multifator (MFA) na AWS no Guia do Usuário do IAM.

## 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 obter a lista completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do Usuário do IAM.

## Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos contar com credenciais temporárias em vez de criar usuários do IAM com 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 usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. 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 IAMAdmins e conceder a esse grupo permissões para administrar recursos do IAM.

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 usuário do IAM (em vez de um perfil) no Guia do usuário do IAM.

## Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando

uma URL personalizada. Para obter mais informações sobre métodos para o uso de perfis, consulte Utilizar perfis do IAM no Guia do usuário do IAM.

Funções do IAM 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 mais informações sobre perfis para federação, consulte Criar um perfil para um provedor de identidades de terceiros no Guia do Usuário do IAM. Se você usar o Centro de identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no Manual do Usuário do AWS IAM Identity Center .
- Permissões temporárias para usuários do IAM –- um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas –- é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta 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 perfis e políticas baseadas em recurso para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.
- 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 no 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 usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa 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. As solicitações do FAS 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 solicitações de FAS, consulte Encaminhar sessões de acesso.

  - Função de serviço: um perfil de serviço é um perfil do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criar um perfil para delegar permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
  - 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 administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.
- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para saber se deseja usar perfis do IAM, consulte Quando criar um perfil do IAM (em vez de um usuário) no Guia do usuário do IAM.

## 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 documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão geral das políticas JSON no Guia do Usuário do IAM.

Os administradores podem usar políticas AWS JSON 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 aos usuários permissões para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do

IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

As políticas do IAM definem permissões para uma ação independente do método usado para executar 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 da AWS Management Console AWS CLI, da ou da AWS API.

### Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. 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 Criando políticas do IAM no Guia do Usuário do IAM.

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 Escolher entre políticas gerenciadas e políticas em linha no Guia do Usuário do IAM.

### Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM 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 do IAM em uma política baseada em recursos.

## Listas de controle de acesso (ACLs)

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

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Para saber mais sobre ACLs, consulte Visão geral da lista de controle de acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

## 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 atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). 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 identidades do IAM no Guia do Usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON 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 atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte Como os SCPs Funcionam no Manual do Usuário do AWS Organizations .
- 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 do Usuário do IAM.

### 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 políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

## Como os Grupos de recursos funcionam com o IAM

Antes de usar o IAM para gerenciar o acesso aos Grupos de recursos, você precisa saber quais atributos do IAM estão disponíveis para uso com os Grupos de recursos. Para ter uma visão geral de como os Grupos de recursos e outros serviços da AWS funcionam com o IAM, consulte Serviços da AWS compatíveis com o IAM no Guia do usuário do IAM.

Tópicos

- Políticas baseadas em identidade dos Grupos de recursos
- Políticas baseadas em recursos
- Autorização baseada em tags dos Grupos de recursos
- Perfis do IAM dos Grupos de recursos

### Políticas baseadas em identidade dos Grupos de recursos

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, bem como as condições sob as quais as ações são permitidas ou negadas. Os Grupos de recursos são compatíveis com ações, recursos e chaves de condição específicos. Para conhecer todos os elementos usados em uma política JSON, consulte Referência de elementos de política JSON do IAM no Manual do usuário do IAM.

Ações

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

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome que a operação

de API da AWS associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Há também algumas operações que exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

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

As ações de políticas nos Grupos de recursos usam o seguinte prefixo antes da ação: `resource-groups:`. As ações do Tag Editor são executadas inteiramente no console, mas têm o prefixo `resource-explorer` nas entradas do log.

Por exemplo, para conceder permissão a alguém para criar um grupo de Grupos de recursos com a operação da API `CreateGroup` dos Grupos de recursos, inclua a ação `resource-groups:CreateGroup` na política. As instruções de política devem incluir um elemento `Action` ou `NotAction`. Os Grupos de recursos definem seu próprio conjunto de ações que descrevem as tarefas que você pode realizar com esse serviço.

Para especificar várias ações de Grupos de recursos e do Tag Editor em uma única declaração, separe-as com vírgulas, conforme o seguinte:

```
"Action": [
      "resource-groups:action1",
      "resource-groups:action2",
      "resource-explorer:action3"
```

Você também pode especificar várias ações usando caracteres curinga (*). Por exemplo, para especificar todas as ações que começam com a palavra `List`, inclua a seguinte ação:

```
"Action": "resource-groups:List*"
```

Para ver uma lista de ações de Grupos de recursos, consulte Ações, recursos e chaves de condição para o AWS Resource Groups no Manual do usuário do IAM.

Recursos

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

O elemento `Resource` de política JSON especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou um elemento `NotResource`. Como prática recomendada, especifique um recurso usando seu Nome do recurso da Amazon (ARN). Isso

pode ser feito para ações que oferecem suporte a um tipo de recurso específico, conhecido como permissões em nível de recurso.

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

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

O único recurso dos Grupos de recursos disponível é um grupo. O recurso de grupo tem o seguinte formato de ARN:

```
arn:${Partition}:resource-groups:${Region}:${Account}:group/${GroupName}
```

Para obter mais informações sobre o formato de ARNs, consulte Nomes de recursos da Amazon (ARNs) e namespaces de serviços da AWS.

Por exemplo, para especificar um grupo de recursos `my-test-group` na instrução, use o seguinte ARN:

```
"Resource": "arn:aws:resource-groups:us-east-1:123456789012:group/my-test-group"
```

Para especificar todos os grupos que pertencem a uma conta específica, use o caractere curinga (*):

```
"Resource": "arn:aws:resource-groups:us-east-1:123456789012:group/*"
```

Algumas ações dos Grupos de recursos, como as ações para a criação de recursos, não podem ser executadas em um recurso específico. Nesses casos, você deve usar o caractere curinga (*).

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

Algumas ações da API dos Grupos de recursos envolvem vários recursos. Por exemplo, `DeleteGroup` exclui grupos, portanto, uma entidade principal de chamada deve ter permissões para excluir um grupo específico ou todos os grupos. Para especificar vários recursos em uma única instrução, separe os ARNs com vírgulas.

```
"Resource": [
  "resource1",
```

```
  "resource2"
]
```

Para ver uma lista dos tipos de recursos dos Grupos de recursos e seus ARNs e saber com quais ações você pode especificar o ARN de cada recurso, consulte Ações, recursos e chaves de condição para o AWS Resource Groups no Manual do usuário do IAM.

Chaves de condição

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

O elemento `Condition` (ou bloco de `Condition`) permite que você especifique condições nas quais uma instrução está em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usam 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 elemento `Condition`, a AWS os avaliará usando uma operação lógica `AND`. Se você especificar vários valores para uma única chave de condição, a AWS avaliará a condição usando uma operação lógica `OR`. Todas as condições devem ser atendidas para que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar as condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um recurso somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte Elementos de política do IAM: variáveis e tags no Guia do usuário do IAM.

A AWS oferece suporte a chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição globais da AWS, consulte Chaves de contexto de condição globais da AWS no Guia do usuário do IAM.

Os Grupos de recursos definem seu próprio conjunto de chaves de condição e também oferecem suporte ao uso de algumas chaves de condição globais. Para ver todas as chaves de condição globais da AWS, consulte Chaves de contexto de condição globais da AWS no Manual do usuário do IAM.

Para ver uma lista de chaves de condição dos Grupos de recursos e saber com quais ações e recursos você pode usar uma chave de condição, consulte Ações, recursos e chaves de condição para o AWS Resource Groups no Manual do usuário do IAM.

Exemplos

Para ver exemplos das políticas baseadas em identidade dos Grupos de recursos, consulte Exemplos de políticas baseadas em identidade do AWS Resource Groups.

## Políticas baseadas em recursos

Os Grupos de recursos não oferecem suporte a políticas baseadas em recurso.

## Autorização baseada em tags dos Grupos de recursos

Você pode anexar tags a grupos em Grupos de recursos ou transmitir tags em uma solicitação para os Grupos de recursos. Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys` chaves de condição. Você pode aplicar tags a um grupo ao criar ou atualizar o grupo. Para obter mais informações sobre como marcar um grupo em Grupos de recursos, consulte Criação de grupos baseados em consultas no AWS Resource Groups e Atualizar grupos no AWS Resource Groups neste guia.

Para visualizar um exemplo de política baseada em identidade para limitar o acesso a um recurso baseado em tags desse recurso, consulte Visualizar grupos baseados em tags.

## Perfis do IAM dos Grupos de recursos

Perfil do IAM é uma entidade dentro da sua conta da AWS que tem permissões específicas. Grupos de recursos não têm nem usam perfis de serviço.

Uso de credenciais temporárias com Grupos de recursos

Nos Grupos de recursos, você pode usar credenciais temporárias para fazer login com federação, assumir um perfil do IAM ou assumir um perfil entre contas. As credenciais de segurança temporárias são obtidas chamando AWS STS operações da API como AssumeRole ou GetFederationToken.

Funções vinculadas ao serviço

Funções vinculadas ao serviço permitem que os serviços da AWS acessem recursos em outros serviços para concluir uma ação em seu nome.

Os Grupos de recursos não têm nem usam perfis vinculados a serviços.

Perfis de serviço

Esse recurso permite que um serviço assuma um perfil de serviço em seu nome.

Os Grupos de recursos não têm nem usam perfis de serviço.

## Políticas gerenciadas pela AWS para o AWS Resource Groups

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

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

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

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

Políticas gerenciadas pela AWS para Grupos de recursos

- ResourceGroupsServiceRolePolicy

### Política gerenciada pela AWS: ResourceGroupsServiceRolePolicy

Você não pode anexar a `ResourceGroupsServiceRolePolicy` a nenhuma entidade do IAM. Essa política é anexada a um perfil vinculado a serviços que permite que os Grupos de recursos realizem ações em seu nome. Para obter mais informações, consulte Usar perfis vinculados a serviços para Grupos de recursos.

Esta política concede as permissões necessárias para que os Grupos de recursos recuperem informações sobre os recursos em seus Grupos de recursos e quaisquer pilhas do AWS

CloudFormation às quais esses recursos pertençam. Isso permite que os Grupos de recursos gerem eventos do CloudWatch para o atributo de eventos do ciclo de vida do grupo.

Para ver a versão mais recente desta política gerenciada pela AWS, consulte `ResourceGroupsServiceRolePolicy` no console do IAM.

## Política gerenciada pela AWS: ResourceGroupsandTagEditorFullAccess

Ao anexar uma política a uma entidade principal, você atribui à entidade permissões que estão definidas na política. As políticas gerenciadas pela AWS facilitam a atribuição das devidas permissões a usuários, grupos e perfis em comparação à elaboração de suas próprias políticas.

Esta política concede as permissões necessárias para acesso total à funcionalidade de Grupos de recursos e Tag Editor.

Para ver a versão mais recente desta política gerenciada pela AWS, consulte `ResourceGroupsandTagEditorFullAccess` no console do IAM.

Para obter mais informações sobre essa política, consulte ResourceGroupsandTagEditorFullAccess no Guia de referência de políticas gerenciadas pela AWS.

## Política gerenciada pela AWS: ResourceGroupsandTagEditorReadOnlyAccess

Ao anexar uma política a uma entidade principal, você atribui à entidade permissões que estão definidas na política. As políticas gerenciadas pela AWS facilitam a atribuição das devidas permissões a usuários, grupos e perfis em comparação à elaboração de suas próprias políticas.

Esta política concede as permissões necessárias para acesso somente leitura à funcionalidade de Grupos de recursos e Tag Editor.

Para ver a versão mais recente desta política gerenciada pela AWS, consulte `ResourceGroupsandTagEditorReadOnlyAccess` no console do IAM.

Para obter mais informações sobre esta política, consulte ResourceGroupsandTagEditorReadOnlyAccess no Guia de referência de políticas gerenciadas pela AWS.

## Atualizações de Grupos de recursos para políticas gerenciadas pela AWS

Visualizar detalhes sobre as atualizações nas políticas gerenciadas pela AWS para Grupos de recursos 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 dos Grupos de recursos.

| Alteração | Descrição | Data |
| --- | --- | --- |
| Atualização da política — ResourceGroupsandTagEditorFullAccess | Grupos de recursos atualizou uma política para incluir mais permissões de AWS CloudFormation. | 10 de agosto de 2023 |
| Atualização da política — ResourceGroupsandTagEditorReadOnlyAccess | Grupos de recursos atualizou uma política para incluir mais permissões de AWS CloudFormation. | 10 de agosto de 2023 |
| Nova política — ResourceGroupsServiceRolePolicy | Grupos de recursos adicionou uma nova política para apoiar seu perfil vinculado a serviços. | 17 de novembro de 2022 |
| Os Grupos de recursos começaram a monitorar alterações | Grupos de recursos começaram a monitorar alterações nas suas políticas gerenciadas pela AWS. | 17 de novembro de 2022 |

## Usar perfis vinculados a serviços para Grupos de recursos

O AWS Resource Groups usa funções vinculadas ao serviço do AWS Identity and Access Management (IAM). O perfil vinculado a serviços é um tipo exclusivo de perfil do IAM vinculado diretamente aos Grupos de recursos. Os perfis vinculados ao serviço são predefinidos pelos Grupos de recursos e incluem todas as permissões que o serviço requer para chamar outros serviços da Serviços da AWS em seu nome.

Um perfil vinculado a serviços facilita a configuração dos Grupos de recursos porque você não precisa adicionar as permissões necessárias manualmente. Os Grupos de recursos define as permissões dos perfis vinculados a serviços e define políticas de confiança em cada uma, garantindo que somente o serviço dos Grupos de recursos possa assumir suas funções. As permissões

definidas incluem a política de confiança e a política de permissões, e essa política de permissões não pode ser anexada a nenhuma outra entidade do IAM.

Para obter informações sobre outros produtos que oferecem suporte às funções vinculadas a serviços, consulte AWS services that work with IAM (Serviços da AWS compatíveis com o IAM) e procure os serviços que apresentam Yes (Sim) na coluna Service-linked roles (Funções vinculadas a serviços). Escolha um Sim com um link para visualizar a documentação da função vinculada a esse serviço.

## Permissões de perfis vinculados a serviços para Grupos de recursos

Os Grupos de recursos usam perfis vinculados a serviços para dar suporte aos eventos do ciclo de vida do grupo. Escolha o link no nome do perfil para ver o perfil no console do IAM depois de criá-lo.

- `AWSServiceRoleForResourceGroups`

Os Grupos de recursos usam as permissões desse perfil para consultar os proprietários da Serviços da AWS de seus recursos para ajudar a resolver a associação ao grupo e manter o grupo atualizado. Ele permite que os Grupos de recursos emitam eventos relacionados a serviços para o serviço Amazon EventBridge.

O perfil vinculado a serviços `AWSServiceRoleForResourceGroups` confia somente no seguinte serviço para assumir o perfil:

- `resourcegroups.amazonaws.com`

As permissões anexadas ao perfil vêm da seguinte política gerenciada pela AWS. Escolha o link no nome da política para visualizar a política no console do IAM.

- `Políticas gerenciadas pela AWS para o AWS Resource Groups`

## Criar um perfil vinculado a serviços para Grupos de recursos

> **Important**
>
> Este perfil vinculado a serviços pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os atributos compatíveis com esse perfil. Para obter mais informações, consulte Um novo perfil apareceu em minha Conta da AWS.

Para criar o perfil vinculado a serviços, ative o atributo de eventos do ciclo de vida do grupo.

## Como editar um perfil vinculado a serviços para Grupos de recursos

Os Grupos de recursos não permitem editar o perfil vinculado a serviços AWSServiceRoleForResourceGroups. Depois que você criar uma função vinculada a serviço, não poderá alterar o nome da função, pois várias entidades podem fazer referência à função. No entanto, você poderá editar a descrição da função usando o IAM. Para ter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

## Como excluir um perfil vinculado a serviços para Grupos de recursos

Você pode excluir o perfil vinculado a serviços somente após desativar o atributo de eventos do ciclo de vida do grupo.

> **Important**
>
> - A AWS impede que você remova o perfil vinculado a serviços até que você primeiro desative o atributo de eventos do ciclo de vida do grupo que o criou.
> - Recomendamos que você não exclua o perfil vinculado a serviços, desde que tenha Grupos de recursos em sua Conta da AWS. O serviço dos Grupos de recursos não poderá interagir com outros Serviços da AWS para gerenciar seus grupos se você excluir esse perfil.

### Excluir manualmente a função vinculada ao serviço

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

#### Console

Para excluir o perfil vinculado a serviços dos grupos de serviço

1. Abra a página Perfis no console do IAM.
2. Encontre o perfil chamado AWSServiceRoleForResourceGroups e marque a caixa de seleção ao lado dele.
3. Escolha Delete (Excluir).

4. Confirme sua intenção de excluir o perfil inserindo o nome dele na caixa e, em seguida, escolha Excluir.

O perfil desaparece da sua lista de perfis no console do IAM.

AWS CLI

Para excluir o perfil vinculado a serviços dos grupos de serviço

Para excluir o perfil, digite o comando a seguir com os parâmetros exatamente como mostrados. Não substitua nenhum dos valores.

```
$ aws iam delete-service-linked-role \
    --role-name AWSServiceRoleForResourceGroups
{
    "DeletionTaskId": "task/aws-service-role/resource-groups.amazonaws.com/
AWSServiceRoleForResourceGroups/34e58943-e9a5-4220-9856-fc565EXAMPLE"
}
```

O comando retorna um ID de tarefa. A exclusão real do perfil ocorre de forma assíncrona. Você pode verificar o status da exclusão do perfil passando o identificador de tarefa fornecido para o seguinte comando da AWS CLI.

```
$ aws iam get-service-linked-role-deletion-status \
    --deletion-task-id "task/aws-service-role/resource-groups.amazonaws.com/
AWSServiceRoleForResourceGroups/34e58943-e9a5-4220-9856-fc565EXAMPLE"
{
    "Status": "SUCCEEDED"
}
```

### Regiões com suporte a perfis vinculados a serviços dos Grupos de recursos

Os Grupos de recursos oferecem suporte perfis vinculados a serviços em todas as Regiões da AWS em que o serviço estiver disponível. Para obter mais informações, consulte Regiões e endpoints do AWS.

## Exemplos de políticas baseadas em identidade do AWS Resource Groups

Por padrão, as entidades principais do IAM, como os usuários e as funções, não têm permissão para criar ou modificar recursos dos Grupos de recursos . Eles também não podem executar tarefas

usando o AWS Management Console, a AWS CLI ou AWS uma API. Um administrador do IAM deve criar políticas do IAM que concedam às entidades principais permissão para executar operações de API específicas nos recursos especificados de que elas precisam. O administrador deve anexar essas políticas às entidades principais que exigem essas permissões.

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 dos Grupos de recursos em 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 e a API dos Grupos de recursos

Para acessar o console do Tag Editor e do AWS Resource Groups, bem como a API, você deve ter um conjunto mínimo de permissões. Essas permissões dão autorização para que você liste e visualize detalhes sobre os recursos dos Grupos de recursos na sua conta da AWS. Se você criar uma política baseada em identidade mais restritiva do que as permissões mínimas requeridas, o console e os comandos da API não funcionarão conforme planejado para as entidades principais (usuários ou perfis do IAM) com essa política.

Para garantir que essas entidades ainda possam usar Grupos de recursos, anexe a seguinte política (ou uma política que contenha as permissões listadas na seguinte política) às entidades. Para obter mais informações, consulte Adição de permissões a um usuário no Manual do usuário do IAM:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "resource-groups:*",
```

```
        "cloudformation:DescribeStacks",
        "cloudformation:ListStackResources",
        "tag:GetResources",
        "tag:TagResources",
        "tag:UntagResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "resource-explorer:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

Para obter mais informações sobre como conceder acesso a Grupos de recursos, consulte Conceder permissões para usar um AWS Resource Groups Editor de tags neste guia.

## Permitir que os usuários 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": "*"
        }
    ]
}
```

## Visualizar grupos baseados em tags

Você pode usar condições em sua política baseada em identidade para controlar o acesso aos recursos dos Grupos de recursos baseados em tags. Este exemplo mostra como você pode criar uma política que permite visualizar um recurso; neste exemplo, um grupo de recursos. No entanto, a permissão é concedida somente se a tag do grupo `project` tiver o mesmo valor que a tag `project` anexada à entidade principal da chamada.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "resource-groups:ListGroups",
            "Resource": "arn:aws:resource-groups::region:account_ID:group/group_name"
        },
        {
            "Effect": "Allow",
            "Action": "resource-groups:ListGroups",
            "Resource": "arn:aws:resource-groups::region:account_ID:group/group_name",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/project": "${aws:PrincipalTag/
project}"}
            }
        }
    ]
}
```

Você pode anexar esta política às entidades principais na sua conta. Se uma entidade principal com a chave de tag `project` e o valor da tag `alpha` tentar visualizar um grupo de recursos, o grupo também deverá ser marcado como `project=alpha`. Caso contrário, o usuário terá o acesso negado. A chave da tag de condição `project` corresponde a `Project` e a `project` 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.

## Solução de problemas AWS Resource Groups de identidade e acesso

Use as seguintes informações para ajudar a diagnosticar e corrigir problemas comuns que podem ser encontrados ao trabalhar com os Grupos de recursos e o IAM.

Tópicos

- Não tenho autorização para executar uma ação nos Grupos de recursos
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha AWS conta acessem meus Resource Groups

### Não tenho autorização para executar uma ação nos Grupos 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. Caso seu administrador seja a pessoa que forneceu suas credenciais de início de sessão.

O erro de exemplo a seguir ocorre quando o usuário `mateojackson` tenta usar o console para visualizar detalhes sobre um grupo, mas não tem a permissão `resource-groups:ListGroups`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: resource-groups:ListGroups on resource: arn:aws:resource-groups::us-
west-2:123456789012:group/my-test-group
```

Neste caso, Mateo pede ao administrador para atualizar suas políticas para permitir a ele o acesso ao recurso `my-test-group` usando a ação `resource-groups:ListGroups`.

### Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não tem autorização para executar a ação `iam:PassRole`, as suas políticas deverão ser atualizadas para permitir a passagem de um perfil para os Grupos de recursos.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O erro de exemplo a seguir ocorre quando uma usuária do IAM chamada`marymajor` tenta usar o console para executar uma ação nos Grupos de recursos. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

## Quero permitir que pessoas fora da minha AWS conta acessem meus Resource Groups

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 os Grupos de recursos são compatíveis com esses atributos, consulte Como os Grupos de recursos funcionam com o 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 usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a recursos entre contas no IAM no Guia do usuário do IAM.

# Registrar em log e monitorar nos Grupos de recursos

Todas as ações do AWS Resource Groups são registradas no AWS CloudTrail.

## Registrar em log chamadas de API do AWS Resource Groups com o AWS CloudTrail

AWS Resource Groups e o Tag Editor são integrados ao AWS CloudTrail, serviço que fornece um registro das ações executadas por um usuário, perfil ou serviço da AWS nos Grupos de recursos ou no Tag Editor. O CloudTrail captura todas as chamadas de API para os Grupos de recursos como eventos, incluindo as chamadas do console dos Grupos de recursos ou do Tag Editor e de chamadas de código para APIs dos Grupos de recursos. Se você criar uma trilha, poderá habilitar a entrega contínua de eventos do CloudTrail para um bucket do Amazon S3, incluindo eventos para os Grupos de recursos. Se você não configurar uma trilha, ainda poderá visualizar os eventos mais recentes no console do CloudTrail em Event history (Histórico de eventos). Usando as informações coletadas pelo CloudTrail, é possível determinar a solicitação feita para os Grupos de recursos, o endereço IP no qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita, além de detalhes adicionais.

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

### Informações de Grupos de recursos no CloudTrail

O CloudTrail é habilitado em sua conta da AWS quando ela é criada. Quando ocorre uma atividade no console dos Grupos de recursos ou do Tag Editor, essa atividade é registrada em um evento do CloudTrail junto com outros eventos de produtos da AWS em Histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em sua conta da AWS. Para obter mais informações, consulte Como visualizar eventos com o histórico de eventos do CloudTrail.

Para ter um registro de eventos contínuo em sua conta da AWS, incluindo eventos dos Grupos 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. A trilha registra em log eventos de todas as regiões na partição da AWS e entrega os arquivos de log para o bucket do Amazon S3 especificado por você. Além disso, é possível

configurar outros serviços da AWS para analisar mais ainda mais e agir com base nos dados de eventos coletados nos logs do CloudTrail. Para obter mais informações, consulte:

- Visão geral da criação de uma trilha
- Serviços e integrações compatíveis com o CloudTrail
- Configurar notificações do Amazon SNS para o CloudTrail
- Receber arquivos de log do CloudTrail de várias regiões e receber arquivos de log do CloudTrail de várias contas

Todas as ações dos Grupos de recursos são registradas pelo CloudTrail e são documentadas na Referência de APIs do AWS Resource Groups. As ações dos Grupos de recursos no CloudTrail são mostradas como eventos com o endpoint da API `resource-groups.amazonaws.com` como fonte. Por exemplo, as chamadas para as APIs `CreateGroup`, `GetGroup` e `UpdateGroupQuery` geram entradas nos arquivos de log do CloudTrail. As ações do Tag Editor no console são registradas pelo CloudTrail e mostradas como eventos com o endpoint interno da API `resource-explorer` como fonte.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário raiz ou do usuário do IAM.
- Se a solicitação foi feita com credenciais de segurança temporárias de uma função ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte o Elemento `userIdentity` do CloudTrail.

## Noções básicas sobre as entradas de arquivos de log dos Grupos 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 origem 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 das chamadas de API pública. Dessa forma, eles não são exibidos em uma ordem específica.

O exemplo a seguir mostra uma entrada de log do CloudTrail que demonstra a ação `CreateGroup`.

```
{"eventVersion":"1.05",
"userIdentity":{
    "type":"AssumedRole",
    "principalId":"ID number:AWSResourceGroupsUser",
    "arn":"arn:aws:sts::831000000000:assumed-role/Admin/AWSResourceGroupsUser",
    "accountId":"831000000000","accessKeyId":"ID number",
    "sessionContext":{
        "attributes":{
            "mfaAuthenticated":"false",
            "creationDate":"2018-06-05T22:03:47Z"
            },
        "sessionIssuer":{
            "type":"Role",
            "principalId":"ID number",
            "arn":"arn:aws:iam::831000000000:role/Admin",
            "accountId":"831000000000",
            "userName":"Admin"
            }
        }
    },
"eventTime":"2018-06-05T22:18:23Z",
"eventSource":"resource-groups.amazonaws.com",
"eventName":"CreateGroup",
"awsRegion":"us-west-2",
"sourceIPAddress":"100.25.190.51",
"userAgent":"console.amazonaws.com",
"requestParameters":{
    "Description": "EC2 instances that we are using for application staging.",
    "Name": "Staging",
    "ResourceQuery": {
      "Query": "string",
      "Type": "TAG_FILTERS_1_0"
      },
    "Tags": {
      "Key":"Phase",
      "Value":"Stage"
      }
    },
"responseElements":{
    "Group": {
      "Description":"EC2 instances that we are using for application staging.",
      "groupArn":"arn:aws:resource-groups:us-west-2:831000000000:group/Staging",
      "Name":"Staging"
```

```
     },
    "resourceQuery": {
      "Query":"string",
      "Type":"TAG_FILTERS_1_0"
     }
    },
"requestID":"de7z64z9-d394-12ug-8081-7zz0386fbcb6",
"eventID":"8z7z18dz-6z90-47bz-87cf-e8346428zzz3",
"eventType":"AwsApiCall",
"recipientAccountId":"831000000000"
}
```

# Validação de conformidade para Grupos de recursos

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

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

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

  > **Note**
  >
  > Nem todos Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte a Referência dos serviços qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.

- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

## Resiliência nos Grupos de recursos

O AWS Resource Groups executa backups automatizados nos recursos de serviços internos. Esses backups não são configuráveis pelo usuário. Os backups são criptografados, em repouso e em trânsito. Os Grupos de recursos armazenam dados de clientes no Amazon DynamoDB.

A infraestrutura global da AWS se baseia em Regiões da AWS e zonas de disponibilidade. A Regiões da AWS oferece várias zonas de disponibilidade separadas e isoladas fisicamente que são conectadas com baixa latência, altas taxas de throughput e em redes altamente redundantes. Com as zonas de disponibilidade, você pode projetar e operar aplicações e bancos de dados que executam o failover automaticamente entre as zonas de disponibilidade sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center tradicionais.

Mesmo a perda total dos grupos de recursos do usuário não resultaria na perda de dados do cliente, porque a maioria dos dados do cliente é replicada em zonas de disponibilidade (AZs) da AWS. Se você excluir grupos acidentalmente, entre em contato com a Central do AWS Support.

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

## Segurança da infraestrutura nos Grupos de recursos

Não há outras formas de isolar o tráfego de serviço ou rede fornecido pelos Grupos de recursos. Se aplicável, use isolamento específico da AWS. Você pode usar a API e o console dos grupos de recursos em uma VPC para ajudar a maximizar a privacidade e a segurança da infraestrutura.

Por ser um serviço gerenciado, o AWS Resource Groups é protegido pela segurança da rede global da AWS. Para obter informações sobre serviços de segurança da AWS e como a AWS protege a infraestrutura, consulte Segurança na Nuvem AWS. Para projetar seu ambiente da AWS usando as práticas recomendadas de segurança de infraestrutura, consulte Proteção de infraestrutura em Pilar segurança: AWS Well-Architected Framework.

Você usa chamadas de API publicadas pela AWS para acessar os Grupos de recursos por meio da rede. Os clientes devem oferecer suporte para:

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

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

Os Grupos de recursos não oferecem suporte a políticas baseadas em recurso.

# Melhores práticas de segurança para os Grupos de recursos

As práticas recomendadas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas práticas recomendadas podem não ser adequadas ou suficientes no seu ambiente, trate-as como considerações úteis em vez de requisitos.

- Use o princípio de privilégio mínimo para conceder acesso aos grupos. Grupos de recursos são compatíveis com permissões no nível do recurso. Conceda acesso a grupos específicos somente conforme necessário para usuários específicos. Evite usar asteriscos em declarações de política que atribuam permissões a todos os usuários ou a todos os grupos. Para obter mais informações sobre privilégios mínimos, consulte Conceder privilégio mínimo no Guia do usuário do IAM.
- Mantenha as informações privadas fora dos campos públicos. O nome de um grupo é tratado como metadados do serviço. Os nomes dos grupos não são criptografados. Não coloque informações confidenciais nos nomes dos grupos. As descrições dos grupos são privadas.

  Não coloque informações privadas ou confidenciais nas chaves ou valores das tags.
- Use a autorização com base na marcação sempre que apropriado. Os Grupos de recursos aceitam autorização baseada em tags. Você pode marcar grupos e, em seguida, atualizar as políticas anexadas às suas entidades principais do IAM, como usuários e funções, para definir o nível de acesso com base nas tags aplicadas a um grupo. Para obter mais informações sobre usar autorização baseada em tags de recurso, consulte Controlar o acesso a recursos da AWS usando tags de recurso no Guia do usuário do IAM.

  Muitos produtos da AWS oferecem suporte à autorização baseada em tags para seus recursos. Esteja ciente de que a autorização baseada em tags pode ser configurada para recursos de membros em um grupo. Se o acesso aos recursos de um grupo for restrito por tags, usuários ou grupos não autorizados talvez não consigam realizar ações ou automações nesses recursos. Por exemplo, se uma instância do Amazon EC2 em um de seus grupos estiver marcada com uma chave de tag de `Confidentiality` e um valor de tag de `High`, e você não estiver autorizado a executar comandos em recursos marcados como `Confidentiality:High`, as ações ou as automações que você executa na instância do EC2 falharão, mesmo que as ações sejam bem-sucedidas para outros recursos no grupo de recursos. Para obter mais informações sobre quais serviços oferecem suporte à autorização baseada em tags para seus recursos, consulte Produtos da AWS que funcionam com o IAM no Guia do usuário do IAM.

  Para obter mais informações sobre como desenvolver uma estratégia de marcação para seus produtos da AWS, consulte Estratégias de marcação da AWS.

# Cotas de serviço para grupos de recursos

A tabela a seguir descreve os limites no AWS Resource Groups (Grupos de recursos). É possível solicitar o aumento de alguns desses limites. Para solicitar um aumento de limite, acesse o console Service Quotas. Para ter informações sobre os limites que podem ser alterados, consulte Service Quotas.

> **Note**
>
> As seguintes definições se aplicam à descrição das cotas abaixo:
>
> - Grupo de recursos — Um conjunto de recursos da AWS que estão na mesma Região da AWS e atendem aos critérios especificados na consulta do grupo.

| Recurso | Limite padrão |
| --- | --- |
| Número máximo de recursos por grupo por Conta da AWS por Região da AWS | 100 |

# Referência do AWS Resource Groups

Use os tópicos nesta seção para localizar informações de referência para diversos aspectos do AWS Resource Groups.

## Service Quotas para Grupos de recursos

| Nome | Padrão | Ajustá | Descrição |
| --- | --- | --- | --- |
| Grupos de recurso por conta | Cada região compatível: 100 | Yes (Sim) | O número máximo de grupos de recursos que podem ser criados nesta conta. Um grupo de recursos é uma coleção de recursos da AWS que correspondem a um critério específico. |

> **Note**
>
> Você pode solicitar alterações nas cotas marcadas como ajustáveis usando a página do AWS Resource Groups no console Service Quotas.

## Políticas gerenciadas da AWS disponíveis para uso com o AWS Resource Groups

As políticas de permissão do IAM gerenciadas pela AWS permitem que você conceda permissões pré-configuradas às entidades principais do IAM, como perfis e usuários, em sua conta. As políticas gerenciadas da AWS são testadas e seguem as recomendações de melhores práticas, para que você possa usá-las de forma confiável nos cenários para os quais elas foram definidas. À medida que novos tipos de recursos são aceitos como membros de grupos de recursos e à medida que novos tipos de recursos oferecem suporte à marcação, a AWS automatiza automaticamente essas políticas para apoiá-las. Você não precisa fazer nada.

A tabela a seguir lista as políticas de permissão do IAM gerenciadas pela AWS disponíveis para você usar para conceder permissões a AWS Resource Groups.

| Nome da política e ARN | Descrição |
| --- | --- |
| AWSResourceGroupsReadOnlyAccess<br><br>`arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess` | Concede acesso somente leitura ao Console de Gerenciamento do AWS Resource Groups. Inclui permissão para visualizar os detalhes de um recurso, incluindo a lista de tags anexadas. Esta política não concede permissão para fazer alterações em grupos de recursos ou tags. |
| ResourceGroupsandTagEditorReadOnlyAccess<br><br>`arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess` | Concede acesso somente leitura ao Console de Gerenciamento do AWS Resource Groups, incluindo o Tag Editor. Inclui permissão para visualizar os detalhes de um recurso, incluindo suas tags. Você pode usar o Tag Editor para visualizar recursos que correspondem às consultas de tags. Esta política não concede permissão para fazer alterações em grupos de recursos ou tags. |
| ResourceGroupsandTagEditorFullAccess<br><br>`arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess` | Concede acesso administrativo total ao console de gerenciamento do AWS Resource Groups. Ele inclui permissões para visualizar, criar e modificar grupos de recursos. Também inclui permissões para visualizar, definir e modificar tags para quaisquer recursos compatíveis com o Tag Editor. |

# AWS Resource Groups histórico do documento

| Alteração | Descrição | Data |
| --- | --- | --- |
| Suporte para mais tipos de recursos | Agora, mais tipos de recursos são suportados pelo Resource Groups e pelo Tag Editor. | 30 de maio de 2024 |
| Políticas AWS ResourceGroupsandTagEditorFullAccess gerenciadas atualizadas e ResourceGroupsandTagEditorReadOnlyAccess | O Resource Groups atualizou duas políticas AWS gerenciadas para adicionar mais AWS CloudFormation permissões. | 10 de agosto de 2023 |
| Service Quotas para Grupos de recursos | Agora você pode ver os limites de cota dos Grupos de recursos usando o Service Quotas. | 29 de junho de 2023 |
| Atualização das práticas recomendadas do IAM | Guia atualizado para alinhamento com as práticas recomendadas do IAM. Para obter mais informações, consulte Práticas recomendadas de segurança no IAM. | 3 de janeiro de 2023 |
| As informações do Tag Editor foram movidas para seu próprio guia | A documentação do Tag Editor foi removida deste guia e movida para o novo Guia do usuário do Tag Editor. | 13 de dezembro de 2022 |
| Os grupos de recurso agora podem incluir recursos do Amazon Keyspaces (para Apache Cassandra) | AWS Resource Groups agora suporta a inclusão de recursos para Amazon Keyspaces (para Apache Cassandra) em um grupo de recursos. | 20 de outubro de 2022 |

| | | |
|---|---|---|
| Depreciação de tipos de recursos | Os seguintes tipos de recursos não são mais compatíveis com o Tag Editor: `AWS::RoboMaker::Robot` , `AWS::RoboMaker::Fleet` e `AWS::RoboMaker::DeploymentJob` . | 17 de maio de 2022 |
| Nova política AWS gerenciada - ResourceGroupsServiceRolePolicy | Os Resource Groups adicionaram uma nova política AWS gerenciada no AWS Identity and Access Management (IAM) para dar suporte à função vinculada ao serviço do serviço. | 12 de janeiro de 2022 |
| Eventos do ciclo de vida do grupo | Agora, os Resource Groups podem gerar CloudWatch eventos no Amazon Events para alertá-lo quando ocorrerem alterações em seus grupos de recursos. | 12 de janeiro de 2022 |
| Grupos de recursos agora podem ser usados pelo Amazon VPC Network Access Analyzer para monitorar tráfego de rede indesejado para seus recursos. AWS | Você pode usar AWS Resource Groups para especificar as fontes e os destinos para seus requisitos de acesso à rede. | 3 de dezembro de 2021 |
| Suporte adicional para recursos do AWS Resilience Hub | AWS Resource Groups agora suporta a inclusão de recursos para o AWS Resilience Hub em um grupo de recursos. | 18 de novembro de 2021 |

| | | |
|---|---|---|
| Suporte adicional para recursos do Amazon Pinpoint | AWS Resource Groups agora suporta a inclusão de recursos para o Amazon Pinpoint em um grupo de recursos. | 11 de novembro de 2021 |
| Foi adicionado suporte para grupos de recursos que são configurados e gerenciados pelo AppRegistry | AWS Resource Groups agora oferece suporte a grupos de recursos que contêm configurações de serviço para recursos em aplicativos que você cria usando AWS Service Catalog AppRegistry. Para mais informações, consulte Configurações de serviço na Referência da API AWS Resource Groups . | 15 de setembro de 2021 |
| Suporte adicional para recursos do Amazon OpenSearch Service | AWS Resource Groups agora suporta a inclusão de recursos para o Amazon OpenSearch Service em um grupo de recursos. | 11 de agosto de 2021 |
| Adicionado suporte para recursos do AWS Braket | AWS Resource Groups agora suporta a inclusão de recursos para AWS Braket em um grupo de recursos. | 30 de junho de 2021 |
| Suporte adicional para recursos de contêineres do Amazon EMR | AWS Resource Groups agora suporta a inclusão de recursos para contêineres do Amazon EMR em um grupo de recursos. | 27 de abril de 2021 |

| | | |
|---|---|---|
| Suporte adicional para recursos de AWS serviços adicionais | AWS Resource Groups agora suporta a inclusão de recursos para os seguintes serviços em um grupo de recursos: Amazon CodeGuru Reviewer, Amazon Elastic Inference, Amazon Forecast, Amazon Fraud Detector e Service Quotas. | 25 de fevereiro de 2021 |
| Capítulo adicional sobre segurança e conformidade. | Discute como os Grupos de recursos protegem suas informações e se mantêm em conformidade com os padrões normativos. | 30 de julho de 2020 |

| | | |
|---|---|---|
| Suporte adicional para grupos de recursos configurados para produtos da AWS | Agora você pode criar grupos de recursos associados a um AWS serviço e configurar como o serviço pode interagir com os recursos que estão no grupo. Nesta primeira versão do atributo, você pode criar um grupo de recursos que contém reservas de capacidad e do Amazon EC2 e, em seguida, iniciar instâncias do Amazon EC2 no grupo. Se houver capacidade em uma ou mais reservas do grupo que corresponda à sua instância, essa instância usará a reserva. Se a instância não corresponder a nenhuma reserva disponível no grupo, ela será executada como uma instância sob demanda. Para obter mais informaçõ es, consulte Como trabalhar com grupos de reserva de capacidade no Guia do usuário do Amazon EC2. | 29 de julho de 2020 |
| Foi adicionado suporte para AWS IoT Greengrass recursos. | Agora, mais tipos de recursos são compatíveis com AWS Resource Groups o Tag Editor. | 25 de março de 2020 |

| | | |
|---|---|---|
| Exibir dados de operações para AWS Resource Groups | No AWS Systems Manager console, a AWS Resource Groups página exibe os dados de operações de um grupo selecionado em quatro guias: Details, Config CloudTrail,,. OpsItems Essas guias não estão disponíveis ao visualiza r um grupo no console Grupos de recursos. Você pode usar as informações nessas guias para ajudar a entender quais recursos em um grupo estão em conformidade e funcionan do corretamente, e quais recursos exigem ação. Se precisar agir em um recurso, você poderá usar registros do Systems Manager Automation para executar tarefas comuns de operações de manutençã o e solução de problemas. Para obter mais informaçõ es, consulte Visualização de dados de operações para AWS Resource Groups no Guia de usuário do AWS Systems Manager . | 16 de março de 2020 |
| Verifique a conformidade com as políticas de tags | Depois de criar e anexar políticas de tags às contas que usam AWS Organizations, você pode encontrar tags não compatíveis em recursos nas contas da sua organização. | 26 de novembro de 2019 |

| | | |
|---|---|---|
| Suporte para mais tipos de recursos | Agora, mais tipos de recursos são compatíveis com AWS Resource Groups o Tag Editor. | 4 de outubro de 2019 |
| Novos tipos de recursos suportados pelo AWS Resource Groups | Agora, mais tipos de recursos são suportados pelo AWS Resource Groups, especialmente para grupos baseados em uma AWS CloudFormation pilha. | 5 de agosto de 2019 |
| Novos tipos de recursos suportados pelo AWS Resource Groups | As APIs REST do Amazon API Gateway, CloudWatch os eventos do Amazon Events e os tópicos do Amazon SNS agora são tipos de recursos compatíveis em. AWS Resource Groups | 27 de junho de 2019 |
| O Tag Editor agora suporta a localização de recursos não marcados | Agora, você pode pesquisar recursos no Tag Editor que não tenham valores de tag aplicados a uma chave de tag específica. | 18 de junho de 2019 |
| Novos tipos de recursos compatíveis com AWS Resource Groups o Tag Editor | Mais de 50 novos tipos de recursos foram adicionados AWS Resource Groups e o suporte ao Editor de tags. | 6 de junho de 2019 |

| | | |
|---|---|---|
| AWS Resource Groups e o console do Tag Editor sai do AWS Systems Manager console | O console AWS Resource Groups e o Tag Editor agora é independente do console do Systems Manager. Embora você ainda possa encontrar ponteiros para o AWS Resource Groups console na barra de navegação esquerda do Systems Manager, você pode abrir o console do Resource Groups and Tag Editor diretamente do menu suspenso no canto superior esquerdo do. AWS Management Console | 5 de junho de 2019 |
| Novos recursos de autorização e controle de acesso dos Grupos de recursos | Os Grupos de recursos agora oferecem suporte a políticas baseadas em ação, permissões no nível de recurso e autorização com base em tags. | 24 de maio de 2019 |
| Grupos de recursos e ferramentas de Tag Editor herdados mais antigos não estão mais disponíveis | Menções sobre Grupos de recursos e Tag Editor mais antigos, clássicos ou herdados foram removidas. Essas ferramentas não estão mais disponíveis na AWS. Em vez disso, use AWS Resource Groups um editor de tags. | 14 de maio de 2019 |

| | | |
|---|---|---|
| O Tag Editor agora é compatível com recursos de marcação em várias regiões | O Tag Editor agora permite pesquisar e gerenciar tags de recursos em várias regiões, com sua região atual adicionada às consultas de recursos por padrão. | 2 de maio de 2019 |
| O Tag Editor agora é compatível com a exportação dos resultados da consulta para um CSV | Você pode exportar os resultados de uma consulta na página Localizar recursos a serem marcados para um arquivo em formato CSV. Uma nova coluna Região é mostrada nos resultados de consultas do Tag Editor. O Tag Editor agora permite pesquisar recursos que têm valores vazios para uma determinada chave de tag. Os valores de chaves de tags são preenchidos automaticamente conforme você digita um valor exclusivo entre chaves existentes. | 2 de abril de 2019 |

| | | |
|---|---|---|
| O Tag Editor agora é compatível com a adição de todos os tipos de recurso a uma consulta | Você pode aplicar tags a até 20 tipos de recurso individuais em uma única operação, ou escolher Todos os tipos de recurso para consultar todos os tipos de recurso em uma região. O preenchimento automático foi adicionado ao campo Chave de tag de uma consulta para ajudar a habilitar chaves de tags consistentes entre recursos. Se as alterações de tags falharem em alguns recursos, você poderá tentar novamente as alterações de tags apenas nos recursos nos quais as alterações de tags falharam. | 19 de março de 2019 |
| O Tag Editor agora oferece suporte a vários tipos de recurso em uma pesquisa | Você pode aplicar tags a até 20 tipos de recurso em uma única operação. Você também pode escolher as colunas que são mostradas nos resultados de pesquisa, incluindo colunas para cada chave de tag exclusiva encontradas nos resultados da pesquisa ou recursos selecionados dos resultados. | 26 de fevereiro de 2019 |
| Documentação adicionada para o novo Tag Editor | A seção “Trabalhando com o Tag Editor” descreve como usar a nova experiência do console do AWS Tag Editor. | 13 de fevereiro de 2019 |

| | | |
|---|---|---|
| Novos tipos de recurso compatíveis com grupos nos Grupos de recursos | Adicionados novos tipos de recurso que agora são compatíveis nos grupos de recursos. | 4 de fevereiro de 2019 |
| Experiência do usuário avançada para adicionar tags a consultas dos Grupos de recursos baseados em tags | Pequenas alterações na experiência do usuário do console para adição de tags em uma consulta baseada em tag. | 17 de dezembro de 2018 |
| AWS CloudFormation suporte de consulta baseado em pilha adicionado ao Resource Groups | Você pode criar grupos de recursos nos quais a consulta é baseada em uma AWS CloudFormation pilha. Depois de escolher uma pilha, você pode escolher quais tipos de recurso da pilha você deseja que sejam exibidos na consulta do grupo. | 13 de novembro de 2018 |
| Resource Groups e CloudTrail | O Resource Groups agora oferece AWS CloudTrai l suporte. Você pode ver e trabalhar com registros de todas as chamadas da API Resource Groups em CloudTrail. | 29 de junho de 2018 |

- Versão da API: 2017-11-27
- Última atualização da documentação: 24 de setembro de 2019

## Atualizações anteriores

A tabela a seguir descreve alterações importantes em cada versão do Guia do usuário do AWS Resource Groups  antes de junho de 2018.

| Alteração | Descrição | Data |
| --- | --- | --- |
| Lançamento inicial | Lançamento inicial da próxima geração do AWS Resource Groups | 29 de novembro de 2017 |

# Glossário da AWS

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.

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.