Guía del usuario

AWS Resource Groups

AWS Resource Groups: Guía del usuario

Table of Contents

¿Qué son los grupos de recursos?

Puede utilizar grupos de recursos para organizar sus recursos de AWS. AWS Resource Groups es el servicio que le permite administrar y automatizar tareas en grandes cantidades de recursos al mismo tiempo. En esta guía, se muestra cómo crear y administrar grupos de recursos en AWS Resource Groups. Las tareas que puede realizar en un recurso varían en función del servicio de AWS que utilice. Para obtener una lista de los servicios admitidos por AWS Resource Groups y una breve descripción de lo que cada servicio le permite hacer con un grupo de recursos, consulte AWS servicios que funcionan con AWS Resource Groups.

Puede obtener acceso a Resource Groups a través de cualquiera de los puntos de entrada a continuación.

- En la AWS Management Console, en la barra de navegación superior, elija Servicios. A continuación, en Administración y gobernanza, elija Resource Groups y Tag Editor.

  Enlace directo: consola de AWS Resource Groups
- Mediante la API de Resource Groups, en comandos de la AWS CLI o los lenguajes de programación del SDK de AWS. Para obtener más información, consulte la Referencia de API de AWS Resource Groups.

Para trabajar con grupos de recursos en la página de inicio de la AWS Management Console

1. Inicie sesión en la AWS Management Console.
2. En la barra de navegación, elija Services (Servicios).
3. A continuación, en Administración y gobernanza, elija Resource Groups y Tag Editor.
4. En el panel de navegación de la izquierda, elija Resource Groups guardados para trabajar con un grupo existente o Crear un grupo para crear uno nuevo.

¿Qué son los grupos de recursos?

En AWS, un recurso es una entidad con la que se puede trabajar. Entre los ejemplos se incluyen una instancia Amazon EC2, una pila de AWS CloudFormation y un bucket de Amazon S3. Si trabaja con varios recursos, puede resultarle útil administrarlos como un grupo en lugar de transferirlos de un servicio de AWS a otro para cada tarea. Si administra un gran número de recursos relacionados, como las instancias EC2 que componen una capa de aplicación, es probable que necesite realizar

acciones por lotes en dichos recursos de forma simultánea. Entre los ejemplos de acciones por lotes se incluyen:

- La aplicación de actualizaciones o parches de seguridad.
- La actualización de aplicaciones.
- La apertura o el cierre de puertos para el tráfico de red.
- La recopilación de datos específicos de monitorización y de logs de la flota de instancias.

Un grupo de recursos es un conjunto de recursos de AWS que se encuentra en la misma Región de AWS y que coincide con los criterios especificados en la consulta del grupo. En Resource Groups, hay dos tipos de consultas que puede utilizar para crear un grupo. Ambos tipos de consultas incluyen recursos especificados en el formato `AWS::service::resource`.

- Consultas basadas en etiquetas

  Un grupo de recursos basado en etiquetas basa su pertenencia a una consulta que especifica una lista de tipos de recursos y etiquetas. Las etiquetas son claves que ayudan a identificar y ordenar los recursos de la organización. Opcionalmente, las etiquetas incluyen valores para las claves.

  > **Important**
  >
  > No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Usamos etiquetas para proporcionarle servicios de facturación y administración. Las etiquetas no se han diseñado para usarse con información privada o confidencial.

- Consultas basadas en una pila de AWS CloudFormation

  Un grupo de recursos de AWS CloudFormation basado en pilas basa su membresía en una consulta que especifica una pila de AWS CloudFormation en su cuenta en la región actual. Puede elegir opcionalmente tipos de recursos dentro de la pila que desee que estén en el grupo. Puede basar su consulta únicamente en una sola pila de AWS CloudFormation.

Grupos de recursos vinculados a servicios

Algunos Servicios de AWS definen grupos de recursos que solo se pueden crear y administrar mediante la consola y las API de ese servicio. Tiene limitaciones en cuanto a lo que puede hacer

con estos grupos en la consola de Resource Groups. Para obtener más información, consulte Configuraciones de servicio para grupos de recursos en la Guía de referencia de la API de AWS Resource Groups.

Los grupos de recursos pueden estar anidados; es decir, un grupo de recursos puede contener grupos de recursos existentes en la misma región.

Casos de uso de los grupos de recursos

De forma predeterminada, la AWS Management Console está organizada por servicio de AWS. Sin embargo, con Resource Groups puede crear una consola personalizada que organice y consolide la información en función de los criterios especificados en las etiquetas o los recursos de una pila de AWS CloudFormation. En la lista siguiente, se describen algunos de los casos en los que la agrupación de recursos puede ayudarle a organizar los recursos.

- Una aplicación que consta de diversas fases, como por ejemplo, el desarrollo, la puesta en marcha y la producción.
- Los proyectos administrados por varios departamentos o personas.
- Un conjunto de recursos de AWS que se utilizan simultáneamente para un proyecto común o que se desea administrar o supervisar como un grupo.
- Un conjunto de recursos relacionados con aplicaciones que se ejecutan en una plataforma específica, como, por ejemplo, Android o iOS.

Por ejemplo, supongamos que está desarrollando una aplicación web y que mantiene diferentes conjuntos de recursos para las etapas alfa, beta y de lanzamiento. Cada versión se ejecuta en Amazon EC2 con un volumen de almacenamiento de Amazon Elastic Block Store. Utiliza Elastic Load Balancing para administrar el tráfico y Route 53 para administrar el dominio. Sin Resource Groups, podría tener que acceder a múltiples consolas simplemente para comprobar el estado de sus servicios o modificar la configuración de una versión de su aplicación.

Con Resource Groups, utiliza una única página para ver y administrar sus recursos. Por ejemplo, supongamos que utiliza la herramienta para crear un grupo de recursos para cada versión (alfa, beta y de lanzamiento) de su aplicación. Para comprobar los recursos de la versión alfa de la aplicación, abra el grupo de recursos. A continuación, consulte la información consolidada en la página de su grupo de recursos. Para modificar un recurso específico, elija los enlaces de este en la página del grupo de recursos para obtener acceso a la consola de servicios que tiene la configuración que necesita.

AWS Resource Groups y permisos

Los permisos de la característica Resource Groups son a nivel de cuenta. Las entidades principales de IAM (como roles y usuarios) que compartan la cuenta podrán trabajar con los grupos de recursos que usted cree, siempre que tengan los permisos de IAM correctos.

Las etiquetas son propiedades de los recursos y, por tanto, pueden compartirse entre todos los recursos de la cuenta. Los usuarios de un departamento o grupo especializado pueden utilizar un vocabulario común (etiquetas) para crear grupos de recursos acordes con sus roles y responsabilidades. Tener un conjunto común de etiquetas también significa que cuando los usuarios comparten un grupo de recursos, no tienen que preocuparse de que falte información en las etiquetas o la información sea contradictoria.

Recursos de AWS Resource Groups

En Resource Groups, el único recurso disponible son los grupos. Los grupos tienen asociados nombres de recurso de Amazon (ARN) únicos. Para obtener más información sobre los ARN, consulte Nombres de recursos de Amazon (ARN) y espacios de nombres de servicios de AWS en la Referencia general de Amazon Web Services.

Tipo de recurso	Formato de ARN
Grupo de recursos	`arn:aws:resource-groups:` *`region`*`:`*`account`*`:group/`*`group-name`

Cómo funciona el etiquetado

Las etiquetas son pares de clave y valor que funcionan como metadatos para organizar los recursos de AWS. Con la mayoría de los recursos de AWS, tiene la opción de añadir etiquetas al crear el recurso, ya sea una instancia de Amazon EC2, un bucket de Amazon S3 o cualquier otro tipo de recurso. No obstante, también puede añadir etiquetas a varios recursos compatibles a la vez mediante Tag Editor. Primero cree una consulta para recursos de distintos tipos y, a continuación, añada, elimine o sustituya etiquetas para los recursos de los resultados de búsqueda. Las consultas basadas en etiquetas asignan un operador AND a las etiquetas, por lo que devolverán los recursos que coincidan con los tipos de recursos especificados y con todas las etiquetas especificadas.

> **Important**
>
> No almacene información de identificación personal (PII) ni otra información confidencial en las etiquetas. Usamos etiquetas para proporcionarle servicios de facturación y administración. Las etiquetas no se han diseñado para usarse con información privada o confidencial.

Para obtener más información, consulte la Guía del usuario de Tag Editor. Utilice Tag Editor para etiquetar los recursos compatibles; para etiquetar otros recursos adicionales, utilice la funcionalidad de etiquetado de la consola del servicio en la que cree y administre el recurso.

Introducción a AWS Resource Groups

En AWS, un recurso es una entidad con la que se puede trabajar. Entre los ejemplos se incluyen una instancia Amazon EC2, un bucket de Amazon S3 o una zona alojada de Amazon Route 53. Si trabaja con varios recursos, puede resultarle útil administrarlos como un grupo en lugar de transferirlos de un servicio de AWS a otro para cada tarea.

En esta sección, se muestra cómo comenzar a utilizar AWS Resource Groups. En primer lugar, organice los recursos de AWS etiquetándolos en Tag Editor. A continuación, cree consultas en Resource Groups que incluyan los tipos de recursos que desea incluir en un grupo y las etiquetas que ha aplicado a los recursos.

Una vez que haya creado grupos en Resource Groups, utilice herramientas de AWS Systems Manager como Automation para simplificar las tareas de administración de sus grupos de recursos.

Para obtener más información acerca de cómo empezar a trabajar con las características y herramientas de AWS Systems Manager, consulte la Guía del usuario de AWS Systems Manager.

Temas

Requisitos previos para trabajar con AWS Resource Groups

Antes de comenzar a trabajar con los grupos de recursos, asegúrese de que tiene una cuenta de AWS activa que disponga de recursos y de los derechos necesarios para etiquetar recursos y crear grupos.

Inscríbase en AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea una. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

Crear recursos de

Puede crear un grupo de recursos vacío, pero no podrá realizar ninguna tarea con los miembros del grupo de recursos hasta que haya recursos en él. Para obtener más información sobre los tipos de recursos admitidos, consulte Tipos de recursos que puede usar con un AWS Resource Groups editor de etiquetas.

Configuración de permisos

Para hacer pleno uso de Resource Groups y Tag Editor, es posible que necesite más permisos para etiquetar recursos o para las claves de etiquetas y los valores de un recurso. Estos permisos se dividen en las categorías siguientes:

- Los permisos para los servicios individuales, para que pueda etiquetar los recursos de dichos servicios e incluirlos en los grupos de recursos.
- Los permisos necesarios para usar la consola de Tag Editor
- Permisos necesarios para usar la AWS Resource Groups consola y la API.

Si es administrador, puede proporcionar permisos a sus usuarios mediante la creación de políticas a través del servicio AWS Identity and Access Management (IAM). Primero debe crear sus principios, como las funciones o los usuarios de IAM, o bien asociar identidades externas a su AWS entorno

mediante un servicio como. AWS IAM Identity Center A continuación, aplique las políticas con los permisos que necesitan los usuarios. Para obtener información acerca de cómo crear y asociar políticas de IAM;, consulte Uso de las políticas.

Permisos para servicios individuales

> **Important**
>
> En esta sección, se describen los permisos que son necesarios para etiquetar recursos desde las API y las consolas de otros servicios, y para añadir dichos recursos a grupos de recursos.

Como se describe en ¿Qué son los grupos de recursos?, cada grupo de recursos representa un conjunto de recursos de los tipos especificados que comparten una o varias claves de etiquetas o valores. Para añadir etiquetas a un recurso, debe tener los permisos necesarios para el servicio al que pertenece el recurso. Por ejemplo, para etiquetar instancias de Amazon EC2, debe tener permisos para las acciones de etiquetado en la API de dicho servicio, como los que se muestran en la Guía del usuario de Amazon EC2.

Para utilizar plenamente la característica de grupos de recursos, necesita otros permisos que le permitan tener acceso a la consola de un servicio e interactuar con los recursos disponibles en ella. Para ver ejemplos de dichas políticas para Amazon EC2, consulte Ejemplos de políticas para trabajar en la consola de Amazon EC2 en la Guía del usuario de Amazon EC2.

Permisos obligatorios para Resource Groups y Tag Editor

Para utilizar Resource Groups y Tag Editor, se deben añadir los siguientes permisos a la instrucción de política del usuario en IAM. Puede añadir políticas AWS gestionadas que sean mantenidas y guardadas up-to-date por AWS, o bien puede crear y mantener su propia política personalizada.

Uso de políticas AWS administradas para los permisos de Resource Groups y Tag Editor

AWS Resource Groups y Tag Editor admiten las siguientes políticas AWS administradas que puedes usar para proporcionar un conjunto predefinido de permisos a tus usuarios. Puede adjuntar estas políticas administradas a cualquier usuario, rol o grupo del mismo modo que lo haría con cualquier otra política que cree.

ResourceGroupsandTagEditorReadOnlyAccess

Esta política concede al rol de IAM o al usuario adjunto permiso para llamar a las operaciones de solo lectura de Resource Groups y Tag Editor. Para leer las etiquetas de un recurso, también debe tener permisos para ese recurso mediante una política independiente (consulte la siguiente nota importante).

ResourceGroupsandTagEditorFullAccess

Esta política concede al rol de IAM o usuario adjunto permiso para llamar a cualquier operación de Resource Groups y a las operaciones de lectura y escritura de etiquetas en Tag Editor. Para leer o escribir las etiquetas de un recurso, también debe tener permisos para ese recurso mediante una política independiente (consulte la siguiente nota importante).

Important

Las dos políticas anteriores conceden permiso para llamar a las operaciones Resource Groups y Tag Editor y usar esas consolas. Para las operaciones de Resource Groups, estas políticas son suficientes y otorgan todos los permisos necesarios para trabajar con cualquier recurso de la consola de Resource Groups.
Sin embargo, para las operaciones de etiquetado y la consola de Tag Editor, los permisos son más detallados. Debe tener los permisos no solo para invocar la operación, sino también los permisos adecuados para el recurso específico a cuyas etiquetas está intentando acceder. En función del tipo de operaciones, puede asociar una de estas políticas:

- La política AWS gestionada ReadOnlyAccessconcede permisos a las operaciones de solo lectura para los recursos de cada servicio. AWS actualiza automáticamente esta política con los nuevos AWS servicios a medida que están disponibles.
- Muchos servicios proporcionan políticas AWS administradas de solo lectura específicas para cada servicio que puede utilizar para limitar el acceso únicamente a los recursos proporcionados por ese servicio. Por ejemplo, Amazon EC2 proporciona AmazonEC2. ReadOnlyAccess
- Podría crear su propia política que conceda acceso únicamente a las operaciones de solo lectura muy específicas para los pocos servicios y recursos a los que desea que accedan sus usuarios. Esta política utiliza una estrategia de “lista de permitidos” o una estrategia de lista de rechazados.

Una estrategia de lista de permitidos aprovecha el hecho de que el acceso está denegado de forma predeterminada hasta que se permita explícitamente en una política. Por lo tanto, puede utilizar una política como la del siguiente ejemplo:

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

Como alternativa, puede utilizar una estrategia de “lista de denegados” que permita el acceso a todos los recursos excepto a aquellos que bloquee de forma explícita.

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

Añadir manualmente los permisos de Resource Groups y Tag Editor

- `resource-groups:*` (Este permiso permite todas las acciones de Resource Groups. Si, por el contrario, desea restringir las acciones que están disponibles para un usuario, puede sustituir el asterisco por una acción específica de Resource Groups o por una lista de acciones separadas por comas)
- `cloudformation:DescribeStacks`
- `cloudformation:ListStackResources`

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

> **Note**
>
> El `resource-groups:SearchResources` permiso permite a Tag Editor enumerar los recursos al filtrar la búsqueda mediante claves o valores de etiquetas.
> El `resource-explorer:ListResources` permiso permite a Tag Editor enumerar los recursos cuando se buscan recursos sin definir las etiquetas de búsqueda.

Para usar Resource Groups y Tag Editor en la consola, también necesita permiso para ejecutar la acción `resource-groups:ListGroupResources`. Este permiso es necesario para mostrar los tipos de recursos disponibles en la región actual. Por el momento, no se admite el uso de condiciones de política con `resource-groups:ListGroupResources`.

Otorgar permisos para usar AWS Resource Groups un editor de etiquetas

Para añadir una política de uso AWS Resource Groups de un editor de etiquetas a un usuario, haga lo siguiente.

1. Abra la consola de IAM.
2. En el panel de navegación, seleccione Usuarios.
3. Busca el usuario al que quieres conceder los permisos AWS Resource Groups de Tag Editor. Elija el nombre del usuario para abrir la página de propiedades del usuario.
4. Elija Añadir permisos.
5. Elija Adjuntar directamente políticas existentes.
6. Elija Crear política.
7. En la pestaña JSON, pegue la instrucción de política siguiente:

```
{
```

```
  "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 instrucción de política de ejemplo únicamente concede permisos para las acciones de AWS Resource Groups y Tag Editor. No permite el acceso a AWS Systems Manager las tareas de la AWS Resource Groups consola. Por ejemplo, esta política no concede permiso para utilizar los comandos de Systems Manager Automation. Para realizar tareas de Systems Manager con los grupos de recursos, debe tener permisos de Systems Manager asociados a su política (como, por ejemplo, `ssm:*`). Para obtener más información acerca de la concesión de acceso a Systems Manager, consulte Configuración del acceso a Systems Manager en la Guía del usuario de AWS Systems Manager .

8. Elija Revisar política.
9. Asigne un nombre y una descripción a la política nueva. (por ejemplo, `AWSResourceGroupsQueryAPIAccess`).
10. Elija Crear política.
11. Ahora que la política está guardada en IAM, puede asociarla a otros usuarios. Para obtener más información sobre cómo añadir una política a un usuario, consulte Agregar permisos asociando políticas directamente al usuario en la Guía del usuario de IAM.

Más información sobre la AWS Resource Groups autorización y el control de acceso

Resource Groups admite lo siguiente.

- Políticas basadas en acciones. Por ejemplo, puede crear una política que permita a los usuarios realizar operaciones ListGroups, pero no otras.
- Permisos de nivel de recursos. Permisos de nivel de recursos utilizando ARN para especificar recursos individuales en la política.
- Autorización basada en etiquetas. Resource Groups admite el uso de etiquetas de recursos en el estado de una política. Por ejemplo, puede crear una política que permita a los usuarios de Resource Groups el acceso completo a un grupo que haya etiquetado.
- Credenciales temporales. Los usuarios pueden asumir un rol con una política que permita AWS Resource Groups las operaciones.

Resource Groups no admite políticas basadas en recursos.

Resource Groups no utiliza ningún rol vinculado a servicios.

Para obtener más información sobre cómo Resource Groups y Tag Editor se integran con AWS Identity and Access Management (IAM), consulte los siguientes temas de la Guía del AWS Identity and Access Management usuario.

- AWS servicios que funcionan con IAM
- Claves de condiciones, recursos y acciones para AWS Resource Groups
- Control del acceso mediante políticas

Crear grupos basados en consultas en AWS Resource Groups

Temas

- Tipos de consultas de grupos de recursos
- Construir una consulta basada en etiquetas y crear un grupo
- Cree un grupo basado en pilas de AWS CloudFormation

Tipos de consultas de grupos de recursos

En AWS Resource Groups, una consulta es la base de un grupo basado en consultas. Puede basar un grupo de recursos en uno de los dos tipos de consultas.

Consultas basadas en etiquetas

Las consultas basadas en etiquetas incluyen listas de tipos de recursos que se especifican con el formato siguiente `AWS::service::resource`, así como etiquetas. Las etiquetas son claves que ayudan a identificar y ordenar los recursos de la organización. Opcionalmente, las etiquetas incluyen valores para las claves.

Para una consulta basada en etiquetas, también debe especificar las etiquetas compartidas por los recursos que desea que sean miembros del grupo. Por ejemplo, si desea crear un grupo de recursos que tenga todas las instancias de Amazon EC2 y los buckets de Amazon S3 que está utilizando para llevar a cabo la etapa de pruebas de una aplicación y dispone de instancias y buckets que se han etiquetado de esta manera, elija los tipos de recurso `AWS::EC2::Instance` y `AWS::S3::Bucket` en la lista desplegable y, a continuación, especifique la clave de etiqueta **`Stage`** con un valor de etiqueta de **`Test`**.

La sintaxis del parámetro `ResourceQuery` de un grupo de recursos basado en etiquetas contiene los siguientes elementos:

- `Type`

  Este elemento indica qué tipo de consulta define este grupo de recursos. Para crear un grupo de recursos basado en etiquetas, especifique el valor `TAG_FILTERS_1_0` de la siguiente manera:

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

- `Query`

  Este elemento define la consulta real que se utiliza para compararla con los recursos. El secreto debe contener una estructura JSON con los siguientes elementos:

  - `ResourceTypeFilters`

    Este elemento limita los resultados solo a los tipos de recursos que coinciden con el filtro. Puede especificar los valores siguientes:

  - `"AWS::AllSupported"`: para especificar que los resultados pueden incluir recursos de cualquier tipo que coincidan con la consulta y que actualmente son compatibles con el servicio Resource Groups.
  - `"AWS::service-id::resource-type`: una lista separada por comas de cadenas de especificación de tipos de recursos con este formato: , como por ejemplo `"AWS::EC2::Instance"`.
- `TagFilters`

  Este elemento especifica los pares de cadenas clave/valor que se comparan con las etiquetas adjuntas a los recursos. Los que tengan una clave de etiqueta y un valor que coincidan con el filtro se incluyen en el grupo. Cada filtro consta de los siguientes elementos:

  - `"Key"`: una cadena con un nombre de clave. Únicamente los recursos de la cuenta que están etiquetados con un par de clave-valor coincidente con las siguientes claves:
  - `"Values"`: una cadena con una lista de valores separados por comas para la clave especificada. Únicamente los recursos de la cuenta que están etiquetados con un par de clave-valor coincidente son miembros del grupo.

Todos estos elementos JSON deben combinarse en una representación de cadena de una sola línea de la estructura JSON. Por ejemplo, considere una `Query` con la siguiente estructura JSON de ejemplo. Esta consulta debe coincidir únicamente con las instancias de Amazon EC2 que tengan la etiqueta “Stage” con el valor “Test”.

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

Ese JSON se puede representar como la siguiente cadena de una sola línea y se puede usar como el valor del elemento `Query`. Como el valor de una estructura JSON debe ser una cadena entre comillas dobles, debe evitar los caracteres de comillas dobles o barras diagonales incrustados precediendo a cada uno de ellos con una barra invertida, como se muestra a continuación:

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

La cadena `ResourceQuery` completa se representa como se muestra aquí, como un parámetro de comando CLI:

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

basadas en una pila de AWS CloudFormation

En una consulta basada en una pila de AWS CloudFormation, elija una pila de AWS CloudFormation de su cuenta en la región actual y, a continuación, elija los tipos de recursos de la pila que desea que estén en el grupo. Puede basar su consulta únicamente en una pila de AWS CloudFormation.

> **Note**
>
> Una pila de AWS CloudFormation puede contener otras pilas de AWS CloudFormation “secundarias”. Sin embargo, un grupo de recursos basado en una pila “principal” no obtiene todos los recursos de las pilas secundarias como miembros del grupo. Los grupos de recursos agregan las pilas secundarias al grupo de recursos de la pila principal como miembros de un solo grupo y no las amplían.

Resource Groups admite consultas basadas en pilas de AWS CloudFormation que tienen uno de los siguientes estados.

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

> **Important**
>
> Solo los recursos que se crean directamente como parte de la pila de la consulta se incluyen en el grupo de recursos. Los recursos creados posteriormente por los miembros

de la pila AWS CloudFormation no se convierten en miembros del grupo. Por ejemplo, si un grupo de escalado automático es creado por AWS CloudFormation como parte de la pila, entonces ese grupo de escalado automáticoes miembro del grupo. Sin embargo, una instancia de Amazon EC2 creada por ese grupo de escalado automático como parte de su operación no es miembro del grupo de recursos basado en la pila de AWS CloudFormation.

Si crea un grupo basado en una pila de AWS CloudFormation y el estado de la pila cambia a uno que ya no se admite como una base para una consulta de grupo, como `DELETE_COMPLETE`, el grupo de recursos seguirá existiendo, pero no tendrá recursos miembros.

Después de crear un grupo de recursos, puede realizar tareas en los recursos del grupo.

La sintaxis del parámetro `ResourceQuery` de un grupo de recursos CloudFormation basado en etiquetas contiene los siguientes elementos:

- `Type`

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

  Para crear un grupo de recursos AWS CloudFormation basado en etiquetas, especifique el valor `CLOUDFORMATION_STACK_1_0` de la siguiente manera:

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

- `Query`

  Este elemento define la consulta real que se utiliza para compararla con los recursos. Contiene una representación de cadena de una estructura JSON con los siguientes elementos:

  - `ResourceTypeFilters`

    Este elemento limita los resultados solo a los tipos de recursos que coinciden con el filtro. Puede especificar los valores siguientes:

    - `"AWS::AllSupported"`: para especificar que los resultados pueden incluir recursos de cualquier tipo que coincidan con la consulta.

  - `"AWS::service-id::resource-type`: una lista separada por comas de cadenas de especificación de tipos de recursos con este formato: , como por ejemplo `"AWS::EC2::Instance"`.
- `StackIdentifier`

  Este elemento especifica el Nombre de recurso de Amazon (ARN) de la pila de AWS CloudFormation cuyos recursos desea incluir en el grupo.

Todos estos elementos JSON deben combinarse en una representación de cadena de una sola línea de la estructura JSON. Por ejemplo, considere una `Query` con la siguiente estructura JSON de ejemplo. Esta consulta debe coincidir únicamente con los buckets de Amazon S3 que forman parte de la pila de AWS CloudFormation especificada.

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

Ese JSON se puede representar como la siguiente cadena de una sola línea y se puede usar como el valor del elemento `Query`. Como el valor de una estructura JSON debe ser una cadena entre comillas dobles, debe evitar los caracteres de comillas dobles o barras diagonales incrustados precediendo a cada uno de ellos con una barra invertida, como se muestra a continuación:

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

La cadena `ResourceQuery` completa se representa como se muestra aquí, como un parámetro de comando 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\"}'
```

Construir una consulta basada en etiquetas y crear un grupo

Los siguientes procedimientos le muestran cómo crear una consulta basada en etiquetas y usarla para crear un grupo de recursos.

Console

1. Inicie sesión en la consola de AWS Resource Groups.
2. En el panel de navegación, elija Crear Resource Group.
3. En la páginaCrear grupo basado en consultas, en Tipo de grupo, elija el tipo de grupo Basado en etiquetas.
4. En Criterios de agrupación, elija los tipos de recursos que desea que formen parte del grupo de recursos. Puede incluir un máximo de 20 tipos de recursos en una consulta. Para este tutorial, elija AWS::EC2::Instance y AWS::S3::Bucket.
5. Aun en Criterios de agrupación, para las Etiquetas, especifique una clave de etiqueta o un par de clave y valor para limitar los recursos coincidentes e incluir solo aquellos que estén etiquetados con los valores especificados. Elija Añadir o pulse Intro cuando haya terminado de definir la etiqueta. En este ejemplo, filtre los recursos que tienen una clave de etiqueta Etapa. El valor de la etiqueta es opcional, pero permite limitar aún más los resultados de la consulta. Puede añadir varios valores a una clave de etiqueta añadiendo un operador `OR` entre los valores de las etiquetas. Para añadir más etiquetas, elija Añadir. Las consultas asignan un operador `AND` a las etiquetas, por lo que devolverán los recursos que coincidan con los tipos de recursos especificados y con todas las etiquetas especificadas.
6. Aun en Criterio de agrupamiento, elija Vista previa de los recursos del grupo para devolver la lista de instancias EC2 y buckets de S3 de la cuenta que coincidan con las etiquetas o las claves de etiqueta especificadas.
7. Una vez que tenga los resultados que desea, cree un grupo basado en esta consulta.

    a. En la página Crear un grupo de recursos, en Nombre de grupo, escriba un nombre para el grupo.

    El nombre de un grupo de recursos puede tener un máximo de 128 caracteres de longitud e incluir letras, números, guiones, puntos y guiones bajos. El nombre no puede comenzar por `AWS` ni `aws`. Estas cadenas están reservadas. El nombre de un grupo de recursos debe ser único en la región actual de la cuenta.

    b. (Opcional) En Descripción del grupo, escriba una descripción para el grupo.

c. (Opcional) En Etiquetas del grupo, añada pares de clave y valor de etiqueta que se aplicarán solamente al grupo de recursos, no a los recursos miembros del grupo.

   Las etiquetas del grupo son útiles si tiene previsto que este grupo vaya a formar parte de un grupo más grande. Dado que es necesario especificar al menos una clave de etiqueta para crear un grupo, asegúrese de añadir como mínimo una clave de etiqueta en Etiquetas del grupo para los grupos que tiene previsto anidar en grupos más grandes.

8. Cuando termine, elija Crear grupo.

AWS CLI & AWS SDKs

Un grupo basado en etiquetas se basa en una consulta de tipo `TAG_FILTERS_1_0`.

1. En una sesión de la AWS CLI, escriba lo siguiente, reemplazando los valores de nombre de grupo, descripción, tipos de recursos, claves de etiqueta y valores de etiqueta por los suyos propios y, a continuación, pulse Intro. Las descripciones pueden tener un máximo de 512 caracteres de longitud e incluir letras, números, guiones, guiones bajos, puntuación y espacios. Puede incluir un máximo de 20 tipos de recursos en una consulta. El nombre de un grupo de recursos puede tener un máximo de 128 caracteres de longitud e incluir letras, números, guiones, puntos y guiones bajos. El nombre no puede comenzar por `AWS` ni `aws`. Estas cadenas están reservadas. El nombre de un grupo de recursos debe ser único en la cuenta.

   Al menos es obligatorio un valor para `ResourceTypeFilters`. Para especificar todos los tipos de recursos, utiliceAWS::AllSupported como el 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\"]}]}"}'
```

   El siguiente comando es un ejemplo.

```
$ 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\"]}]}"}'
```

El siguiente comando es un ejemplo que incluye todos los tipos de recursos admitidos.

```
$ 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. El comando devuelve lo siguiente.

   - Una descripción completa del grupo que se ha creado.
   - La consulta de recursos que ha utilizado para crear el grupo.
   - Las etiquetas que están asociadas al grupo.

Cree un grupo basado en pilas de AWS CloudFormation

Los siguientes procedimientos le muestran cómo crear una consulta basada en consultas y usarla para crear un grupo de recursos.

Console

1. Inicie sesión en la consola de AWS Resource Groups.
2. En el panel de navegación, elija Crear Resource Group.
3. En Crear grupo basado en consultas, en Tipo de grupo, elija el tipo de grupo Basado en la pila de CloudFormation.
4. Elija la pila que desea que sea la base de su grupo. Un grupo de recursos se puede basar solo en una pila. Para filtrar la lista de pilas, empiece a escribir el nombre de la pila. En la lista aparecen solo las pilas con estados compatibles.
5. Elija los tipos de recursos en la pila que desea incluir en el grupo. Para este tutorial, mantenga el valor predeterminado de Todos los tipos de recursos admitidos. Para obtener más información acerca de qué tipos de recursos son compatibles y pueden estar en el grupo, consulte Tipos de recursos que puede usar con un AWS Resource Groups editor de etiquetas.

6. Elija Ver recursos del grupo para devolver la lista de recursos de la pila de AWS CloudFormation que coincidan con los tipos de recursos que ha seleccionado.
7. Una vez que tenga los resultados que desea, cree un grupo basado en esta consulta.

    a. En la página Detalles del grupo, en Nombre de grupo, escriba un nombre para el grupo de recursos.

    El nombre de un grupo de recursos puede tener un máximo de 128 caracteres de longitud e incluir letras, números, guiones, puntos y guiones bajos. El nombre no puede comenzar por `AWS` ni `aws`. Estas cadenas están reservadas. El nombre de un grupo de recursos debe ser único en la región actual de la cuenta.

    b. (Opcional) En Descripción del grupo, escriba una descripción para el grupo.

    c. (Opcional) En Etiquetas del grupo, añada pares de clave y valor de etiqueta que se aplicarán solamente al grupo de recursos, no a los recursos miembros del grupo.

    Las etiquetas del grupo son útiles si tiene previsto que este grupo vaya a formar parte de un grupo más grande. Dado que es necesario especificar al menos una clave de etiqueta para crear un grupo, asegúrese de añadir como mínimo una clave de etiqueta en Etiquetas del grupo para los grupos que tiene previsto anidar en grupos más grandes.
8. Cuando termine, elija Crear grupo.

AWS CLI & AWS SDKs

Un grupo basado en pilas de AWS CloudFormation se basa en una consulta de tipo `CLOUDFORMATION_STACK_1_0`.

1. Ejecute el siguiente comando, sustituyendo los valores de nombre de grupo, descripción, identificador de pila y tipos de recursos por los suyos. Las descripciones pueden tener un máximo de 512 caracteres de longitud e incluir letras, números, guiones, guiones bajos, puntuación y espacios.

    Si no identifica los tipos de recursos, Resource Groups incluye todos los tipos de recursos admitidos en la pila. Puede incluir un máximo de 20 tipos de recursos en una consulta. El nombre de un grupo de recursos puede tener un máximo de 128 caracteres de longitud e incluir letras, números, guiones, puntos y guiones bajos. El nombre no puede comenzar por `AWS` ni `aws`. Estas cadenas están reservadas. El nombre de un grupo de recursos debe ser único en la cuenta.

El *stack_identifier* es el ARN de la pila, como se muestra en el comando de ejemplo.

```
$ 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\"]}"}'
```

El siguiente comando es un ejemplo.

```
$ 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. El comando devuelve lo siguiente.

   - Una descripción completa del grupo que se ha creado.
   - La consulta de recursos que ha utilizado para crear el grupo.

Actualización de grupos en AWS Resource Groups

Para actualizar un grupo de recursos basado en etiquetas en Resource Groups, puede editar la consulta y las etiquetas que constituyen la base del grupo. Solo podrá agregar y eliminar recursos del grupo mediante la aplicación de cambios en la consulta o las etiquetas. No se pueden seleccionar recursos específicos para añadirlos al grupo o eliminarlos de este. La mejor forma de añadir o eliminar un recurso específico de un grupo es editar las etiquetas del recurso. A continuación, compruebe que la consulta de etiquetas del grupo de recursos incluye u omite la etiqueta, en función de si desea incluir el recurso en el grupo.

Para actualizar un grupo de recursos basado en una pila de AWS CloudFormation, puede elegir una pila diferente. También puede añadir o eliminar tipos de recursos de la pila que desee que formen parte del grupo. Para cambiar los recursos disponibles en la pila, actualice la plantilla de

AWS CloudFormation que ha utilizado para crear la pila y, a continuación, actualice la pila en AWS CloudFormation. Para obtener más información acerca de cómo actualizar una pila de AWS CloudFormation, consulte Actualizaciones de pilas deAWS CloudFormation en la Guía del usuario de AWS CloudFormation

En la AWS CLI, utilice estos dos comandos para actualizar los grupos.

- `update-group`, para actualizar la descripción de un grupo.
- `update-group-query`, para actualizar la consulta de recursos y las etiquetas que determinan los recursos que forman parte del grupo.

No puede cambiar un grupo basado en una pila de AWS CloudFormation en la consola por un grupo de consulta basado en etiquetas o viceversa. Sin embargo, puede hacerlo mediante la API de Resource Groups, que se incluye en la AWS CLI.

Actualizar grupos de consultas basados en etiquetas

Console

Actualizar un grupo basado en etiquetas cambiando los tipos de recursos o etiquetas de la consulta en la que se basa el grupo. También puede añadir o modificar la descripción del grupo.

1. Inicie sesión en la Consola de AWS Resource Groups.
2. En el panel de navegación, en Resource Groups guardados, seleccione un grupo y, a continuación, seleccione Editar.

> **Note**
>
> Solo puede actualizar los grupos de recursos de su propiedad. La columna Propietario muestra la propiedad de la cuenta de cada grupo de recursos. Se crearon todos los grupos con un propietario de cuenta distinto del grupo en el que has iniciado sesiónAWS License Manager. Para obtener más información, consulte Grupos de recursos de hostAWS License Manager en la Guía del usuario de License Manager.

3. En la página Editar grupo, dentro de Criterios de agrupación, añada o elimine tipos de recursos. Puede incluir un máximo de 20 tipos de recursos en una consulta. Para eliminar un tipo de recurso, elija X en la etiqueta del tipo de recurso. Elija View group resources (Ver

recursos del grupo) para ver cómo afectan los cambios a los recursos que forman el grupo. En este tutorial, añadimos el tipo de recurso AWS::RDS::DBInstance a la consulta.

4. Aún dentro de Criterios de agrupación, edite las etiquetas según sea necesario. En este ejemplo, filtramos los recursos que tienen un clave de etiqueta Stage (Etapa) y añadimos un valor de etiqueta Test (Pruebas). El valor de la etiqueta es opcional, pero permite limitar aún más los resultados de la consulta. Para eliminar una etiqueta, seleccione X en el rótulo de la etiqueta.
5. En Información adicional, puede editar la descripción del grupo. No puede editar el nombre de un grupo después de crearlo.
6. (Opcional) En Etiquetas del grupo, puede añadir o eliminar etiquetas. Las etiquetas del grupo son metadatos sobre el grupo de recursos. No afectan a los recursos que lo componen. Para cambiar los recursos que devuelve la consulta del grupo de recursos, edite las etiquetas del área Criterios de agrupación.

   Las etiquetas del grupo son útiles si tiene previsto que este grupo vaya a formar parte de un grupo más grande. Para crear un grupo, es necesario especificar al menos una clave de etiqueta. Por lo tanto, asegúrese de añadir al menos una clave de etiqueta en Etiquetas de grupo a los grupos que planea anidar en grupos más grandes.
7. Elija Previsualizar recursos del grupo para obtener la lista actualizada de instancias EC2, buckets de S3 e instancias de base de datos de Amazon RDS de la cuenta que coincidan con las claves de etiqueta especificadas. Si no ve los recursos que esperaba en la lista, asegúrese de que estos estén etiquetados con las etiquetas que ha especificado en Criterios de agrupación.
8. Cuando haya terminado, elija Guardar cambios.

AWS CLI & AWS SDKs

En la AWS CLI, utilizará dos comandos diferentes para actualizar la consulta de un grupo y la descripción de un grupo de recursos. No se puede editar el nombre de un grupo existente. En la AWS CLI puede cambiar un grupo basado en etiquetas por un grupo basado en una pila de CloudFormation o viceversa.

1. Si no desea cambiar la descripción del grupo, omita este paso y continúe en el siguiente. En una sesión de la AWS CLI, escriba lo siguiente, reemplazando los valores del nombre y la descripción del grupo por los suyos propios, y, a continuación, pulse Intro.

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

El siguiente comando es un ejemplo.

```
$ 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."
```

El comando devuelve una descripción completa actualizada del grupo.

2. Para actualizar la consulta y las etiquetas de un grupo, escriba el siguiente comando. Sustituya los valores del nombre del grupo, los tipos de recursos, las claves de las etiquetas y los valores de las etiquetas por los suyos. Luego pulse Intro. Puede incluir un máximo de 20 tipos de recursos en una 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\"]}]}"}'
```

El siguiente comando es un ejemplo.

```
$ 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\"]}]}"}'
```

El comando devuelve la consulta actualizada como resultado.

Actualización de un grupo basado en una pila de AWS CloudFormation

Console

No puede cambiar un grupo basado en una pila de AWS CloudFormation por un grupo basado en etiquetas en la AWS Management Console. Sin embargo, puede cambiar la pila en la que se basa el grupo o cambiar los tipos de recursos de la pila que desee incluir en el grupo. También puede añadir o modificar la descripción del grupo.

1. Inicie sesión en la Consola de AWS Resource Groups.
2. En el panel de navegación, en Resource Groups guardados, seleccione un grupo y, a continuación, seleccione Editar.
3.
> **Note**
>
> Solo puede actualizar los grupos de recursos de su propiedad. La columna Propietario muestra la propiedad de la cuenta de cada grupo de recursos. Se crearon todos los grupos con un propietario de cuenta distinto del grupo en el que has iniciado sesiónAWS License Manager. Para obtener más información, consulte Grupos de recursos de hostAWS License Manager en la Guía del usuario de License Manager.

4. Para cambiar la pila en la que se basa su grupo, seleccione la pila de la lista desplegable en la página Editar grupo, dentro de Criterios de agrupación. Un grupo de recursos se puede basar solo en una pila. Para filtrar la lista de pilas, empiece a escribir el nombre. En la lista aparecen solo las pilas con estados compatibles. Para obtener una lista de estados compatibles consulte Crear grupos basados en consultas en AWS Resource Groups en esta guía.
5. Añadir o eliminar tipos de recursos. En la lista desplegable solo se muestran los tipos de recursos disponibles en la pila. El valor predeterminado es Todos los tipos de recursos compatibles. Puede incluir un máximo de 20 tipos de recursos en una consulta. Para eliminar un tipo de recurso, elija X en la etiqueta del tipo de recurso. Para obtener más información acerca de qué tipos de recursos son compatibles y pueden estar en el grupo, consulte Tipos de recursos que puede usar con un AWS Resource Groups editor de etiquetas.
6. Elija Previsualizar recursos del grupo para devolver la lista de recursos de la pila de AWS CloudFormation que coincidan con los tipos de recursos que ha seleccionado.

7. En Información adicional, puede editar la descripción del grupo. No puede editar el nombre de un grupo después de crearlo.
8. Añada o elimine etiquetas en Etiquetas del grupo. Las etiquetas del grupo son metadatos sobre el grupo de recursos. No afectan a los recursos que lo componen. Para cambiar los recursos que devuelve la consulta del grupo de recursos, edite las etiquetas de Criterios de agrupación.

   Las etiquetas del grupo son útiles si tiene previsto que este grupo vaya a formar parte de un grupo más grande. Para crear un grupo, es necesario especificar al menos una clave de etiqueta. Por lo tanto, asegúrese de añadir al menos una clave de etiqueta en Etiquetas de grupo a los grupos que planea anidar en grupos más grandes.
9. Cuando haya terminado, elija Guardar cambios.

AWS CLI & AWS SDKs

En la AWS CLI, utilizará dos comandos diferentes para actualizar la consulta de un grupo y la descripción de un grupo de recursos. No se puede editar el nombre de un grupo existente. En la AWS CLI puede cambiar un grupo basado en etiquetas por un grupo basado en una pila de CloudFormation o viceversa.

1. Si no desea cambiar la descripción del grupo, omita este paso y continúe en el siguiente. Ejecute el siguiente comando, sustituyendo los valores de nombre de grupo y descripción por los suyos.

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

   El siguiente comando es un ejemplo.

   ```
   $ 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."
   ```

   El comando devuelve una descripción completa actualizada del grupo.
2. Para actualizar la consulta y las etiquetas de un grupo, ejecute el siguiente comando. Sustituya los valores del nombre del grupo, el identificador de la pila y los tipos de recursos

por los suyos. Para añadir tipos de recursos, proporcione la lista completa de tipos de recursos en el comando, no solo los tipos de recursos que esté añadiendo. Puede incluir un máximo de 20 tipos de recursos en una consulta.

El *stack_identifier* es el ARN de la pila, como se muestra en el comando de ejemplo.

```
$ 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\"]}"}'
```

El siguiente comando es un ejemplo.

```
$ 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\"]}"}'
```

El comando devuelve la consulta actualizada como resultado.

Eventos del ciclo de vida de los grupos: supervisión de los grupos de recursos para detectar cambios

Después de AWS Resource Groups organizar los recursos en grupos, puede supervisarlos para detectar cambios que se presenten como eventos. Puede recibir una notificación sobre un evento grupal como una señal para tomar algún tipo de acción. Por ejemplo, puede configurar una notificación que se envíe cada vez que cambie la pertenencia de un grupo. Puede utilizar un evento de la adición de un nuevo miembro del grupo para activar una función de Lambda que revise el cambio mediante programación para garantizar que los nuevos miembros del grupo cumplan con los requisitos de cumplimiento establecidos por su organización. Una función de Lambda de este tipo podría aplicar una corrección automática para cualquier miembro nuevo del grupo que no cumpla

con esos requisitos. Un evento provocado por la eliminación de un miembro del grupo podría activar una función de Lambda que lleve a cabo cualquier limpieza necesaria, como la eliminación de los recursos vinculados.

Al activar los eventos del ciclo de vida de los grupos para sus grupos de recursos, permite que Amazon EventBridge capture los eventos relacionados con los cambios en sus grupos y los ponga a disposición de todos los distintos servicios de destino compatibles con EventBridge. A continuación, puede configurar esos servicios de destino para que realicen automáticamente las acciones que requiera su situación. Estos objetivos incluyen una variedad de servicios de AWS como Amazon Simple Notification Service (Amazon SNS), Amazon Simple Queue Service (Amazon SQS) y AWS Lambda. Con servicios como Lambda, sus eventos pueden disparar respuestas programáticas que utilizan código para realizar cualquier acción que necesite. Para obtener una lista de los servicios de AWS que puede segmentar con EventBridge, consulte los destinos de Amazon EventBridge en la Guía del usuario de Amazon EventBridge.

Al activar los eventos del ciclo de vida de un grupo, AWS Resource Groups crea los siguientes elementos:

- Un rol vinculado a un servicio AWS Identity and Access Management (IAM) que tiene permiso para supervisar sus recursos y así detectar cualquier cambio en sus etiquetas y sus AWS CloudFormation pilas, lo que facilita la detección de cualquier cambio en los recursos que forman parte de una pila.
- Una regla de EventBridge gestionada por Resource Groups que captura los detalles de cualquier cambio en las etiquetas o pilas de sus recursos. EventBridge usa esta regla para notificar dichos cambios a Resource Groups. Luego, esto permite a Resource Groups generar eventos de pertenencia para enviarlos a EventBridge a que se procesen sus reglas personalizadas.

El rol vinculado al servicio solo lo puede asumir el servicio Resource Groups. Para obtener más información sobre el rol vinculado a un servicio que utiliza Resource Groups para esta característica, consulte Uso de roles vinculados a servicios para Resource Groups.

Cuando esta característica está activada, Resource Groups genera un evento al realizar cualquiera de los siguientes cambios en un grupo de recursos:

- Crear un nuevo grupo de recursos.
- Actualice la consulta que define la pertenencia al grupo de recursos basado en consultas.
- Actualice la configuración de un grupo de recursos vinculado a un servicio.

- Actualice la descripción de un grupo de recursos.
- Elimine un grupo de recursos.
- Cambie la pertenencia a un grupo de recursos agregando o quitando un recurso del grupo. Un cambio de pertenencia también puede ocurrir cuando cambian las etiquetas o cuando cambia una pila de AWS CloudFormation.

Important

- Para recibir y responder correctamente a los eventos de grupo, debe realizar cambios en Resource Groups y EventBridge. Puede realizar los cambios en cualquier orden, pero no se publicará ningún evento de grupo en los destinos de EventBridge hasta que realice cambios en ambos servicios.

- Los cambios en el grupo de recursos no incluyen los cambios en ninguna de las etiquetas adjuntas al propio grupo de recursos. Para generar eventos en función de los cambios en las etiquetas de sus grupos, debe usar una regla de EventBridge que utilice la fuente `aws.tag`, en lugar de la fuente `aws.resource-groups`. Para obtener más información, consulte Eventos de cambios de las etiquetas en los Recursos de AWS en la Guía del usuario de Amazon EventBridge.

Temas

Activación de eventos del ciclo de vida del grupo en Resource Groups

Puede recibir notificaciones sobre los cambios en el ciclo de vida de sus grupos de recursos en los eventos del ciclo de vida de los grupos. A continuación, Resource Groups proporciona información sobre los cambios de sus grupos en Amazon EventBridge. En EventBridge, puede evaluar los cambios y actuar en consecuencia mediante las reglas que defina en el EventBridge servicio.

Permisos mínimos

Para activar los eventos del ciclo de vida del grupo en su cuenta Cuenta de AWS, debe iniciar sesión como director AWS Identity and Access Management (IAM) con los siguientes permisos:

- `resource-groups:UpdateAccountSettings`
- `iam:CreateServiceLinkedRole`
- `events:PutRule`
- `events:PutTargets`
- `events:DescribeRule`
- `events:ListTargetsByRule`
- `cloudformation:DescribeStacks`
- `cloudformation:ListStackResources`
- `tag:GetResources`

Al activar por primera vez los eventos del ciclo de vida de un grupo en Cuenta de AWS, Resource Groups crea un rol vinculado a un servicio denominado. `AWSServiceRoleForResourceGroups` Esta función gestionada tiene permiso para usar una EventBridge regla gestionada por Resource Groups. La regla supervisa las etiquetas adjuntas a sus recursos y las pilas de AWS CloudFormation de su cuenta para detectar cualquier cambio. A continuación, Resource Groups publica esos cambios en el bus de eventos predeterminado de Amazon EventBridge. El servicio también crea una regla EventBridge administrada denominada`Managed.ResourceGroups.TagChangeEvents`. Esta regla captura los detalles de los cambios en las etiquetas de sus recursos. Esto permite a Resource Groups generar eventos de membresía a los que EventBridge enviarlos para que los procesen sus reglas personalizadas. De este modo, EventBridge las reglas pueden responder a los eventos enviando notificaciones a los destinos configurados de las reglas.

Tras completar estos pasos, las reglas que buscan estos eventos deberían empezar a recibirlos en unos minutos.

Puedes activar los eventos del ciclo de vida del grupo mediante la API del SDK AWS Management Console o mediante un comando de una de las AWS CLI API del SDK.

> **Note**
>
> No puedes activar los eventos del ciclo de vida de un grupo si la cuota de tus grupos de recursos es demasiado alta. Para obtener más información, consulta Cómo ver las cuotas de servicio.

AWS Management Console

Para activar los eventos del ciclo de vida del grupo en la consola de Resource Groups

1. Abra la página de configuración en la consola de Resource Groups.
2. En la sección Eventos del ciclo de vida del grupo, seleccione el interruptor junto a Las notificaciones están desactivadas.
3. En el cuadro de diálogo de confirmación, elija Activar notificaciones.

   El interruptor de características muestra Las notificaciones están activadas.

Esto completa la primera parte del proceso. Después de activar las notificaciones de eventos, puedes crear reglas en Amazon EventBridge que capturen los eventos y los envíen a Specific Servicios de AWS para su procesamiento.

AWS CLI

Para activar los eventos del ciclo de vida grupal mediante el AWS CLI o los AWS SDK

En el siguiente ejemplo, se muestra cómo utilizar el AWS CLI para activar los eventos del ciclo de vida de un grupo en Resource Groups. Introduzca el comando con el parámetro principal del servicio exactamente como se muestra. El resultado muestra tanto el estado actual como el estado deseado de la función.

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

Puede confirmar que la función está activada ejecutando el siguiente comando de ejemplo. Si ambos campos de estado muestran el mismo valor, la operación está completa.

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

Para obtener más información, consulte los siguientes recursos:

- AWS CLI — grupos de recursos de aws update-account-settings y grupos de recursos de aws get-account-settings
- UpdateAccountSettingsAPI — y GetAccountSettings

Crear una EventBridge regla para capturar los eventos del ciclo de vida del grupo y publicar las notificaciones

Puede activar los eventos del ciclo de vida de los grupos de recursos AWS Resource Groups para publicar eventos en Amazon EventBridge. A continuación, puede crear EventBridge reglas que respondan a esos eventos enviándolas a otros Servicios de AWS para su posterior procesamiento.

AWS CLI

El proceso para crear una regla EventBridge que capture los eventos y los envíe al servicio de destino deseado requiere dos comandos de CLI independientes:

1. Cree la EventBridge regla para capturar los eventos que desee
2. Adjunta a la EventBridge regla un objetivo que pueda procesar los eventos

Paso 1: Crea la EventBridge regla para capturar los eventos

El siguiente comando de AWS CLI `put-rule` ejemplo crea una EventBridge regla que captura todos los cambios en los eventos del ciclo de vida de Resource Groups.

```
$ aws events put-rule \
    --name "CatchAllResourceGroupEvents" \
```

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

El resultado incluye el Nombre de recurso de Amazon (ARN) de la nueva regla.

> **Note**
>
> Los valores de parámetros que incluyen cadenas entre comillas tienen reglas de formato diferentes según el sistema operativo y el shell que use. En los ejemplos de esta guía, mostramos los comandos que funcionan en un shell BASH de Linux. Para obtener instrucciones sobre cómo formatear cadenas con comillas incrustadas para otros sistemas operativos, como la línea de comandos de Windows, consulte Uso de comillas dentro de cadenas en la Guía del usuario de AWS Command Line Interface. A medida que las cadenas de parámetros se vuelven más complejas, puede resultar más fácil y menos propenso a errores aceptar el valor de un parámetro de un archivo de texto en lugar de escribirlo directamente en la línea de comandos.

El siguiente patrón de eventos restringe los eventos solo a aquellos que están relacionados con el grupo especificado, identificado por su ARN. Este patrón de eventos es una cadena JSON compleja que resulta mucho menos legible cuando se comprime en una cadena JSON de una sola línea escapada correctamente. En su lugar, puede guardarlo en un archivo.

Guarde la cadena JSON del patrón de eventos en un archivo. En el siguiente ejemplo de código, el archivo es `eventpattern.txt`.

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

A continuación, ejecute el siguiente comando para crear la regla, recuperando el patrón de eventos personalizado del archivo.

```
$ aws events put-rule \
    --name "CatchResourceGroupEventsForMyGroup" \
    --event-pattern file://eventpattern.txt
{
    "RuleArn": "arn:aws:events:us-east-1:123456789012:rule/
CatchResourceGroupEventsForMyGroup"
}
```

Para capturar otros tipos de eventos de Resource Groups, sustituya la cadena `--event-pattern` con filtros como los que se presentan en la sección Ejemplos de patrones de eventos EventBridge personalizados para diferentes casos de uso.

Paso 2: Adjunte a la EventBridge regla un destino que pueda procesar los eventos

Ahora que tiene una regla que captura los eventos que le interesan, puede adjuntar uno o más objetivos para procesar los eventos de algún tipo.

El siguiente comando de AWS CLI `put-targets` adjunta un tema de Amazon Simple Notification Service (Amazon SNS) denominado `my-sns-topic` a la regla que creó en el ejemplo anterior. Todos los suscriptores del tema reciben una notificación cuando se produce un cambio en el grupo especificado en la regla.

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

En este punto, cualquier cambio de grupo que coincida con el patrón de eventos de la regla se envía automáticamente al destino o los destinos configurados. Si, como en el ejemplo anterior, el objetivo es un tema de Amazon SNS, todos los suscriptores del tema recibirán un mensaje con el evento tal y como se describe en Estructura y sintaxis de los eventos del ciclo de vida de Resource Groups.

Para obtener más información, consulte los siguientes recursos:

- AWS CLI: aws events put-rule y aws events put-targets
- API, PutRuley PutTargets

Crear una regla para capturar solo tipos de eventos específicos del ciclo de vida de un grupo

Puede crear una regla con un patrón de eventos personalizado que capture solo los eventos que le interesen. Para obtener información completa sobre cómo filtrar los eventos entrantes mediante un patrón de eventos personalizado, consulta Amazon EventBridge events en la Guía del EventBridge usuario de Amazon.

Por ejemplo, supongamos que desea que una regla procese únicamente las notificaciones de Resource Groups que indican la creación de un nuevo grupo de recursos. Puede utilizar un patrón de eventos personalizado similar al siguiente ejemplo.

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

Ese filtro captura solo los eventos que tienen esos valores exactos en los campos especificados. Para ver una lista completa de los campos de los que puede hacer coincidir, consulte Estructura y sintaxis de los eventos del ciclo de vida de Resource Groups.

Desactivar los eventos del ciclo de vida del grupo

Puede desactivar los eventos del ciclo de vida de los grupos para evitar que AWS Resource Groups emita eventos a Amazon EventBridge. Puede lograrlo utilizando la AWS Management Console o mediante un comando de la AWS CLI o una de las API de SDK.

> **Note**
>
> Al desactivar los eventos del ciclo de vida de un grupo, se elimina la regla de EventBridge gestionada por Resource Groups que se utiliza para analizar las etiquetas y pilas de AWS CloudFormation en busca de cambios. Resource Groups ya no puede transferir esos cambios a EventBridge. Las reglas que haya definido en EventBridge que busquen eventos de Resource Groups dejan de recibir eventos para procesar. Si tiene intención de volver a activar los eventos del ciclo de vida del grupo en el futuro, puede deshabilitar las reglas. Si no desea volver a utilizar esas reglas, puede eliminarlas. Para obtener más

información, consulte Deshabilitar una regla de EventBridge en la Guía del usuario de Amazon EventBridge.
Al desactivar los eventos del ciclo de vida del grupo, no se elimina el rol vinculado al servicio. Puede eliminar manualmente el rol vinculado a un servicio si desea utilizar IAM. Si más adelante necesita volver a activar los eventos del ciclo de vida del grupo y el rol vinculado al servicio no existe, Resource Groups lo vuelve a crear automáticamente.

Permisos mínimos

Para desactivar los eventos del ciclo de vida grupal en su Cuenta de AWS, debe iniciar sesión como entidad principal AWS Identity and Access Management (IAM) con los siguientes permisos:

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

AWS Management Console

Para desactivar las notificaciones de eventos del ciclo de vida del grupo a EventBridge

1. Abra la página de Configuración en la consola de Resource Groups.
2. En la sección Eventos del ciclo de vida del grupo, seleccione el interruptor junto a Las notificaciones están desactivadas.
3. En el cuadro de diálogo de confirmación, elija Desactivar notificaciones.

   Aparece el interruptor de característica: Las notificaciones de eventos están desactivadas.

En este momento, Resource Groups ya no envía eventos al bus de eventos predeterminado de EventBridge y las reglas que tengas ya no reciben eventos de notificación de grupo para procesarlos. Si lo desea, puede eliminar esas reglas para completar la limpieza.

AWS CLI

Para desactivar las notificaciones de eventos del ciclo de vida del grupo a EventBridge

En el siguiente ejemplo, se muestra cómo usar la AWS CLI para desactivar los eventos del ciclo de vida de un grupo en Resource Groups.

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

Para obtener más información, consulte los siguientes recursos:

- AWS CLI: aws resource-groups update-account-settings y aws resource-groups get-account-settings
- API: UpdateAccountSettings y getAccountSettings

Estructura y sintaxis de los eventos del ciclo de vida de Resource Groups

Los eventos del ciclo de vida de AWS Resource Groups adoptan la forma de cadenas de objetos JSON con el siguiente formato general.

```
{
    "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 obtener más información sobre los campos comunes a todos los EventBridge eventos de Amazon, consulta Amazon EventBridge events en la Guía del EventBridge usuario de Amazon. Los detalles específicos de Resource Groups se explican en la siguiente tabla.

Nombre del campo	Tipo	Descripción
`detail-type`	Cadena	En el caso de Resource Groups, el campo `detail-type` tiene siempre uno de los siguientes valores: • `ResourceGroups Group State Change`: representa los cambios en el estado general del grupo y sus propiedades. • `ResourceGroups Group Membership Change`: representa los cambios en la composición del grupo.
`source`	Cadena	En el caso de Resource Groups, este valor es siempre `"aws.resource-groups"`.
`resources`	Una matriz de nombres de recursos de Amazon (ARN)	Este campo siempre incluye el Nombre de recurso de Amazon (ARN) del grupo con el cambio que desencadenó este evento. Este campo también puede incluir los ARN de cualquier recurso agregado o eliminado del grupo, si corresponde.
`detail`	Cadena de objetos JSON	Esta es la carga del evento. El contenido del campo `detail` depende del valor del campo `detail-type`. Para obtener más información, consulte la siguiente sección.

Estructura del campo **`detail`**

El campo `detail` incluye todos los detalles específicos del servicio Resource Groups sobre un cambio específico. El campo `detail` puede adoptar dos formas: un cambio de estado del grupo o un cambio de membresía, según el valor del campo `detail-type` descrito en la sección anterior.

> **Important**
>
> Los grupos de recursos de estos eventos se identifican mediante una combinación del ARN del grupo y un campo `"unique-id"` que contiene un UUID. Al incluir un UUID como parte de la identidad de un grupo de recursos, puede distinguir entre un grupo que se elimina y un grupo diferente que se crea posteriormente con el mismo nombre. Le recomendamos que trate la concatenación del ARN y el identificador único como clave para el grupo de los programas que interactúan con estos eventos.

Cambio de estado del grupo

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

Este valor `detail-type` indica que el estado del propio grupo ha cambiado, incluidos sus metadatos. Este cambio se produce cuando se crea, actualiza o elimina un grupo, tal como se indica en el campo `"change"` del `detail`.

La información incluida en la sección `details` cuando se especifica este `detail-type` incluye los campos que se describen en la siguiente tabla.

Nombre del campo	Tipo	Descripción
`event-sequence`	Doble	Un número que aumenta de forma repetitiva y que especifica la secuencia de eventos de un grupo específico. El número se restablece al eliminar el grupo y crear otro grupo con el mismo nombre.
`group`	Objeto JSON de `Group`	El objeto de grupo asociado al evento por su ARN, nombre e ID único.

Nombre del campo	Tipo	Descripción
`state-change`	Cadena	El tipo de cambio de estado que se ha producido. Puede ser cualquiera de los siguientes valores: • `create` • `update` • `delete`
`old-state`	Objeto JSON de `GroupState`	El estado del grupo antes del cambio. El objeto incluye solo los valores de las propiedades que han cambiado.
`new-state`	Objeto JSON de `GroupState`	El estado del grupo después del cambio. El objeto incluye solo los valores de las propiedades que han cambiado.

El objeto JSON de `group` contiene los elementos que se describen en la siguiente tabla.

Nombre del campo	Tipo	Descripción
`arn`	Cadena	El ARN del grupo.
`name`	Cadena	Es el nombre fácil de recordar del grupo.
`unique-id`	GUID	Un valor GUID único que distingue entre un grupo que se eliminó y un grupo diferente que se creó posteriormente con el mismo nombre y ARN. Utilice la concatenación del ARN y este valor como clave única para el grupo cuando consuma estos eventos en su código.

Los objetos JSON de `GroupState` contienen los elementos que se describen en la siguiente tabla.

Nombre del campo	Tipo	Descripción
`description`	Cadena	Descripción del grupo de recursos proporcionados por el cliente.
`resource-query`	Objeto JSON de `ResourceQuery`	Una representación en JSON de la consulta que define a los miembros del grupo. Este campo solo está presente para los grupos basados en una consulta. La sintaxis de este campo viene definida por el tipo de datos de la ResourceQuery API. Se incluyen ejemplos de esto en los ejemplos de eventos de Create y Update.
`group-configuration`	Objeto JSON de `Configuration`	Una representación en JSON de los parámetros de configuración asociados a un grupo vinculado a un servicio. Para obtener más información, consulte Configuraciones de servicio para grupos de recursos en la referencia de la API de AWS Resource Groups.

Cada uno de los siguientes ejemplos de código ilustra el contenido del campo `detail` para cada tipo de `state-change`.

Create

```
"state-change": "create"
```

El evento indica que se ha creado un grupo nuevo. El evento incluye todas las propiedades de metadatos del grupo establecidas durante la creación del grupo. Este evento suele ir seguido de uno o más eventos de pertenencia a un grupo, a menos que el grupo esté vacío. Las propiedades que tienen un valor nulo no se muestran en el cuerpo del evento.

El siguiente evento de ejemplo indica un grupo de recursos recién creado denominado `my-service-group`. En este ejemplo, el grupo usa una consulta basada en etiquetas que solo coincide con las instancias de Amazon Elastic Compute Cloud (Amazon EC2) que tienen la etiqueta `"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\"}]
                }"
            }
        }
    }
}
```

Update

`"state-change": "update"`

El evento indica que un grupo existente se modificó de alguna manera. El evento incluye solo las propiedades que cambiaron con respecto al estado anterior. Las propiedades que tienen un valor nulo no se muestran en el cuerpo del evento.

El siguiente evento de ejemplo indica que la consulta basada en etiquetas del grupo de recursos del ejemplo anterior se modificó para incluir también los recursos de volumen de Amazon EC2 en el 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"`

El evento indica que se ha eliminado un grupo existente. El campo de detalle no incluye metadatos sobre el grupo aparte de su identificación. El campo `event-sequence` se restablece después de este evento, ya que, por definición, es el último evento de este `arn` y `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"
        }
    }
}
```

Cambio de pertenencia a los grupos

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

Este valor `detail-type` indica que la pertenencia al grupo se modificó debido a la adición o eliminación de un recurso del grupo. Cuando se especifica este `detail-type`, el campo `resources` de nivel superior incluye el ARN del grupo cuya membresía se cambió y los ARN de cualquier recurso que se haya agregado o eliminado del grupo.

La información incluida en la sección `details` cuando se especifica este `detail-type` incluye los campos que se describen en la siguiente tabla.

Nombre del campo	Tipo	Descripción
`event-sequence`	Doble	Un número que aumenta de forma repetitiva y que indica la secuencia de eventos de un grupo específico. El número se restablece cuando se elimina el grupo y cambia su identificador único.
`group`	Objeto JSON de `Group`	Identifica el objeto de grupo asociado al evento por su ARN, nombre e ID único.
`resources`	Matriz de objetos JSON `ResourceChange`	Conjunto de recursos cuya pertenencia a un grupo ha cambiado. Este objeto `ResourceChange` incluye los siguientes campos para cada recurso: • `membership-change` : el valor es `"add"` o `"remove"`. • `arn`: el ARN del recurso agregado o eliminado. • `resource-type` : el tipo de recurso agregado o eliminado.

El siguiente ejemplo de código ilustra el contenido del evento para un tipo de cambio de pertenencia típico. En este ejemplo, se muestra un recurso que se agrega al grupo y otro que se quita del 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"
            }
        ]
    }
}
```

Ejemplos de patrones de eventos EventBridge personalizados para diferentes casos de uso

En el siguiente ejemplo, los patrones de eventos EventBridge personalizados filtran los eventos generados por Resource Groups y los filtran solo a aquellos que le interesen para una regla y un objetivo de eventos específicos.

En los siguientes ejemplos de código, si se necesita un grupo o recurso específico, cambie cada *`marcador de posición introducido por el usuario`* por su información.

Todos los eventos de Resource Groups

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

Eventos de cambio de estado o membresía del grupo

El siguiente ejemplo de código es para todos los cambios de estado del grupo.

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

El siguiente ejemplo de código es para todos los cambios de pertenencia del grupo.

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

Eventos para un grupo específico

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

El ejemplo anterior captura los cambios en el grupo especificado. El siguiente ejemplo hace lo mismo y también captura los cambios cuando el grupo es un recurso miembro de otro grupo.

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

Eventos para un recurso específico

Solo puede filtrar los eventos de cambio de pertenencia a un grupo para recursos de miembros específicos.

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

```
}
```

Eventos para un tipo de recurso específico

Puede utilizar la coincidencia de prefijos con los ARN para hacer coincidir los eventos de un tipo de recurso específico.

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

Como alternativa, puede utilizar la coincidencia exacta mediante identificadores `resource-type`, que podrían coincidir en más de un tipo de forma concisa. A diferencia del ejemplo anterior, el ejemplo siguiente solo coincide con los eventos de cambio de pertenencia al grupo porque los eventos de cambio de estado del grupo no incluyen un campo `resources` en su campo `detail`.

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

Todos los eventos de eliminación de recursos

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

Todos los eventos de eliminación de recursos de un 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" ]
         }
    }
}
```

No puede usar la matriz `resources` de nivel superior que se usó en el primer ejemplo de esta sección para este tipo de filtrado de eventos. Esto se debe a que un recurso del elemento `resources` de nivel superior podría ser un recurso que se está agregando a un grupo y el evento seguiría coincidiendo. En otras palabras, el siguiente ejemplo de código puede devolver eventos inesperados. En su lugar, utilice la sintaxis que se muestra en el ejemplo 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" ]
         }
     }
}
```

Eliminar grupos de recursos de AWS Resource Groups

Puede utilizar la consola de AWS Resource Groups o la AWS CLI para eliminar grupos de recursos de AWS Resource Groups. La eliminación de un grupo de recursos no elimina los recursos que pertenecen al grupo ni las etiquetas de dichos recursos. Solo elimina la estructura del grupo y las etiquetas a nivel de grupo.

Console

Para eliminar grupos de recursos

1. Inicie sesión en la consola de AWS Resource Groups.
2. En el panel de navegación, elija Grupos de recursos guardados.
3. Seleccione el nombre del grupo de recursos que desea eliminar y, a continuación, seleccione Ver detalles.
4. En la página de detalles del grupo, seleccione Eliminar en la esquina superior derecha.
5. Cuando se le pida que confirme la eliminación, elija Eliminar.

AWS CLI & AWS SDKs

Para eliminar grupos de recursos

1. Ejecute el siguiente comando, sustituyendo *resource_group_name* por el nombre de su grupo.

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

2. Cuando se le pida que confirme la eliminación, escriba `yes` y, a continuación, pulse Intro.

AWS servicios que funcionan con AWS Resource Groups

Puede utilizar los siguientes AWS servicios con AWS Resource Groups.

AWS servicio	Uso con Resource Groups
AWS CloudFormation— Cree grupos de recursos AWS CloudFormation mediante una plantilla de pila.	Aprovisione y organice AWS los recursos al mismo tiempo. Organice los recursos por etiquetas. Organice los recursos de otra pila. Recopile información sobre sus AWS recursos en grupos de recursos mediante Amazon CloudWatch o emprenda acciones operativas utilizando AWS Systems Manager.

AWS servicio	Uso con Resource Groups
	Para obtener más información, consulte la referencia sobre ResourceGroups los tipos de recursos en la Guía del AWS CloudFormation usuario.
CloudTrail— Capture todas las acciones del grupo de recursos utilizando AWS CloudTrail.	Recopile información sobre las acciones realizadas en sus grupos de recursos, incluidos detalles como quién realizó la acción (el responsable de IAM, como un rol, un usuario o un rol Servicio de AWS), cuándo se realizó la acción, dónde se produjo la acción (la dirección IP de origen) y más. Luego, estos registros se pueden usar para el análisis o para activar acciones de seguimiento. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.
Amazon CloudWatch: habilite la supervisión en tiempo real de sus AWS recursos y las aplicaciones en las que se ejecuta AWS.	Puede centrar su vista para ver estadísticas y alarmas desde un único grupo de recursos. Para obtener más información, consulte Centrarse en las métricas y las alarmas de un grupo de recursos en la Guía del CloudWatch usuario de Amazon.
Información sobre las CloudWatch aplicaciones de Amazon: detecte problemas comunes con sus aplicaciones basadas en SQL Server y .NET.	Supervise los recursos de .NET y SQL Server que pertenecen a un grupo de recursos. Para obtener más información, consulte Componentes de aplicaciones compatibles en la Guía del CloudWatch usuario de Amazon.

AWS servicio	Uso con Resource Groups
Grupos de tablas de Amazon DynamoDB: organice las tablas de DynamoDB en agrupaciones lógicas para poder administrar sus recursos con mayor facilidad.	Cree, edite y elimine grupos de tablas de DynamoDB desde el menú de acciones de DynamoDB. Para obtener más información, consulte la Guía del desarrollador de Amazon DynamoDB.
Hosts dedicados de Amazon EC2: use las licencias de software existentes por conector, por núcleo o por VM, incluido Windows Server, Microsoft SQL Server, SUSE y Linux Enterprise Server.	Lance instancias de Amazon EC2 en grupos de recursos de host para maximizar el uso de hosts dedicados. Para obtener más información, consulte Trabajar con hosts dedicados en la Guía del usuario de Amazon EC2.
Reservas de capacidad de Amazon EC2: reserve capacidad para que sus instancias de Amazon EC2 la utilicen cuando la necesiten. Puede especificar los atributos de la reserva de capacidad para que solo funcione con las instancias de Amazon EC2 que se lanzan con atributos coincidentes.	Lance sus instancias de Amazon EC2 en grupos de recursos que contengan una o más reservas de capacidad. Si el grupo no tiene una reserva de capacidad con atributos coincidentes y capacidad disponible para una instancia solicitada, la instancia se ejecuta como una instancia bajo demanda. Si posteriormente añade una reserva de capacidad coincidente al grupo de destino, la instancia se emparejará automáticamente con la capacidad reservada y se moverá a ella. Para obtener más información, consulte Trabajar con grupos de reserva de capacidad en la Guía del usuario de Amazon EC2.

AWS servicio	Uso con Resource Groups
AWS License Manager: simplifica el proceso de llevar licencias de proveedores de software a la nube.	Configure un grupo de recursos de hosts para permitir que License Manager administre sus hosts dedicados. Para obtener más información, consulte Grupos de recursos de host en License Manager en la Guía del usuario de License Manager.
AWS Resilience Hub: prepare y proteja sus aplicaciones de las interrupciones.	Descubra las aplicaciones que se definen mediante Resource Groups. Para obtener más información, consulte Mida y mejore la resiliencia de sus aplicaciones con AWS Resilience Hub en el blog de noticias de AWS .
AWS Resource Access Manager— Comparta AWS los recursos específicos de su propiedad con otras cuentas.	Comparta los grupos de recursos del anfitrión mediante AWS RAM. Para obtener más información, consulte Recursos compartibles en la Guía del usuario de AWS RAM .
AWS Service Catalog AppRegistry: Defina y gestione sus aplicaciones y metadatos.	Al crear una aplicación en AppRegistry, ese servicio crea automáticamente un grupo de recursos para esa aplicación. El grupo de recursos de la aplicación es un conjunto de todos los recursos de la aplicación. El servicio también crea un grupo de recursos AWS CloudFormation basado en pilas para cada pila asociada a la aplicación. Para obtener más información, consulte Utilización AppRegistry en la Guía del AWS Service Catalog administrador.

AWS servicio	Uso con Resource Groups
AWS Systems Manager— Habilite la visibilidad y el control de sus AWS recursos.	Recopile información operativa y lleve a cabo acciones masivas en sus aplicaciones basadas en grupos de recursos. En la AWS Systems Manager consola, la página de aplicaciones personalizadas de Application Manager importa y muestra automáticamente los datos de operaciones de las aplicaciones que se basan en grupos de recursos. Puede utilizar la información de Application Manager para ayudarle a determinar qué recursos de una aplicación son conformes y funcionan correctamente y qué recursos requieren una acción. Para obtener más información, consulte Uso de aplicaciones en Application Manager en la Guía del usuario de AWS Systems Manager .
Analizador de acceso a la red Amazon VPC: identifique el acceso no deseado a los recursos de la red en AWS.	Puede especificar los orígenes y los destinos para sus requisitos de acceso a la red mediante AWS Resource Groups. Esto le permite controlar el acceso a la red en todo su AWS entorno, independientemente de cómo configure la red. Para obtener más información, consulte Utilizar Resource Groups con Network Access Scopes en la Guía del usuario de Amazon Virtual Private Cloud.

Configuraciones de servicios para grupos de recursos

Los grupos de recursos le permiten administrar las colecciones de sus AWS recursos como una unidad. Algunos servicios de AWS lo respaldan mediante la realización de las operaciones solicitadas en todos los miembros del grupo. Estos servicios pueden almacenar los ajustes que se

aplicarán a los miembros del grupo como una configuración en forma de estructura de datos JSON adjunta al grupo.

Este tema describe los ajustes de configuración disponibles para los servicios de AWS admitidos.

Temas

- Cómo acceder a la configuración del servicio adjunta a un grupo de recursos
- Sintaxis JSON de la configuración de un servicio
- Tipos de configuración y parámetros admitidos

Cómo acceder a la configuración del servicio adjunta a un grupo de recursos

Los servicios que admiten grupos vinculados a servicios suelen establecer la configuración automáticamente cuando se utilizan las herramientas que proporciona ese servicio, como la consola de administración del servicio o sus operaciones AWS CLI y las del AWS SDK. Algunos servicios administran completamente sus grupos vinculados a servicios y no puedes modificarlos de ninguna manera excepto según lo permitan la consola o los comandos proporcionados por el servicio propietario. AWS Sin embargo, en algunos casos, puedes interactuar con la configuración del servicio mediante las siguientes operaciones de API en los AWS SDK o sus equivalentes: AWS CLI

- Puede adjuntar su propia configuración a un grupo al crear el grupo mediante la CreateGroupoperación.
- Puede modificar la configuración actual adjunta a un grupo mediante la PutGroupConfigurationoperación.
- Puede ver la configuración actual de un grupo de recursos llamando a la GetGroupConfigurationoperación.

Sintaxis JSON de la configuración de un servicio

Un grupo de recursos puede contener una configuración que define los ajustes específicos del servicio aplicables a los recursos que son miembros de ese grupo.

Una configuración se expresa como un objeto JSON. En el nivel más alto, una configuración es una matriz de elementos de configuración de grupo. Cada elemento de configuración de grupo contiene dos elementos: un `Type` para la configuración y un conjunto de `Parameters` definidos por ese tipo.

Cada parámetro contiene un `Name` y un conjunto de uno o más `Values`. El siguiente ejemplo con *`marcadores de posición`* muestra la sintaxis básica de una configuración para un único tipo de recurso de muestra. En este ejemplo, se muestra un tipo con dos parámetros y cada parámetro con dos valores. Los tipos, parámetros y valores válidos se describen en la siguiente sección.

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

Tipos de configuración y parámetros admitidos

Los Resource Groups admiten el uso de los siguientes tipos de configuración. Cada tipo de configuración tiene un conjunto de parámetros válidos para ese tipo.

Temas

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

- AWS::NetworkFirewall::RuleGroup

AWS::ResourceGroups::Generic

Este tipo de configuración especifica los ajustes que imponen los requisitos de pertenencia al grupo de recursos, en lugar de configurar el comportamiento de un tipo de recurso específico para un AWS servicio. Este tipo de configuración es agregada automáticamente por aquellos grupos vinculados a servicios que lo necesiten, como los tipos `AWS::EC2::CapacityReservationPool` y `AWS::EC2::HostManagment`.

Los siguientes `Parameters` son válidos para el `Type` de grupo vinculado al `AWS::ResourceGroups::Generic`.

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

  Este parámetro especifica que el grupo de recursos puede constar únicamente de recursos del tipo o tipos especificados.

  Tipo de datos de valores: cadena

  Valores permitidos:

  - `AWS::EC2::Host`: una `Configuration` con este parámetro y valor es obligatoria cuando la configuración del servicio también contiene una `Configuration` de tipo `AWS::EC2::HostManagement`. Esto garantiza que el grupo `HostManagement` solo pueda contener hosts dedicados de Amazon EC2.
  - `AWS::EC2::CapacityReservation`: se requiere una `Configuration` con este parámetro y valor cuando la configuración del servicio también contiene un elemento de `Configuration` de tipo `AWS::EC2::CapacityReservationPool`. Esto garantiza que un grupo `CapacityReservation` solo pueda contener la reserva de capacidad de Amazon EC2.

  Obligatorio: condicional, en función de otros elementos de `Configuration` asociados al grupo de recursos. Consulte la entrada anterior para ver los valores permitidos.

  El siguiente ejemplo restringe a los miembros del grupo a solo las instancias de host de Amazon EC2.

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

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

- **`deletion-protection`**

  Este parámetro especifica que el grupo de recursos no se puede eliminar a menos que no contenga miembros. Para obtener más información, consulte Grupos de recursos de host en la Guía del usuario de License Manager.

  Tipo de datos de valores: matriz de cadenas

  Valores permitidos: el único valor permitido es `[ "UNLESS_EMPTY" ]` (el valor debe estar en mayúsculas).

  Obligatorio: condicional, en función de otros elementos de `Configuration` vinculados al grupo de recursos. Este parámetro solo es obligatorio cuando el grupo de recursos también tiene otro elemento de `Configuration` con el `Type` de `AWS::EC2::HostManagement`.

  El siguiente ejemplo habilita la protección contra la eliminación del grupo, a menos que el grupo no tenga miembros.

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

`AWS::AppRegistry::Application`

Este `Configuration` tipo especifica que el grupo de recursos representa una aplicación creada por AWS Service Catalog AppRegistry.

El AppRegistry servicio administra completamente los grupos de recursos de este tipo y los usuarios no pueden crearlos, actualizarlos ni eliminarlos de otra manera que no sea mediante las herramientas que proporciona AppRegistry.

> **Note**
>
> Como los grupos de recursos de este tipo los crea y mantiene automáticamente el usuario AWS y no los administra, estos grupos de recursos no se tienen en cuenta para el límite de cuota del número máximo de grupos de recursos que puede crear en su cuenta Cuenta de AWS.

Para obtener más información, consulte Utilización AppRegistry en la Guía del usuario de Service Catalog.

Cuando AppRegistry crea un grupo de recursos vinculado a un servicio de este tipo, también crea automáticamente un grupo AWS CloudFormation vinculado a un servicio adicional e independiente para cada AWS CloudFormation pila asociada a la aplicación.

AppRegistry nombra automáticamente los grupos de este tipo vinculados a servicios que crea con el prefijo `AWS_AppRegistry_Application-` seguido del nombre de la aplicación: `AWS_AppRegistry_Application-`*`MyAppName`*

Los siguientes parámetros son admitidos para el tipo de grupo vinculado a un servicio `AWS::AppRegistry::Application`.

- **`Name`**

  Este parámetro especifica el nombre descriptivo de la aplicación que asignó el usuario cuando se creó en. AppRegistry

  Tipo de datos de valores: cadena

  Valores permitidos: cualquier cadena de texto permitida por el AppRegistry servicio para el nombre de una aplicación.

Obligatorio: sí

- **`Arn`**

  Este parámetro especifica la ruta del nombre de recurso de Amazon (ARN) de la aplicación asignada por. AppRegistry

  Tipo de datos de valores: cadena

  Valores permitidos: un ARN válido.

  Obligatorio: sí

> **Note**
>
> Para cambiar cualquiera de estos elementos, debe modificar la aplicación mediante la AppRegistry consola o el AWS SDK y AWS CLI las operaciones de ese servicio.

Este grupo de recursos de aplicaciones incluye automáticamente como miembros del grupo los grupos de recursos creados para las AWS CloudFormation pilas asociadas a la AppRegistry aplicación. Puede usar la ListGroupResourcesoperación para ver esos grupos secundarios.

El siguiente ejemplo muestra el aspecto de la sección de configuración de un grupo vinculado a un servicio `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

Este `Configuration` tipo especifica que el grupo representa una AWS CloudFormation pila y sus miembros son los AWS recursos creados por esa pila.

Los grupos de recursos de este tipo se crean automáticamente al asociar una AWS CloudFormation pila al AppRegistry servicio. No puede crear, actualizar ni eliminar estos grupos excepto mediante las herramientas que proporciona AppRegistry.

AppRegistry nombra automáticamente los grupos de este tipo vinculados a servicios que se crean con el prefijo `AWS_CloudFormation_Stack-` seguido del nombre de la pila: `AWS_CloudFormation_Stack-`*`MyStackName`*

> **Note**
>
> Como los grupos de recursos de este tipo los crea y mantiene automáticamente el usuario AWS y no los administra, estos grupos de recursos no se tienen en cuenta para el límite de cuota del número máximo de grupos de recursos que puede crear en su. Cuenta de AWS

Para obtener más información, consulte Utilización AppRegistry en la Guía del usuario de Service Catalog.

AppRegistry crea automáticamente un grupo de recursos de este tipo vinculado a un servicio para cada AWS CloudFormation pila que asocie a la AppRegistry aplicación. Estos grupos de recursos se convierten en miembros secundarios del grupo de recursos principal de la AppRegistry aplicación.

Los miembros de este grupo de AWS CloudFormation recursos son los AWS recursos creados como parte de la pila.

Los siguientes parámetros son admitidos para el tipo de grupo vinculado a un servicio `AWS::CloudFormation::Stack`.

- **`Name`**

  Este parámetro especifica el nombre descriptivo de la AWS CloudFormation pila asignado por el usuario cuando se creó la pila.

  Tipo de datos de valores: cadena

  Valores permitidos: cualquier cadena de texto permitida por el AWS CloudFormation servicio para el nombre de una pila.

  Obligatorio: sí

- **`Arn`**

  Este parámetro especifica la ruta del nombre de recurso de Amazon (ARN) de la AWS CloudFormation pila adjunta a la aplicación en. AppRegistry

  Tipo de datos de valores: cadena

  Valores permitidos: un ARN válido.

  Obligatorio: sí

> **Note**
>
> Para cambiar cualquiera de estos elementos, debe modificar la aplicación mediante la AppRegistry consola o un AWS SDK y AWS CLI operaciones equivalentes.

El siguiente ejemplo muestra el aspecto de la sección de configuración de un grupo `AWS::CloudFormation::Stack` vinculado a un servicio.

```
{
    "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

Este tipo de `Configuration` especifica que el grupo de recursos representa un conjunto común de capacidad proporcionado por los miembros del grupo. Los miembros de este grupo de recursos deben ser reservas de capacidad de Amazon EC2. Un grupo de recursos puede incluir tanto las reservas de capacidad que usted posea en su cuenta como las reservas de capacidad que se compartan con usted desde otras cuentas mediante el uso AWS Resource Access Manager. Esto le permite lanzar una instancia de Amazon EC2 utilizando este grupo de recursos como valor para el parámetro de reserva de capacidad. Al hacerlo, la instancia utiliza la capacidad reservada disponible en el grupo. Si el grupo de recursos no tiene capacidad disponible, la instancia se lanza de forma independiente bajo demanda fuera del grupo. Para obtener más información, consulte Trabajar con grupos de reserva de capacidad en la Guía del usuario de Amazon EC2.

Si configura un grupo de recursos vinculado a un servicio con un elemento de `Configuration` de este tipo, también debe especificar elementos de `Configuration` independientes con los siguientes valores:

- Un tipo `AWS::ResourceGroups::Generic` con un parámetro:
  - El parámetro `allowed-resource-types` y un valor único de `AWS::EC2::CapacityReservation`. Esto garantiza que solo las reservas de capacidad de Amazon EC2 puedan ser miembros del grupo de recursos.

El elemento `AWS::EC2::CapacityReservationPool` en una configuración de grupo no admite ningún parámetro.

El siguiente ejemplo muestra el aspecto de la sección de `Configuration` de un grupo de este tipo.

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

`AWS::EC2::HostManagement`

Este identificador especifica la configuración de la administración del host de Amazon EC2 y AWS License Manager que se aplica a los miembros del grupo. Para obtener más información, consulte Alojar grupos de recursos en AWS License Manager.

Si configura un grupo de recursos vinculado a un servicio con un elemento de `Configuration` de este tipo, también debe especificar elementos de `Configuration` independientes con los siguientes valores:

- Un tipo de `AWS::ResourceGroups::Generic`, con un parámetro de `allowed-resource-types` y un valor único de `AWS::EC2::Host`. Esto garantiza que solo los hosts dedicados de Amazon EC2 puedan ser miembros del grupo.
- Un tipo de `AWS::ResourceGroups::Generic`, con un parámetro de `deletion-protection` y un valor único de `UNLESS_EMPTY`. Esto garantiza que el grupo no se pueda eliminar a menos que esté vacío.

Los siguientes parámetros son admitidos para el tipo de grupo vinculado a un servicio `AWS::EC2::HostManagement`.

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

  Además, permite administrar si las instancias se lanzan en un host dedicado específico o en cualquier host disponible con una configuración coincidente. Para obtener más información, consulte Comprensión de la colocación automática y la afinidad en la Guía del usuario de Amazon EC2.

  Tipo de datos de valores: booleano

  Valores permitidos: “verdadero” o “falso” (debe estar en minúsculas).

  Obligatorio: no

```
{
    "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`**

  Este parámetro especifica si un host dedicado del grupo se libera automáticamente una vez finalizada su última instancia en ejecución. Para obtener más información, consulte Lanzamiento de hosts dedicados en la Guía del usuario de Amazon EC2.

  Tipo de datos de valores: booleano

  Valores permitidos: “verdadero” o “falso” (debe estar en minúsculas).

  Obligatorio: no

```
{
    "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`**

  Este parámetro especifica qué familias de tipos de instancias pueden usar las instancias que son miembros de este grupo.

Tipo de datos de valores: matriz de cadenas.

Valores permitidos: cada uno debe ser un identificador de familia de tipos de instancias Amazon EC2 válido, como `C4`, `M5`, `P3dn` o `R5d`.

Obligatorio: no

El siguiente elemento de configuración a modo de ejemplo especifica que las instancias lanzadas solo pueden ser miembros de las familias de tipos de instancias C5 o 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`**

  Este parámetro especifica las rutas del Nombre de recurso de Amazon (ARN) de una o más configuraciones de licencia basadas en núcleos o sockets que desea que se apliquen a los miembros del grupo.

Tipo de datos de valores: matriz de ARN.

Valores permitidos: cada uno debe ser un ARN de configuración de License Manager válido.

Obligatorio: condicional. Puede especificar este parámetro o `any-host-based-license-configuration`, pero no ambos. Algunas opciones se excluyen mutuamente.

El siguiente elemento de configuración a modo de ejemplo especifica que los miembros del grupo pueden usar las dos configuraciones de License Manager especificadas.

```
{
    "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`**

  Este parámetro especifica que no desea asociar una configuración de licencia específica a su grupo. En este caso, todas las configuraciones de licencia basadas en núcleos o sockets están disponibles para los miembros del grupo de recursos de su host. Use este ajuste si tiene un número ilimitado de licencias y desea optimizarlas para el uso del host.

  Tipo de datos de valores: booleano

  Valores permitidos: “verdadero” o “falso” (debe estar en minúsculas).

  Obligatorio: condicional. Puede especificar este parámetro o `allowed-host-based-license-configurations`, pero no ambos. Algunas opciones se excluyen mutuamente.

  El siguiente elemento de configuración a modo de ejemplo especifica que los miembros del grupo pueden usar cualquier configuración de licencia basada en núcleos o sockets.

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

```
}
```

El siguiente ejemplo ilustra la forma de incluir todos los ajustes de administración del host en una sola configuración.

```
{
    "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

Este identificador especifica la configuración de los grupos de AWS Network Firewall reglas que se aplica a los miembros del grupo. Los administradores de firewall pueden especificar el ARN de un grupo de recursos de este tipo para resolver automáticamente las direcciones IP de los miembros del grupo para una regla de firewall, en lugar de tener que enumerar cada dirección manualmente. Para obtener más información, consulte Uso de grupos de recursos basados en etiquetas en AWS Network Firewall.

Puede crear grupos de recursos de este tipo de configuración mediante la consola de Network Firewall o ejecutando un AWS CLI comando o una operación de AWS SDK.

Los grupos de recursos de este tipo de configuración tienen las siguientes restricciones:

- Los miembros del grupo se componen únicamente de recursos de los tipos admitidos por Network Firewall.
- El grupo debe contener una consulta basada en etiquetas para administrar la pertenencia al grupo; todos los recursos de los tipos admitidos con etiquetas que coincidan con la consulta se convierten automáticamente en miembros del grupo.
- No se admiten `Parameters` para este tipo de configuración.
- Para eliminar un grupo de recursos de este tipo de configuración, ningún grupo de reglas de Network Firewall puede hacer referencia a él.

El siguiente ejemplo ilustra las secciones de `ResourceQuery` y `Configuration` de un grupo de este tipo.

```
{
    "Configuration": [
        {
            "Type": "AWS::NetworkFirewall::RuleGroup",
            "Parameters": []
        }
```

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

El siguiente AWS CLI comando de ejemplo crea un grupo de recursos con la configuración y la consulta anteriores.

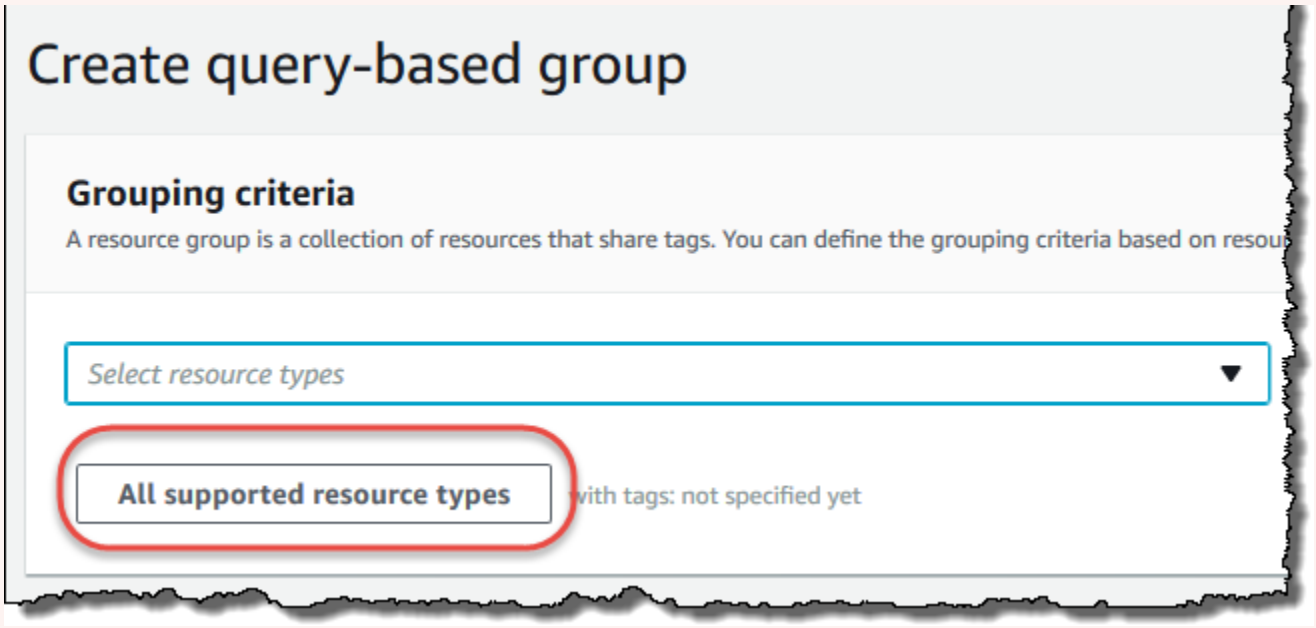
```
$ aws resource-groups create-group \
    --name test-group \
    --resource-query '{"Type": "TAG_FILTERS_1_0", "Query": "{\"ResourceTypeFilters\":
 [\"AWS::EC2::Instance\"], \"TagFilters\": [{\"Key\": \"environment\", \"Values\":
 [\"production\"]}]}"}' \
    --configuration '[{"Type": "AWS::NetworkFirewall::RuleGroup", "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 puede usar con un AWS Resource Groups editor de etiquetas

Puede utilizar el AWS Management Console o el AWS CLI para crear grupos de recursos y, a continuación, interactuar con los recursos de los miembros a través de esos grupos. Puede añadir etiquetas a muchos AWS recursos y, a continuación, utilizarlas para administrar la pertenencia a los grupos. En este tema se describen los tipos de AWS recursos que puede incluir en los grupos de recursos mediante AWS Resource Groups el uso y los tipos de recursos que puede etiquetar mediante el editor de etiquetas.

Important

Un grupo de recursos basado en una consulta para Todos los tipos de recursos admitidos puede añadir miembros automáticamente con el paso del tiempo, a medida que haya nuevos recursos admitidos por Resource Groups. Cuando ejecute automatizaciones u otras tareas por lotes con un grupo de recursos existente basado en Todos los tipos de recursos admitidos, tenga en cuenta que es posible que las acciones se ejecuten en muchos más recursos de los que estaban en el grupo la primera vez que lo creó. Esto también puede significar que las automatizaciones o tareas que haya creado para otros recursos se apliquen a recursos posiblemente no deseados o a recursos en los que las tareas no se puedan completar correctamente. En esos casos, puede agregar un filtro de tipo de recurso para especificar que solo los recursos de los tipos especificados puedan formar parte del grupo.



En las tablas siguientes se enumeran los tipos de recursos que se admiten para etiquetar en Tag Editor, para pertenecer a grupos basados en consultas de etiquetas y para pertenecer a grupos basados en AWS CloudFormation pilas.

Definiciones de columnas

- Etiquetado de Tag Editor: puede etiquetar recursos de este tipo mediante la consola de Tag Editor. De lo contrario, debe utilizar AWS Resource Groups Tagging API o los servicios de etiquetado admitidos de forma nativa por el servicio propietario de ese recurso.
- Grupos basados en etiquetas: puede incluir recursos de este tipo en grupos de recursos cuya pertenencia viene determinada por las etiquetas adjuntas a los recursos. El grupo especifica los nombres y valores de las claves de las etiquetas, y cualquier recurso con etiquetas que coincidan pasa automáticamente a formar parte del grupo
- AWS CloudFormation Grupos basados en pilas: puede incluir recursos de este tipo en grupos de recursos cuyos miembros estén compuestos por los recursos creados como parte de una pila. CloudFormation El grupo especifica el ARN de la pila y todos sus recursos pertenecen automáticamente al grupo. Al añadir etiquetas a una AWS CloudFormation pila, se actualiza la pila.

Para obtener una lista de los tipos de recursos que están obsoletos y que ya no son admitidos por Resource Groups, consulte la sección Tipos de recursos obsoletos al final de este tema.

> **Note**
>
> Resource Groups y Tag Editor admiten los tipos de recursos de la tabla siguiente, pero es posible que algunos tipos de recursos no estén disponibles en la suya Región de AWS.

Amazon API Gateway

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::ApiGateway::Account`	✗ No	✗ No	✓ Sí
`AWS::ApiGateway::ApiKey`	✗ No	✓ Sí	✓ Sí
`AWS::ApiGateway::ClientCertificate`	✗ No	✓ Sí	✗ No
`AWS::ApiGateway::DomainName`	✗ No	✗ No	✓ Sí
`AWS::ApiGateway::RestApi`	✗ No	✓ Sí	✓ Sí
`AWS::ApiGateway::Stage`	✗ No	✓ Sí	✗ No
`AWS::ApiGateway::UsagePlan`	✗ No	✓ Sí	✓ Sí

Amazon API Gateway V2

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::ApiGatewayV2::Api`	✗ No	✓ Sí	✗ No

Analizador de acceso de IAM

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::AccessAnalyzer::Analyzer`	✗ No	✓ Sí	✗ No

AWS Amplify

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Amplify::App`	✗ No	✓ Sí	✗ No

AWS App Mesh

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::AppMesh::Mesh`	✗ No	✓ Sí	✗ No

Amazon AppStream

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en Stack
`AWS::AppStream::AppBlock`	✗ No	✓ Sí	✗ No
`AWS::AppStream::Application`	✗ No	✓ Sí	✗ No
`AWS::AppStream::Fleet`	✓ Sí	✓ Sí	✓ Sí
`AWS::AppStream::ImageBuilder`	✓ Sí	✓ Sí	✓ Sí
`AWS::AppStream::Stack`	✓ Sí	✓ Sí	✓ Sí

AWS AppSync

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::AppSync::DataSource`	✗ No	✗ No	✓ Sí
`AWS::AppSync::GraphQLApi`	✗ No	✗ No	✓ Sí

Amazon Athena

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Athena::DataCatalog`	✗ No	✓ Sí	✗ No
`AWS::Athena::WorkGroup`	✗ No	✓ Sí	✗ No

AWS Backup

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Backup::BackupPlan`	✗ No	✓ Sí	✗ No
`AWS::Backup::BackupVault`	✗ No	✓ Sí	✗ No
`AWS::Backup::ReportPlan`	✗ No	✓ Sí	✗ No

AWS Batch

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::Batch::ComputeEnvironment	✗ No	✓ Sí	✗ No
AWS::Batch::JobQueue	✗ No	✓ Sí	✗ No
AWS::Batch::SchedulingPolicy	✗ No	✓ Sí	✗ No

AWS Billing Conductor

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::BillingConductor::BillingGroup	✗ No	✓ Sí	✓ Sí
AWS::BillingConductor::CustomLineItem	✗ No	✓ Sí	✓ Sí
AWS::BillingConductor::PricingPlan	✗ No	✓ Sí	✓ Sí
AWS::BillingConductor::PricingRule	✗ No	✓ Sí	✓ Sí

Amazon Braket

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Braket::Job`	✗ No	✓ Sí	✗ No
`AWS::Braket::QuantumTask`	✓ Sí	✓ Sí	✗ No

AWS Certificate Manager

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::CertificateManager::Certificate`	✓ Sí	✓ Sí	✓ Sí

AWS Certificate Manager Autoridad de certificación privada

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::ACMPCA::CertificateAuthority`	✗ No	✓ Sí	✗ No

AWS Cloud9

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Cloud9::Environment`	✓ Sí	✓ Sí	✗ No

AWS CloudFormation

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::CloudFormation::Stack`	✓ Sí	✓ Sí	✓ Sí

Amazon CloudFront

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en Stack
`AWS::CloudFront::Distribution`	✓ Sí[1]	✓ Sí[2]	✓ Sí[2]

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en Stack
`AWS::CloudFront::StreamingDistribution`	✓ Sí[1]	✓ Sí[2]	✓ Sí[2]

[1] Este es un recurso para un servicio global alojado en la región Este de EE. UU. (Norte de Virginia). Si quiere usar el Tag Editor para crear o modificar etiquetas para este tipo de recurso, debe incluir el `us-east-1` en la lista Seleccionar regiones, en la sección Buscar recursos para etiquetar, en la consola de Tag Editor.

[2] Este es un recurso para un servicio global alojado en la región Este de EE. UU. (Norte de Virginia). Como los Resource Groups se mantienen por separado para cada región, debe AWS Management Console cambiarlos por uno Región de AWS que contenga los recursos que desee incluir en el grupo. Para crear un grupo de recursos que contenga un recurso global, debe configurar su us-east-1 AWS Management Console para EE. UU. Este (Virginia del Norte) mediante el selector de regiones situado en la esquina superior derecha del. AWS Management Console

AWS Cloud Map

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::ServiceDiscovery::Service`	✗ No	✓ Sí	✗ No

AWS CloudTrail

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::CloudTrail::Channel`	✗ No	✓ Sí	✗ No
`AWS::CloudTrail::EventDataStore`	✗ No	✓ Sí	✗ No
`AWS::CloudTrail::Trail`	✓ Sí	✓ Sí	✓ Sí

Amazon CloudWatch

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en Stack
`AWS::CloudWatch::Alarm`	✓ Sí	✓ Sí	✓ Sí
`AWS::CloudWatch::Dashboard`	✗ No	✗ No	✓ Sí
`AWS::CloudWatch::InsightRule`	✗ No	✓ Sí	✗ No
`AWS::CloudWatch::MetricStream`	✗ No	✓ Sí	✗ No
`AWS::CloudWatch::ServiceLevelObjective`	✗ No	✓ Sí	✗ No

Amazon CloudWatch Logs

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Logs::Destination`	✗ No	✓ Sí	✗ No
`AWS::Logs::LogGroup`	✗ No	✓ Sí	✓ Sí

Amazon CloudWatch Synthetics

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Synthetics::Canary`	✗ No	✓ Sí	✓ Sí

AWS CodeArtifact

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::CodeArtifact::Domain`	✓ Sí	✓ Sí	✓ Sí

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::CodeArtifact::Repository`	✓ Sí	✓ Sí	✓ Sí

AWS CodeBuild

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::CodeBuild::Project`	✓ Sí	✓ Sí	X No

AWS CodeCommit

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::CodeCommit::Repository`	✓ Sí	✓ Sí	X No

AWS CodeDeploy

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::CodeDeploy::Application`	✗ No	✓ Sí	✓ Sí
`AWS::CodeDeploy::DeploymentConfig`	✗ No	✗ No	✓ Sí

CodeGuru Revisor de Amazon

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en Stack
`AWS::CodeGuruReviewer::RepositoryAssociation`	✓ Sí	✓ Sí	✓ Sí

Amazon CodeGuru Profiler

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::CodeGuruProfiler::ProfilingGroup`	✗ No	✓ Sí	✗ No

AWS CodePipeline

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::CodePipeline::CustomActionType`	✗ No	✓ Sí	✗ No
`AWS::CodePipeline::Pipeline`	✓ Sí	✓ Sí	✓ Sí
`AWS::CodePipeline::Webhook`	✓ Sí	✓ Sí	✓ Sí

AWS CodeConnections

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::CodeStarConnections::Connection`	✗ No	✓ Sí	✗ No

Amazon Cognito

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Cognito::IdentityPool`	✓ Sí	✓ Sí	✓ Sí
`AWS::Cognito::UserPool`	✓ Sí	✓ Sí	✓ Sí

Amazon Comprehend

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Comprehend::DocumentClassifier`	✓ Sí	✓ Sí	✗ No

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Comprehend::EntityRecognizer`	✓ Sí	✓ Sí	✗ No

AWS Config

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Config::AggregationAuthorization`	✗ No	✓ Sí	✗ No
`AWS::Config::ConfigRule`	✓ Sí	✓ Sí	✗ No
`AWS::Config::ConfigurationAggregator`	✗ No	✓ Sí	✗ No
`AWS::Config::StoredQuery`	✗ No	✓ Sí	✗ No

Amazon Connect

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Connect::Instance`	✗ No	✓ Sí	✗ No
`AWS::Connect::PhoneNumber`	✗ No	✓ Sí	✗ No

Amazon Connect Wisdom

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Wisdom::Assistant`	✗ No	✓ Sí	✓ Sí
`AWS::Wisdom::AssistantAssociation`	✗ No	✓ Sí	✓ Sí
`AWS::Wisdom::Content`	✗ No	✓ Sí	✗ No
`AWS::Wisdom::KnowledgeBase`	✗ No	✓ Sí	✓ Sí
`AWS::Wisdom::Session`	✗ No	✓ Sí	✗ No

AWS Data Exchange

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::DataExchange::DataSet`	✓ Sí	✓ Sí	✗ No
`AWS::DataExchange::Revision`	✗ No	✓ Sí	✗ No

AWS Data Pipeline

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::DataPipeline::Pipeline`	✓ Sí	✓ Sí	✓ Sí

AWS DataSync

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::DataSync::Task`	✗ No	✓ Sí	✗ No

AWS Database Migration Service

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::DMS::Certificate`	✓ Sí	✓ Sí	✗ No
`AWS::DMS::Endpoint`	✓ Sí	✓ Sí	✓ Sí
`AWS::DMS::EventSubscription`	✓ Sí	✓ Sí	✗ No
`AWS::DMS::ReplicationInstance`	✓ Sí	✓ Sí	✓ Sí
`AWS::DMS::ReplicationSubnetGroup`	✓ Sí	✓ Sí	✗ No
`AWS::DMS::ReplicationTask`	✓ Sí	✓ Sí	✗ No

AWS Device Farm

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::DeviceFarm::InstanceProfile`	✗ No	✓ Sí	✗ No
`AWS::DeviceFarm::Project`	✗ No	✓ Sí	✗ No
`AWS::DeviceFarm::TestGridProject`	✗ No	✓ Sí	✗ No

Amazon DynamoDB

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::DynamoDB::Table`	✓ Sí	✓ Sí	✓ Sí

Amazon EMR

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::EMR::Cluster`	✓ Sí	✓ Sí	✓ Sí

Contenedores de Amazon EMR

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::EMRContainers::JobRun`	✗ No	✓ Sí	✗ No
`AWS::EMRContainers::VirtualCluster`	✓ Sí	✓ Sí	✓ Sí

Amazon EMR sin servidor

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::EMRServerless::Application`	✗ No	✓ Sí	✓ Sí
`AWS::EMRServerless::JobRun`	✗ No	✓ Sí	✗ No

Amazon ElastiCache

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en Stack
`AWS::ElastiCache::CacheCluster`	✓ Sí	✓ Sí	✓ Sí
`AWS::ElastiCache::ParameterGroup`	✗ No	✓ Sí	✗ No
`AWS::ElastiCache::SecurityGroup`	✗ No	✓ Sí	✗ No
`AWS::ElastiCache::Snapshot`	✓ Sí	✓ Sí	✗ No
`AWS::ElastiCache::SubnetGroup`	✗ No	✓ Sí	✗ No
`AWS::ElastiCache::User`	✗ No	✓ Sí	✗ No
`AWS::ElastiCache::UserGroup`	✗ No	✓ Sí	✗ No

AWS Elastic Beanstalk

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::ElasticBeanstalk::Application`	✓ Sí	✓ Sí	× No
`AWS::ElasticBeanstalk::ApplicationVersion`	× No	✓ Sí	× No
`AWS::ElasticBeanstalk::ConfigurationTemplate`	× No	✓ Sí	× No
`AWS::ElasticBeanstalk::Environment`	× No	✓ Sí	× No

Amazon Elastic Compute Cloud (Amazon EC2)

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::EC2::CapacityReservation`	× No	✓ Sí	× No
`AWS::EC2::CapacityReservationFleet`	× No	✓ Sí	× No
`AWS::EC2::CarrierGateway`	× No	✓ Sí	× No
`AWS::EC2::ClientVpnEndpoint`	× No	✓ Sí	× No
`AWS::EC2::CoipPool`	× No	✓ Sí	× No

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::EC2::CustomerGateway	✓ Sí	✓ Sí	✓ Sí
AWS::EC2::DHCPOptions	✓ Sí	✓ Sí	✓ Sí
AWS::EC2::EC2Fleet	× No	✓ Sí	× No
AWS::EC2::EgressOnlyInternetGateway	× No	✓ Sí	× No
AWS::EC2::EIP	✓ Sí	✓ Sí	× No
AWS::EC2::ExportImageTask	× No	✓ Sí	× No
AWS::EC2::ExportInstanceTask	× No	✓ Sí	× No
AWS::EC2::FlowLog	× No	✓ Sí	× No
AWS::EC2::FpgaImage	× No	✓ Sí	× No
AWS::EC2::Host	× No	✓ Sí	× No
AWS::EC2::HostReservation	× No	✓ Sí	× No
AWS::EC2::Image	✓ Sí	✓ Sí	× No
AWS::EC2::ImportImageTask	× No	✓ Sí	× No
AWS::EC2::ImportSnapshotTask	× No	✓ Sí	× No
AWS::EC2::Instance	✓ Sí	✓ Sí	✓ Sí
AWS::EC2::InstanceEventWindow	× No	✓ Sí	× No
AWS::EC2::InternetGateway	✓ Sí	✓ Sí	✓ Sí

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::EC2::IPv4Pool	✗ No	✓ Sí	✗ No
AWS::EC2::IPv6Pool	✗ No	✓ Sí	✗ No
AWS::EC2::KeyPair	✗ No	✓ Sí	✗ No
AWS::EC2::LaunchTemplate	✗ No	✓ Sí	✓ Sí
AWS::EC2::LocalGateway	✗ No	✓ Sí	✗ No
AWS::EC2::LocalGatewayRouteTable	✗ No	✓ Sí	✗ No
AWS::EC2::LocalGatewayRouteTableVirtualInterfaceGroupAssociation	✗ No	✓ Sí	✗ No
AWS::EC2::LocalGatewayRouteTableVPCAssociation	✗ No	✓ Sí	✗ No
AWS::EC2::LocalGatewayVirtualInterface	✗ No	✓ Sí	✗ No
AWS::EC2::LocalGatewayVirtualInterfaceGroup	✗ No	✓ Sí	✗ No
AWS::EC2::NatGateway	✓ Sí	✓ Sí	✓ Sí
AWS::EC2::NetworkAcl	✓ Sí	✓ Sí	✓ Sí
AWS::EC2::NetworkInsightsAccessScope	✗ No	✓ Sí	✗ No
AWS::EC2::NetworkInsightsAccessScopeAnalysis	✗ No	✓ Sí	✗ No

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::EC2::NetworkInsightsAnalysis	✗ No	✓ Sí	✗ No
AWS::EC2::NetworkInsightsPath	✗ No	✓ Sí	✗ No
AWS::EC2::NetworkInterface	✓ Sí	✓ Sí	✓ Sí
AWS::EC2::PlacementGroup	✗ No	✓ Sí	✓ Sí
AWS::EC2::PrefixList	✗ No	✓ Sí	✗ No
AWS::EC2::ReplaceRootVolumeTask	✗ No	✓ Sí	✗ No
AWS::EC2::ReservedInstance	✓ Sí	✓ Sí	✗ No
AWS::EC2::RouteTable	✓ Sí	✓ Sí	✓ Sí
AWS::EC2::SecurityGroup	✓ Sí	✓ Sí	✓ Sí
AWS::EC2::Snapshot	✓ Sí	✓ Sí	✗ No
AWS::EC2::SpotFleet	✗ No	✓ Sí	✗ No
AWS::EC2::SpotInstanceRequest	✓ Sí	✓ Sí	✗ No
AWS::EC2::Subnet	✓ Sí	✓ Sí	✓ Sí
AWS::EC2::SubnetCidrReservation	✗ No	✓ Sí	✗ No
AWS::EC2::TrafficMirrorFilter	✗ No	✓ Sí	✗ No
AWS::EC2::TrafficMirrorSession	✗ No	✓ Sí	✗ No
AWS::EC2::TrafficMirrorTarget	✗ No	✓ Sí	✗ No

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::EC2::TransitGateway	✗ No	✓ Sí	✗ No
AWS::EC2::TransitGatewayAttachment	✗ No	✓ Sí	✗ No
AWS::EC2::TransitGatewayConnectPeer	✗ No	✓ Sí	✗ No
AWS::EC2::TransitGatewayMulticastDomain	✗ No	✓ Sí	✗ No
AWS::EC2::TransitGatewayPolicyTable	✗ No	✓ Sí	✗ No
AWS::EC2::TransitGatewayRouteTable	✗ No	✓ Sí	✗ No
AWS::EC2::TransitGatewayRouteTableAnnouncement	✗ No	✓ Sí	✗ No
AWS::EC2::VerifiedAccessEndpoint	✗ No	✓ Sí	✗ No
AWS::EC2::VerifiedAccessGroup	✗ No	✓ Sí	✗ No
AWS::EC2::VerifiedAccessInstance	✗ No	✓ Sí	✗ No
AWS::EC2::VerifiedAccessTrustProvider	✗ No	✓ Sí	✗ No
AWS::EC2::Volume	✓ Sí	✓ Sí	✓ Sí
AWS::EC2::VPC	✓ Sí	✓ Sí	✓ Sí
AWS::EC2::VPCEndpoint	✗ No	✓ Sí	✗ No
AWS::EC2::VPCEndpointConnection	✗ No	✓ Sí	✗ No
AWS::EC2::VPCEndpointService	✗ No	✓ Sí	✗ No

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::EC2::VPCEndpointServicePermissions`	✗ No	✓ Sí	✗ No
`AWS::EC2::VPCPeeringConnection`	✗ No	✓ Sí	✓ Sí
`AWS::EC2::VPNConnection`	✓ Sí	✓ Sí	✓ Sí
`AWS::EC2::VPNGateway`	✓ Sí	✓ Sí	✓ Sí

Amazon Elastic Container Registry

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::ECR::Repository`	✗ No	✓ Sí	✗ No

Amazon Elastic Container Service

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::ECS::CapacityProvider`	✗ No	✓ Sí	✗ No
`AWS::ECS::Cluster`	✓ Sí	✓ Sí	✗ No
`AWS::ECS::ContainerInstance`	✗ No	✓ Sí	✗ No
`AWS::ECS::Service`	✗ No	✓ Sí	✗ No
`AWS::ECS::Task`	✗ No	✓ Sí	✗ No
`AWS::ECS::TaskDefinition`	✓ Sí	✓ Sí	✗ No
`AWS::ECS::TaskSet`	✗ No	✓ Sí	✗ No

Amazon Elastic File System

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::EFS::FileSystem`	✓ Sí	✓ Sí	✓ Sí

Amazon Elastic Inference

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::ElasticInference::ElasticInferenceAccelerator`	✓ Sí	✓ Sí	✗ No

Amazon Elastic Kubernetes Service (Amazon EKS)

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::EKS::Addon`	✗ No	✓ Sí	✗ No
`AWS::EKS::Cluster`	✓ Sí	✓ Sí	✓ Sí

Elastic Load Balancing

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::ElasticLoadBalancing::LoadBalancer`	✓ Sí	✓ Sí	✓ Sí
`AWS::ElasticLoadBalancingV2::Listener`	× No	✓ Sí	✓ Sí
`AWS::ElasticLoadBalancingV2::ListenerRule`	× No	✓ Sí	✓ Sí
`AWS::ElasticLoadBalancingV2::LoadBalancer`	✓ Sí	✓ Sí	✓ Sí
`AWS::ElasticLoadBalancingV2::TargetGroup`	✓ Sí	✓ Sí	✓ Sí

OpenSearch Servicio Amazon

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Elasticsearch::Domain`	✓ Sí	✓ Sí	✓ Sí

CloudWatch Eventos de Amazon

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Events::EventBus`	✗ No	✓ Sí	✗ No
`AWS::Events::Rule`	✓ Sí	✓ Sí	✓ Sí

> **Note**
>
> Tag Editor no admite las reglas de bus de eventos personalizados.

EventBridge Esquemas de Amazon

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::EventSchemas::Discoverer`	✗ No	✓ Sí	✗ No
`AWS::EventSchemas::Registry`	✗ No	✓ Sí	✗ No
`AWS::EventSchemas::Schema`	✗ No	✓ Sí	✗ No

Amazon FSx

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::FSx::FileSystem`	✓ Sí	✓ Sí	✗ No
`AWS::FSx::StorageVirtualMachine`	✗ No	✓ Sí	✗ No
`AWS::FSx::Volume`	✗ No	✓ Sí	✗ No

Amazon Forecast

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Forecast::Dataset`	✓ Sí	✓ Sí	✗ No
`AWS::Forecast::DatasetGroup`	✓ Sí	✓ Sí	✗ No
`AWS::Forecast::DatasetImportJob`	✓ Sí	✓ Sí	✗ No
`AWS::Forecast::Forecast`	✓ Sí	✓ Sí	✗ No
`AWS::Forecast::ForecastExportJob`	✓ Sí	✓ Sí	✗ No
`AWS::Forecast::Predictor`	✓ Sí	✓ Sí	✗ No

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::Forecast::PredictorBacktestExportJob	✓ Sí	✓ Sí	× No

Amazon Fraud Detector

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::FraudDetector::Detector	✓ Sí	✓ Sí	× No
AWS::FraudDetector::DetectorVersion	× No	✓ Sí	× No
AWS::FraudDetector::EntityType	✓ Sí	✓ Sí	× No
AWS::FraudDetector::EventType	✓ Sí	✓ Sí	× No
AWS::FraudDetector::ExternalModel	✓ Sí	✓ Sí	× No
AWS::FraudDetector::Label	✓ Sí	✓ Sí	× No
AWS::FraudDetector::Model	✓ Sí	✓ Sí	× No
AWS::FraudDetector::ModelVersion	× No	✓ Sí	× No
AWS::FraudDetector::Outcome	✓ Sí	✓ Sí	× No
AWS::FraudDetector::Rule	× No	✓ Sí	× No

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::FraudDetector::Variable`	✓ Sí	✓ Sí	✗ No

Amazon GameLift

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en Stack
`AWS::GameLift::Alias`	✗ No	✓ Sí	✗ No
`AWS::GameLift::GameSessionQueue`	✗ No	✓ Sí	✗ No
`AWS::GameLift::Location`	✗ No	✓ Sí	✗ No
`AWS::GameLift::MatchmakingConfiguration`	✗ No	✓ Sí	✗ No
`AWS::GameLift::MatchmakingRuleSet`	✗ No	✓ Sí	✗ No

AWS Global Accelerator

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::GlobalAccelerator::Accelerator`	✗ No	✓ Sí	✗ No

AWS Glue

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Glue::Crawler`	✓ Sí	✓ Sí	✗ No
`AWS::Glue::Database`	✗ No	✓ Sí	✓ Sí
`AWS::Glue::Job`	✓ Sí	✓ Sí	✗ No
`AWS::Glue::MLTransform`	✗ No	✓ Sí	✗ No
`AWS::Glue::Registry`	✗ No	✓ Sí	✗ No
`AWS::Glue::Trigger`	✓ Sí	✓ Sí	✗ No
`AWS::Glue::Workflow`	✗ No	✓ Sí	✗ No

AWS Glue DataBrew

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::DataBrew::Dataset`	✓ Sí	✓ Sí	✓ Sí
`AWS::DataBrew::Job`	✓ Sí	✓ Sí	✓ Sí
`AWS::DataBrew::Project`	✓ Sí	✓ Sí	✓ Sí
`AWS::DataBrew::Recipe`	✓ Sí	✓ Sí	✓ Sí
`AWS::DataBrew::Schedule`	✓ Sí	✓ Sí	✓ Sí

AWS Ground Station

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::GroundStation::Config`	✗ No	✓ Sí	✗ No
`AWS::GroundStation::DataflowEndpointGroup`	✗ No	✓ Sí	✗ No
`AWS::GroundStation::MissionProfile`	✗ No	✓ Sí	✗ No

Amazon GuardDuty

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en Stack
`AWS::GuardDuty::Detector`	✗ No	✓ Sí	✓ Sí
`AWS::GuardDuty::Filter`	✗ No	✓ Sí	✗ No
`AWS::GuardDuty::IPSet`	✗ No	✓ Sí	✗ No
`AWS::GuardDuty::ThreatIntelSet`	✗ No	✓ Sí	✗ No

Amazon Interactive Video Service

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::IVS::Channel`	✗ No	✓ Sí	✗ No
`AWS::IVS::RecordingConfiguration`	✗ No	✓ Sí	✗ No
`AWS::IVS::StreamKey`	✗ No	✓ Sí	✗ No

AWS Identity and Access Management

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::IAM::InstanceProfile`	✓ Sí[1]	✓ Sí[2]	× No
`AWS::IAM::ManagedPolicy`	✓ Sí[1]	✓ Sí[2]	× No
`AWS::IAM::OpenIDConnectProvider`	✓ Sí[1]	✓ Sí[2]	× No
`AWS::IAM::Role`	× No	× No	✓ Sí[2]
`AWS::IAM::SAMLProvider`	✓ Sí[1]	✓ Sí[2]	× No
`AWS::IAM::ServerCertificate`	✓ Sí[1]	✓ Sí[2]	× No
`AWS::IAM::VirtualMFADevice`	✓ Sí[1]	✓ Sí[2]	× No

[1] Este es un recurso para un servicio global alojado en la región Este de EE. UU. (Norte de Virginia). Si quiere usar el Tag Editor para crear o modificar etiquetas para este tipo de recurso, debe incluir el `us-east-1` en la lista Seleccionar regiones, en la sección Buscar recursos para etiquetar, en la consola de Tag Editor.

[2] Este es un recurso para un servicio global alojado en la región Este de EE. UU. (Norte de Virginia). Como los Resource Groups se mantienen por separado para cada región, debe AWS Management Console cambiarlos por uno Región de AWS que contenga los recursos que desee incluir en el grupo. Para crear un grupo de recursos que contenga un recurso global, debe configurar su us-east-1 AWS Management Console para EE. UU. Este (Virginia del Norte) mediante el selector de regiones situado en la esquina superior derecha del. AWS Management Console

Generador de Imágenes de EC2

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::ImageBuilder::Component`	✗ No	✓ Sí	✗ No
`AWS::ImageBuilder::ContainerRecipe`	✗ No	✓ Sí	✗ No
`AWS::ImageBuilder::DistributionConfiguration`	✗ No	✓ Sí	✗ No
`AWS::ImageBuilder::Image`	✗ No	✓ Sí	✗ No
`AWS::ImageBuilder::ImagePipeline`	✗ No	✓ Sí	✗ No
`AWS::ImageBuilder::ImageRecipe`	✗ No	✓ Sí	✗ No
`AWS::ImageBuilder::InfrastructureConfiguration`	✗ No	✓ Sí	✗ No

Amazon Inspector

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Inspector::AssessmentTemplate`	✗ No	✓ Sí	✓ Sí

AWS IoT

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::IoT::Authorizer	✗ No	✓ Sí	✗ No
AWS::IoT::BillingGroup	✗ No	✓ Sí	✗ No
AWS::IoT::CACertificate	✗ No	✓ Sí	✗ No
AWS::IoT::CustomMetric	✗ No	✓ Sí	✗ No
AWS::IoT::Dimension	✗ No	✓ Sí	✗ No
AWS::IoT::JobTemplate	✗ No	✓ Sí	✗ No
AWS::IoT::MitigationAction	✗ No	✓ Sí	✗ No
AWS::IoT::Policy	✗ No	✓ Sí	✗ No
AWS::IoT::RoleAlias	✗ No	✓ Sí	✗ No
AWS::IoT::ScheduledAudit	✗ No	✓ Sí	✗ No
AWS::IoT::SecurityProfile	✗ No	✓ Sí	✗ No
AWS::IoT::ThingGroup	✗ No	✓ Sí	✗ No
AWS::IoT::ThingType	✗ No	✓ Sí	✗ No
AWS::IoT::TopicRule	✗ No	✓ Sí	✓ Sí

AWS IoT Analytics

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::IoTAnalytics::Channel`	✗ No	✓ Sí	✗ No
`AWS::IoTAnalytics::Dataset`	✓ Sí	✓ Sí	✗ No
`AWS::IoTAnalytics::Datastore`	✗ No	✓ Sí	✗ No
`AWS::IoTAnalytics::Pipeline`	✗ No	✓ Sí	✗ No

AWS IoT Events

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::IoTEvents::AlarmModel`	✗ No	✓ Sí	✗ No
`AWS::IoTEvents::DetectorModel`	✓ Sí	✓ Sí	✓ Sí
`AWS::IoTEvents::Input`	✓ Sí	✓ Sí	✓ Sí

AWS IoT FleetWise

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::IoTFleetWise::Campaign`	✗ No	✓ Sí	✓ Sí
`AWS::IoTFleetWise::DecoderManifest`	✗ No	✓ Sí	✓ Sí
`AWS::IoTFleetWise::Fleet`	✗ No	✓ Sí	✓ Sí
`AWS::IoTFleetWise::ModelManifest`	✗ No	✓ Sí	✓ Sí
`AWS::IoTFleetWise::SignalCatalog`	✗ No	✓ Sí	✓ Sí
`AWS::IoTFleetWise::Vehicle`	✗ No	✓ Sí	✓ Sí

AWS IoT Greengrass

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Greengrass::ConnectorDefinition`	✓ Sí	✓ Sí	✗ No
`AWS::Greengrass::CoreDefinition`	✓ Sí	✓ Sí	✗ No
`AWS::Greengrass::DeviceDefinition`	✓ Sí	✓ Sí	✗ No
`AWS::Greengrass::FunctionDefinition`	✓ Sí	✓ Sí	✗ No

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Greengrass::Group`	✓ Sí	✓ Sí	✗ No
`AWS::Greengrass::LoggerDefinition`	✓ Sí	✓ Sí	✗ No
`AWS::Greengrass::ResourceDefinition`	✓ Sí	✓ Sí	✗ No
`AWS::Greengrass::SubscriptionDefinition`	✓ Sí	✓ Sí	✗ No

AWS IoT Greengrass Version 2

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::GreengrassV2::ComponentVersion`	✗ No	✓ Sí	✗ No

Consola de AWS IoT SiteWise

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::IoTSiteWise::Asset`	✗ No	✓ Sí	✗ No
`AWS::IoTSiteWise::AssetModel`	✗ No	✓ Sí	✗ No
`AWS::IoTSiteWise::Dashboard`	✗ No	✓ Sí	✗ No
`AWS::IoTSiteWise::Gateway`	✗ No	✓ Sí	✗ No
`AWS::IoTSiteWise::Portal`	✗ No	✓ Sí	✗ No
`AWS::IoTSiteWise::Project`	✗ No	✓ Sí	✗ No

AWS IoT Wireless

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::IoTWireless::Destination`	✗ No	✓ Sí	✗ No
`AWS::IoTWireless::DeviceProfile`	✗ No	✓ Sí	✗ No
`AWS::IoTWireless::FuotaTask`	✗ No	✓ Sí	✗ No
`AWS::IoTWireless::MulticastGroup`	✗ No	✓ Sí	✗ No

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::IoTWireless::NetworkAnalyzerConfiguration	✗ No	✓ Sí	✗ No
AWS::IoTWireless::ServiceProfile	✗ No	✓ Sí	✗ No
AWS::IoTWireless::TaskDefinition	✗ No	✓ Sí	✗ No
AWS::IoTWireless::WirelessDevice	✗ No	✓ Sí	✗ No
AWS::IoTWireless::WirelessGateway	✗ No	✓ Sí	✗ No

AWS Key Management Service

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::KMS::Alias	✗ No	✗ No	✓ Sí
AWS::KMS::Key	✓ Sí	✓ Sí	✓ Sí

Amazon Keyspaces (para Apache Cassandra)

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Cassandra::Keyspace`	✗ No	✓ Sí	✓ Sí
`AWS::Cassandra::Table`	✗ No	✓ Sí	✗ No

Amazon Kinesis

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Kinesis::Stream`	✓ Sí	✓ Sí	✓ Sí

Amazon Managed Service para Apache Flink

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::KinesisAnalytics::Application`	✓ Sí	✓ Sí	✓ Sí

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::KinesisAnalyticsV2::Application`	✗ No	✗ No	✓ Sí

Amazon Data Firehose

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::KinesisFirehose::DeliveryStream`	✗ No	✓ Sí	✓ Sí

AWS Lambda

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Lambda::Alias`	✗ No	✗ No	✓ Sí
`AWS::Lambda::EventSourceMapping`	✗ No	✗ No	✓ Sí
`AWS::Lambda::Function`	✓ Sí	✓ Sí	✓ Sí

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::Lambda::LayerVersion	✗ No	✗ No	✓ Sí
AWS::Lambda::Version	✗ No	✗ No	✓ Sí

Amazon Lightsail

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::Lightsail::Bucket	✗ No	✓ Sí	✗ No
AWS::Lightsail::Certificate	✗ No	✓ Sí	✗ No
AWS::Lightsail::Container	✗ No	✓ Sí	✗ No
AWS::Lightsail::Disk	✗ No	✓ Sí	✗ No
AWS::Lightsail::Distribution	✗ No	✓ Sí	✗ No
AWS::Lightsail::Instance	✗ No	✓ Sí	✗ No
AWS::Lightsail::StaticIp	✗ No	✓ Sí	✗ No

Amazon MQ

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::AmazonMQ::Broker`	✓ Sí	✓ Sí	✗ No
`AWS::AmazonMQ::Configuration`	✓ Sí	✓ Sí	✗ No

Amazon Macie

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Macie::ClassificationJob`	✓ Sí	✓ Sí	✗ No
`AWS::Macie::CustomDataIdentifier`	✓ Sí	✓ Sí	✓ Sí
`AWS::Macie::FindingsFilter`	✓ Sí	✓ Sí	✓ Sí
`AWS::Macie::Member`	✓ Sí	✓ Sí	✗ No

Amazon Managed Blockchain

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::ManagedBlockchain::Accessor`	✗ No	✓ Sí	✗ No

Transmisión gestionadada de Amazon para Apache Kafka

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Kafka::Cluster`	✓ Sí	✓ Sí	✗ No

AWS Elemental MediaConnect

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::MediaConnect::Flow`	✗ No	✓ Sí	✗ No
`AWS::MediaConnect::FlowEntitlement`	✗ No	✓ Sí	✗ No

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::MediaConnect::FlowOutput`	✗ No	✓ Sí	✗ No
`AWS::MediaConnect::FlowSource`	✗ No	✓ Sí	✗ No

AWS Elemental MediaPackage

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::MediaPackage::Channel`	✗ No	✓ Sí	✗ No
`AWS::MediaPackage::PackagingConfiguration`	✗ No	✓ Sí	✗ No
`AWS::MediaPackage::PackagingGroup`	✗ No	✓ Sí	✗ No

AWS Network Manager

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::NetworkManager::CoreNetwork`	✗ No	✓ Sí	✗ No
`AWS::NetworkManager::Device`	✗ No	✓ Sí	✗ No
`AWS::NetworkManager::GlobalNetwork`	✗ No	✓ Sí	✗ No
`AWS::NetworkManager::Link`	✗ No	✓ Sí	✗ No
`AWS::NetworkManager::Site`	✗ No	✓ Sí	✗ No
`AWS::NetworkManager::VpcAttachment`	✗ No	✓ Sí	✗ No

OpenSearch Servicio Amazon OpenSearch

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::OpenSearchService::Domain`	✓ Sí	✓ Sí	✓ Sí

AWS OpsWorks

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::OpsWorks::Instance`	✗ No	✓ Sí	✓ Sí
`AWS::OpsWorks::Layer`	✗ No	✓ Sí	✓ Sí
`AWS::OpsWorks::Stack`	✗ No	✓ Sí	✓ Sí

AWS Organizations

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Organizations::Account`	✓ Sí	✓ Sí	✗ No
`AWS::Organizations::OrganizationalUnit`	✗ No	✓ Sí	✗ No
`AWS::Organizations::Policy`	✗ No	✓ Sí	✗ No
`AWS::Organizations::Root`	✓ Sí	✓ Sí	✗ No

Amazon Pinpoint

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Pinpoint::App`	✗ No	✓ Sí	✓ Sí
`AWS::Pinpoint::EmailTemplate`	✗ No	✓ Sí	✓ Sí
`AWS::Pinpoint::PushTemplate`	✗ No	✓ Sí	✓ Sí
`AWS::Pinpoint::SmsTemplate`	✗ No	✓ Sí	✓ Sí
`AWS::Pinpoint::VoiceTemplate`	✗ No	✓ Sí	✗ No

API de SMS y voz de Amazon Pinpoint

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::PinpointSMSVoiceV2::Pool`	✗ No	✓ Sí	✗ No

Amazon Quantum Ledger Database (Amazon QLDB)

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::QLDB::Ledger`	✓ Sí	✓ Sí	✓ Sí
`AWS::QLDB::Stream`	× No	✓ Sí	✓ Sí

Amazon Redshift

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Redshift::Cluster`	✓ Sí	✓ Sí	✓ Sí
`AWS::Redshift::ClusterParameterGroup`	✓ Sí	✓ Sí	✓ Sí
`AWS::Redshift::ClusterSecurityGroup`	× No	✓ Sí	✓ Sí
`AWS::Redshift::ClusterSubnetGroup`	✓ Sí	✓ Sí	✓ Sí
`AWS::Redshift::DBGroup`	× No	✓ Sí	× No
`AWS::Redshift::DBName`	× No	✓ Sí	× No
`AWS::Redshift::DBUser`	× No	✓ Sí	× No
`AWS::Redshift::EventSubscription`	× No	✓ Sí	× No

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::Redshift::HSMClientCertificate	✓ Sí	✓ Sí	✗ No
AWS::Redshift::HSMConfiguration	✗ No	✓ Sí	✗ No
AWS::Redshift::Namespace	✗ No	✓ Sí	✗ No
AWS::Redshift::Snapshot	✗ No	✓ Sí	✗ No
AWS::Redshift::SnapshotCopyGrant	✗ No	✓ Sí	✗ No
AWS::Redshift::SnapshotSchedule	✗ No	✓ Sí	✗ No
AWS::Redshift::UsageLimit	✗ No	✓ Sí	✗ No

Amazon Relational Database Service (Amazon RDS)

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::RDS::CustomDBEngineVersion	✗ No	✓ Sí	✗ No
AWS::RDS::DBCluster	✓ Sí	✓ Sí	✓ Sí
AWS::RDS::DBClusterEndpoint	✗ No	✓ Sí	✗ No
AWS::RDS::DBClusterParameterGroup	✓ Sí	✓ Sí	✓ Sí

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::RDS::DBClusterSnapshot	✓ Sí	✓ Sí	✗ No
AWS::RDS::DBInstance	✓ Sí	✓ Sí	✓ Sí
AWS::RDS::DBParameterGroup	✓ Sí	✓ Sí	✓ Sí
AWS::RDS::DBProxy	✗ No	✓ Sí	✗ No
AWS::RDS::DBProxyEndpoint	✗ No	✓ Sí	✗ No
AWS::RDS::DBProxyTargetGroup	✗ No	✓ Sí	✗ No
AWS::RDS::DBSecurityGroup	✓ Sí	✓ Sí	✓ Sí
AWS::RDS::DBSnapshot	✓ Sí	✓ Sí	✗ No
AWS::RDS::DBSubnetGroup	✓ Sí	✓ Sí	✓ Sí
AWS::RDS::Deployment	✗ No	✓ Sí	✗ No
AWS::RDS::EventSubscription	✓ Sí	✓ Sí	✗ No
AWS::RDS::OptionGroup	✓ Sí	✓ Sí	✗ No
AWS::RDS::ReservedDBInstance	✓ Sí	✓ Sí	✗ No

AWS Resource Access Manager

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::RAM::ResourceShare`	✓ Sí	✓ Sí	✗ No

AWS Resource Groups

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::ResourceGroups::Group`	✓ Sí	✓ Sí	✓ Sí

AWS Robomaker

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::RoboMaker::DeploymentJob`	✗ No	✓ Sí	✗ No
`AWS::RoboMaker::Fleet`	✗ No	✓ Sí	✗ No

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::RoboMaker::Robot`	✗ No	✓ Sí	✗ No
`AWS::RoboMaker::RobotApplication`	✓ Sí	✓ Sí	✗ No
`AWS::RoboMaker::SimulationApplication`	✓ Sí	✓ Sí	✗ No
`AWS::RoboMaker::SimulationJob`	✓ Sí	✓ Sí	✗ No

Amazon Route 53

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Route53::Domain`	✓ Sí[1]	✓ Sí[2]	✗ No
`AWS::Route53::HealthCheck`	✓ Sí[1]	✓ Sí[2]	✓ Sí[2]
`AWS::Route53::HostedZone`	✓ Sí[1]	✓ Sí[2]	✓ Sí[2]

[1] Este es un recurso para un servicio global alojado en la región Este de EE. UU. (Norte de Virginia). Si quiere usar el Tag Editor para crear o modificar etiquetas para este tipo de recurso, debe incluir el `us-east-1` en la lista Seleccionar regiones, en la sección Buscar recursos para etiquetar, en la consola de Tag Editor.

² Este es un recurso para un servicio global alojado en la región Este de EE. UU. (Norte de Virginia). Como los Resource Groups se mantienen por separado para cada región, debe AWS Management Console cambiarlos por uno Región de AWS que contenga los recursos que desee incluir en el grupo. Para crear un grupo de recursos que contenga un recurso global, debe configurar su us-east-1 AWS Management Console para EE. UU. Este (Virginia del Norte) mediante el selector de regiones situado en la esquina superior derecha del. AWS Management Console

Amazon Route 53 Resolver

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Route53Resolver::FirewallDomainList`	✗ No	✓ Sí²	✗ No
`AWS::Route53Resolver::FirewallRuleGroup`	✗ No	✓ Sí²	✗ No
`AWS::Route53Resolver::FirewallRuleGroupAssociation`	✗ No	✓ Sí²	✗ No
`AWS::Route53Resolver::ResolverEndpoint`	✓ Sí¹	✓ Sí²	✗ No
`AWS::Route53Resolver::ResolverQueryLoggingConfig`	✗ No	✓ Sí²	✗ No
`AWS::Route53Resolver::ResolverRule`	✓ Sí¹	✓ Sí²	✗ No

¹ Este es un recurso para un servicio global alojado en la región Este de EE. UU. (Norte de Virginia). Si quiere usar el Tag Editor para crear o modificar etiquetas para este tipo de recurso, debe incluir el `us-east-1` en la lista Seleccionar regiones, en la sección Buscar recursos para etiquetar, en la consola de Tag Editor.

² Este es un recurso para un servicio global alojado en la región Este de EE. UU. (Norte de Virginia). Como los Resource Groups se mantienen por separado para cada región, debe AWS Management Console cambiarlos por uno Región de AWS que contenga los recursos que desee incluir en el grupo. Para crear un grupo de recursos que contenga un recurso global, debe configurar su us-east-1 AWS Management Console para EE. UU. Este (Virginia del Norte) mediante el selector de regiones situado en la esquina superior derecha del. AWS Management Console

Amazon S3 Glacier

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Glacier::Vault`	✓ Sí	✓ Sí	✗ No

Amazon SageMaker

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en Stack
`AWS::SageMaker::AppImageConfig`	✗ No	✓ Sí	✗ No
`AWS::SageMaker::CodeRepository`	✗ No	✓ Sí	✗ No
`AWS::SageMaker::Endpoint`	✗ No	✓ Sí	✓ Sí
`AWS::SageMaker::EndpointConfig`	✗ No	✓ Sí	✓ Sí

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en Stack
AWS::SageMaker::HyperParameterTuningJob	✗ No	✓ Sí	✗ No
AWS::SageMaker::Image	✗ No	✓ Sí	✗ No
AWS::SageMaker::LabelingJob	✗ No	✓ Sí	✗ No
AWS::SageMaker::Model	✗ No	✓ Sí	✓ Sí
AWS::SageMaker::ModelPackageGroup	✗ No	✓ Sí	✓ Sí
AWS::SageMaker::NotebookInstance	✓ Sí	✓ Sí	✓ Sí
AWS::SageMaker::Pipeline	✗ No	✓ Sí	✗ No
AWS::SageMaker::Project	✗ No	✓ Sí	✓ Sí
AWS::SageMaker::TrainingJob	✗ No	✓ Sí	✗ No
AWS::SageMaker::TransformJob	✗ No	✓ Sí	✗ No
AWS::SageMaker::Workteam	✗ No	✓ Sí	✗ No

AWS Secrets Manager

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::SecretsManager::Secret`	✓ Sí	✓ Sí	✓ Sí

AWS Service Catalog

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::ServiceCatalog::CloudFormationProduct`	✗ No	✓ Sí	✓ Sí
`AWS::ServiceCatalog::Portfolio`	✗ No	✓ Sí	✓ Sí

AWS Service Catalog AppRegistry

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::ServiceCatalogAppRegistry::Application`	✗ No	✓ Sí	✗ No
`AWS::ServiceCatalogAppRegistry::AttributeGroup`	✗ No	✓ Sí	✗ No

Service Quotas

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::ServiceQuotas::Quota`	✗ No	✓ Sí	✗ No

Amazon Simple Email Service

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::SES::ConfigurationSet`	✓ Sí	✓ Sí	✓ Sí
`AWS::SES::ContactList`	✓ Sí	✓ Sí	✓ Sí
`AWS::SES::DedicatedIpPool`	✓ Sí	✓ Sí	× No
`AWS::SES::Identity`	✓ Sí	✓ Sí	× No

Amazon Simple Notification Service

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::SNS::Topic`	✓ Sí	✓ Sí	✓ Sí

Amazon Simple Queue Service

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::SQS::Queue`	✓ Sí	✓ Sí	✓ Sí

Amazon Simple Storage Service (Amazon S3)

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::S3::Bucket`	✓ Sí	✓ Sí	✓ Sí
`AWS::S3::Job`	X No	✓ Sí	X No
`AWS::S3::StorageLens`	X No	✓ Sí	X No

AWS Step Functions

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::StepFunctions::Activity`	✓ Sí	✓ Sí	✓ Sí
`AWS::StepFunctions::StateMachine`	✓ Sí	✓ Sí	✓ Sí

Storage Gateway

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::StorageGateway::Gateway`	✓ Sí	✓ Sí	X No
`AWS::StorageGateway::Volume`	X No	✓ Sí	X No

AWS Systems Manager

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::SSM::Association	✗ No	✓ Sí	✗ No
AWS::SSM::AutomationExecution	✗ No	✓ Sí	✗ No
AWS::SSM::Document	✗ No	✓ Sí	✓ Sí
AWS::SSM::MaintenanceWindow	✗ No	✓ Sí	✗ No
AWS::SSM::ManagedInstance	✗ No	✓ Sí	✗ No
AWS::SSM::OpsItem	✗ No	✓ Sí	✗ No
AWS::SSM::OpsMetadata	✗ No	✓ Sí	✗ No
AWS::SSM::Parameter	✓ Sí	✓ Sí	✓ Sí
AWS::SSM::PatchBaseline	✗ No	✓ Sí	✓ Sí

AWS Systems Manager para SAP

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::SystemsManagerSAP::Application	✗ No	✓ Sí	✓ Sí

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::SystemsManagerSAP::Database`	✗ No	✓ Sí	✗ No

Amazon Timestream

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Timestream::ScheduledQuery`	✗ No	✓ Sí	✓ Sí

AWS Transfer Family

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Transfer::Certificate`	✗ No	✓ Sí	✗ No
`AWS::Transfer::Connector`	✗ No	✓ Sí	✗ No
`AWS::Transfer::Profile`	✗ No	✓ Sí	✗ No

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::Transfer::Workflow`	✗ No	✓ Sí	✗ No

AWS WAF

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::WAF::Rule`	✗ No	✓ Sí	✗ No
`AWS::WAF::WebACL`	✗ No	✓ Sí	✗ No

Amazon WorkSpaces

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en Stack
`AWS::WorkSpaces::Workspace`	✓ Sí	✓ Sí	✓ Sí

AWS X-Ray

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
`AWS::XRay::Group`	✗ No	✓ Sí	✗ No
`AWS::XRay::SamplingRule`	✗ No	✓ Sí	✗ No

Tipos de recursos obsoletos

Los siguientes tipos de recursos ya no admitidos para la funcionalidad especificada.

Servicio	Tipo de recurso	Cambio en la compatibilidad	Fecha
AWS RoboMaker	`AWS::RoboMaker::Robot`	Tag Editor ya no lo admite.	2 de mayo de 2022
AWS RoboMaker	`AWS::RoboMaker::Fleet`	Tag Editor ya no lo admite.	2 de mayo de 2022
AWS RoboMaker	`AWS::RoboMaker::DeploymentJob`	Tag Editor ya no lo admite.	2 de mayo de 2022

Creación de grupos de recursos con AWS CloudFormation

AWS Resource Groups está integrado con AWS CloudFormation, un servicio que le ayuda a modelar y configurar sus recursos de AWS para que pueda dedicar menos tiempo a crear y administrar sus recursos e infraestructura. Puede crear una plantilla que describa todos los recursos de AWS que desea (como los grupos de recursos) y AWS CloudFormation aprovisionará y configurará estos recursos por usted.

Cuando utiliza AWS CloudFormation, puede volver a utilizar su plantilla para configurar sus grupos de recursos de forma coherente y repetida. Describa los recursos una vez y luego suministre los mismos recursos una y otra vez en varias Cuentas de AWS y regiones.

Grupos de recursos y plantillas AWS CloudFormation

Para suministrar y configurar recursos para los grupos de recursos y sus servicios relacionados, debe entender las plantillas de AWS CloudFormation. Las plantillas son archivos de texto con formato JSON o YAML. Estas plantillas describen los recursos que desea aprovisionar en sus pilas de AWS CloudFormation. Si no está familiarizado con JSON o YAML, puede utilizar Designer de AWS CloudFormation para comenzar a utilizar las plantillas de AWS CloudFormation. Para obtener más información, consulte ¿Qué es Designer de AWS CloudFormation? en la Guía del usuario de AWS CloudFormation.

Los grupos de recursos permiten crear grupos de recursos en AWS CloudFormation. Para obtener más información, incluyendo ejemplos de plantillas JSON y YAML para los recursos, consulte la referencia del tipo de recurso de AWS Resource Groups en la Guía del usuario de AWS CloudFormation.

Obtener más información sobre AWS CloudFormation

Para obtener más información acerca de AWS CloudFormation, consulte los siguientes recursos:

- AWS CloudFormation
- Guía del usuario de AWS CloudFormation
- Referencia de la API de AWS CloudFormation
- Guía del usuario de la interfaz de la línea de comandos de AWS CloudFormation

Seguridad en AWS Resource Groups

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

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

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad que se aplican a AWS Resource Groups, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad se determina según el servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

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

Temas

Protección de los datos en AWS Resource Groups

El modelo de responsabilidad compartida de AWS se aplica a la protección de datos de AWS Resource Groups. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. También es responsable de la configuración de seguridad y de las tareas de administración para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS.

Para proteger los datos, recomendamos proteger las credenciales de Cuenta de AWS y configurar cuentas de usuario individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, cada usuario recibe solamente los permisos necesarios para cumplir con sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

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

Se recomienda encarecidamente no ingresar información confidencial o sensible, como por ejemplo direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Incluye las situaciones en las que debe trabajar con Resource Groups u otros Servicios de AWS a través de la consola, la API, la AWS CLI o los SDK de AWS. Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres puede ser empleado para los

registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Cifrado de datos

En comparación con otros servicios de AWS, AWS Resource Groups tiene una superficie expuesta a ataques mínima, ya que no proporciona una forma de cambiar, agregar o eliminar recursos de AWS, excepto en el caso de los grupos. Resource Groups recopila sobre usted la siguiente información específica del servicio.

- Nombres de grupos (no cifrados ni privados)
- Descripciones de grupos (no cifradas, pero privadas)
- Recursos de los miembros en grupos (se almacenan en registros no cifrados)

Cifrado en reposo

No hay formas adicionales de aislar el servicio o el tráfico de red específico de Resource Groups. Si corresponde, utilice un aislamiento específico de AWS. Puede usar la API y la consola de Resource Groups en una VPC para maximizar la privacidad y la seguridad de la infraestructura.

Cifrado en tránsito

Los datos de AWS Resource Groups se cifran cuando se transfieren a la base de datos interna del servicio para realizar copias de seguridad. Esto no es configurable por el usuario.

Administración de claves

AWS Resource Groups no está integrado actualmente con AWS Key Management Service y no es compatible con AWS KMS keys.

Privacidad del tráfico entre redes

AWS Resource Groups utiliza HTTPS para todas las transmisiones entre los usuarios de Resource Groups y AWS. Resource Groups usa la seguridad de la capa de transporte (TLS) 1.2, pero también admite TLS 1.0 y 1.1.

Administración de identidad y acceso para AWS Resource Groups

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Resource Groups. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que se realice en Resource Groups.

Usuario de servicio: si utiliza el servicio Resource Groups para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Resource Groups para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en Resource Groups, consulte Solución de problemas AWS Resource Groups de identidad y acceso.

Administrador de servicio: si está a cargo de los recursos de Resource Groups en su empresa, probablemente tenga acceso completo a Resource Groups. Su trabajo consiste en determinar a qué características y recursos de Resource Groups deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para

obtener más información sobre cómo su empresa puede utilizar IAM con Resource Groups, consulte Cómo funciona Resource Groups con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a Resource Groups. Para ver ejemplos de políticas basadas en identidades de Resource Groups que puede utilizar en IAM, consulte Ejemplos de políticas basadas en identidad de AWS Resource Groups.

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAM Identity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWSen la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede

asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para

obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

- Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar un AWS rol a una instancia EC2 y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations .
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en

función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona Resource Groups con IAM

Antes de utilizar IAM para administrar el acceso a Resource Groups, debe comprender qué características de IAM están disponibles para su uso con Resource Groups. Para obtener una perspectiva general sobre cómo funcionan y otros servicios de AWS con IAM, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Temas

- Políticas basadas en identidad de Resource Groups
- Políticas basadas en recursos
- Autorización basada en etiquetas de Resource Groups
- Roles de IAM en Resource Groups

Políticas basadas en identidad de Resource Groups

Con las políticas basadas en identidad de IAM, puede especificar las acciones y recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Resource Groups admite acciones específicas, recursos y claves de condición. Para obtener información sobre todos los elementos que utiliza en una política JSON, consulte Referencia de los elementos de las políticas JSON de IAM en la Guía del usuario de IAM.

Acciones

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y bajo qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo

nombre que la operación de API de AWS asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Las acciones de políticas de Resource Groups utilizan el siguiente prefijo antes de la acción: `resource-groups:`. Las acciones de Tag Editor se realizan íntegramente en la consola, pero tienen el prefijo `resource-explorer` en las entradas de registro.

Por ejemplo, para conceder a alguien permiso para crear Resource Groups con la operación de la API de Resource Groups `CreateGroup`, incluya la acción `resource-groups:CreateGroup` en su política. Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`. Resource Groups define su propio conjunto de acciones que describen las tareas que se pueden realizar con este servicio.

Para especificar varias acciones de Resource Groups y Tag Editor en una única instrucción, sepárelas con comas del siguiente modo:

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

Puede utilizar caracteres comodín (*) para especificar varias acciones. Por ejemplo, para especificar todas las acciones que comiencen con la palabra `List`, incluya la siguiente acción:

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

Para ver una lista de acciones de Resource Groups, consulte Acciones, recursos y claves de condición de AWS Resource Groups en la Guía del usuario de IAM.

Recursos

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y bajo qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica

recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

El único recurso disponible en Resource Groups es el grupo. El recurso de tiene el siguiente formato de ARN:

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

Para obtener más información acerca del formato de los ARN, consulte Nombres de recursos de Amazon (ARN) y espacios de nombres de servicios de AWS.

Por ejemplo, para especificar la el grupo de recursos `my-test-group` en su instrucción, utilice el siguiente ARN:

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

Para especificar todos los grupos que pertenecen a una cuenta específica, utilice el carácter comodín (*):

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

Algunas acciones de Resource Groups, como las empleadas para la creación de recursos, no se pueden llevar a cabo en un recurso específico. En dichos casos, debe utilizar el carácter comodín (*).

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

Algunas acciones de la API de Resource Groups se utilizan varios recursos. Por ejemplo, `DeleteGroup` elimina grupos, por lo tanto, quien realiza la llamada a la entidad principal debe tener permisos para eliminar un grupo específico o todos los grupos. Para especificar varios recursos en una única instrucción, separe los ARN con comas.

```
"Resource": [
  "resource1",
  "resource2"
]
```

Para consultar una lista de tipos de recursos de Resource Groups y sus ARN y saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones, recursos y claves de condición en la Guía del usuario AWS Resource Groups de IAM.

Claves de condición

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y bajo qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición con una operación lógica `OR`. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para obtener más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

Resource Groups define su propio conjunto de claves de condición y también admite el uso de algunas claves de condición globales. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

Para consultar una lista de claves de condición de Resource Groups y saber con qué acciones y recursos puede usar una clave de condición, consulte Acciones, recursos y claves de condición AWS Resource Groups en la Guía del usuario de IAM.

Ejemplos

Para ver ejemplos de Resource Groups basadas en políticas de identidades, consulte Ejemplos de políticas basadas en identidad de AWS Resource Groups.

Políticas basadas en recursos

Resource Groups no admite políticas basadas en recursos.

Autorización basada en etiquetas de Resource Groups

Puede asociar etiquetas a grupos en Resource Groups o transferirlas en una solicitud a Resource Groups. Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`. Puede aplicar etiquetas a un grupo al crear o actualizar el grupo. Para obtener acerca del etiquetado de un grupo en Resource Groups, consulte Crear grupos basados en consultas en AWS Resource Groups y Actualización de grupos en AWS Resource Groups en esta guía.

Para consultar un ejemplo de política basada en la identidad para limitar el acceso a un recurso en función de las etiquetas de ese recurso, consulte Visualización de grupos basados en etiquetas.

Roles de IAM en Resource Groups

Un rol de IAM es una entidad de la cuenta de AWS que dispone de permisos específicos. Resource Groups no tiene ni utiliza roles de servicio.

Uso de credenciales temporales con Resource Groups

En Resource Groups, puede utilizar credenciales temporales para iniciar sesión con federación, asumir un rol de IAM o asumir un rol de acceso entre cuentas. Las credenciales de seguridad temporales se obtienen mediante una llamada a operaciones de la API de AWS STS, como AssumeRole o GetFederationToken.

Roles vinculados a servicios

Los roles vinculados a servicios permiten a los servicios de AWS obtener acceso a los recursos de otros servicios para completar una acción en su nombre.

Resource Groups no tiene ni utiliza roles vinculados a servicios.

Roles de servicio

Esta característica permite que un servicio asuma un rol de servicio en su nombre.

Resource Groups no tiene ni utiliza roles de servicio.

Políticas administradas de AWS para AWS Resource Groups

Una política administrada de AWS es una política independiente que AWS crea y administra. Las políticas administradas de AWS se diseñan para ofrecer permisos para muchos casos de uso comunes, por lo que puede empezar a asignar permisos a los usuarios, grupos y roles.

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

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

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

AWS: políticas administradas para Resource Groups

- ResourceGroupsServiceRolePolicy

Política administrada de AWS: ResourceGroupsServiceRolePolicy

No puede adjuntar `ResourceGroupsServiceRolePolicy` a sus entidades IAM usted mismo. Esta política puede estar adjunta a un rol vinculado a servicios que permite a Resource Groups realizar acciones en su nombre. Para obtener más información, consulte Uso de roles vinculados a servicios para Resource Groups.

Esta política concede los permisos necesarios para que Resource Groups recupere información sobre los recursos de sus grupos de recursos y cualquier pila de AWS CloudFormation a la que

pertenezcan esos recursos. Esto permite a Resource Groups generar eventos de CloudWatch para la característica de eventos del ciclo de vida del grupo.

Para ver la versión más reciente de esta política administrada de AWS, consulte `ResourceGroupsServiceRolePolicy` en la consola de IAM.

Política administrada de AWS: ResourceGroupsandTagEditorFullAccess

Al asociar una política a una entidad principal, concede a la entidad los permisos que están definidos en la política. Las políticas administradas de AWS le permiten la asignación de los permisos adecuados a los usuarios, grupos y roles, en lugar de tener que escribir las políticas usted mismo.

Esta política concede los permisos necesarios para el acceso completo a las funciones Resource Groups y Tag Editor.

Para ver la versión más reciente de esta política administrada de AWS, consulte `ResourceGroupsandTagEditorFullAccess` en la consola de IAM.

Para obtener más información sobre esta política, consulte ResourceGroupsandTagEditorFullAccess en la Guía de referencia de políticas gestionadas de AWS.

Política administrada de AWS: ResourceGroupsandTagEditorReadOnlyAccess

Al asociar una política a una entidad principal, concede a la entidad los permisos que están definidos en la política. Las políticas administradas de AWS le permiten la asignación de los permisos adecuados a los usuarios, grupos y roles, en lugar de tener que escribir las políticas usted mismo.

Esta política concede los permisos necesarios para el acceso completo a las funciones Resource Groups y Tag Editor.

Para ver la versión más reciente de esta política administrada de AWS, consulte `ResourceGroupsandTagEditorReadOnlyAccess` en la consola de IAM.

Para obtener más información sobre esta política, consulte ResourceGroupsandTagEditorReadOnlyAccess en la Guía de referencia de políticas gestionadas de AWS.

Resource Groups actualiza las políticas administradas de AWS

Es posible consultar los detalles sobre las actualizaciones de las políticas administradas de AWS para Resource Groups, debido a que este servicio comenzó a realizar el seguimiento de estos

cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos de Resource Groups.

Cambio	Descripción	Fecha
Actualización de política: ResourceGroupsandTagEditorFullAccess	Resource Groups actualizó una política para incluir permisos de AWS CloudFormation adicionales.	10 de agosto de 2023
Actualización de política: ResourceGroupsandTagEditorReadOnlyAccess	Resource Groups actualizó una política para incluir permisos de AWS CloudFormation adicionales.	10 de agosto de 2023
Nueva política: ResourceGroupsServiceRolePolicy	Resource Groups agregó una nueva política para respaldar su función vinculada al servicio.	17 de noviembre de 2022
Resource Groups comenzó a realizar un seguimiento de los cambios	Resource Groups comenzó el seguimiento de los cambios de las políticas administradas por AWS.	17 de noviembre de 2022

Uso de roles vinculados a servicios para Resource Groups

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

Un rol vinculado a un servicio simplifica la configuración de Resource Groups porque ya no tendrá que agregar manualmente los permisos necesarios. Resource Groups define los permisos de sus roles vinculados a servicios y establece políticas de confianza en cada uno de ellos para garantizar que solo el servicio Resource Groups pueda asumir sus roles. Los permisos definidos incluyen las

políticas de confianza y de permisos, y que la política de permisos no se puede adjuntar a ninguna otra entidad de IAM.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Yes (Sí) en la columna Service-linked roles (Roles vinculados a servicios). Seleccione una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de roles vinculados a servicios para Resource Groups

Resource Groups utiliza el siguiente rol vinculado a un servicio para respaldar los eventos del ciclo de vida del grupo. Elija el enlace que aparece en el nombre del rol para verlo en la consola de IAM después de crearlo.

- `AWSServiceRoleForResourceGroups`

Resource Groups utiliza los permisos de este rol para consultar a Servicios de AWS sobre los propietarios de sus recursos a fin de resolver la pertenencia a grupos y mantener el grupo actualizado. Permite a Resource Groups emitir eventos relacionados con el servicio al servicio Amazon EventBridge.

El rol vinculado a servicio `AWSServiceRoleForResourceGroups` confía solo en el siguiente servicio para asumir el rol:

- `resourcegroups.amazonaws.com`

Los permisos asociados al rol provienen de la siguiente política administrada de AWS. Seleccione el enlace en el nombre de la política para ver la política en la consola IAM.

- `Políticas administradas de AWS para AWS Resource Groups`

Creación del rol vinculado a servicio para Resource Groups

> **Important**
>
> Este rol vinculado al servicio puede aparecer en su cuenta si ha completado una acción en otro servicio que utilice las características compatibles con este rol. Para más información, consulte Un nuevo rol apareció en mi Cuenta de AWS.

Para crear el rol vinculado a un servicio, active la característica de eventos del ciclo de vida del grupo.

Edición de un rol vinculado a un servicio para Resource Groups

Resource Groups no le permite editar el rol vinculado al servicio AWSServiceRoleForResourceGroups. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol utilizando IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio para Resource Groups

Puede eliminar el rol vinculado a un servicio solo después de desactivar la característica de eventos del ciclo de vida del grupo.

> **Important**
>
> - AWS le impide eliminar el rol vinculado al servicio hasta que desactive por primera vez la característica de eventos del ciclo de vida del grupo que lo creó.
> - Le recomendamos que no elimine el rol vinculado al servicio mientras tenga algún grupo de recursos en su Cuenta de AWS. El servicio Resource Groups no puede interactuar con otros Servicios de AWS para administrar sus grupos si elimina este rol.

Eliminar manualmente el rol vinculado al servicio

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

Console

Para eliminar el rol vinculado a servicios de Resource Groups

1. Abra la consola de IAM en la página Roles.
2. Busque el rol denominado AWSServiceRoleForResourceGroups y active la casilla de verificación situada junto a él.
3. Elija Eliminar.

4. Confirme su intención de eliminar el rol introduciendo el nombre del rol en el cuadro y, a continuación, seleccione Eliminar.

El rol desaparecerá de la lista de roles en la consola de IAM.

AWS CLI

Para eliminar el rol vinculado a servicios de Resource Groups

Para eliminar el rol, ingrese el siguiente comando con los parámetros exactamente como se muestran. No reemplace ninguno de los 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"
}
```

El comando devuelve un ID de tarea. La eliminación efectiva del rol se produce de forma asíncrona. Puede comprobar el estado de la eliminación del rol pasando el identificador de tarea proporcionado al siguiente comando 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"
}
```

Regiones admitidas para los roles vinculados a servicios de Resource Groups

Resource Groups admite el uso de roles vinculados a servicios en todas las Regiones de AWS en las que el servicio está disponible. Para obtener más información, consulte Regiones y puntos de conexión de AWS.

Ejemplos de políticas basadas en identidad de AWS Resource Groups

De forma predeterminada, las entidades principales de IAM, como los roles y usuarios, no tienen permiso para crear, ver ni modificar recursos de Resource Groups. Tampoco pueden realizar

tareas mediante la AWS Management Console, la AWS CLI, o la API de AWS. Un administrador de IAM debe crear políticas de IAM que concedan permiso a la entidades principales para realizar operaciones de API concretas en los recursos especificados que necesiten. El administrador debe adjuntar esas políticas a las entidades principales que necesiten esos permisos.

Para obtener información acerca de cómo crear una política basada en identidad de IAM con estos documentos de políticas JSON de ejemplo, consulte Creación de políticas en la pestaña JSON en la Guía del usuario de IAM.

Temas

Prácticas recomendadas relativas a políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Resource Groups de la cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidad:

- Comience con las políticas administradas por AWS y continúe con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de trabajo, utilice las políticas administradas por AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en la Cuenta de AWS. Se recomienda definir políticas administradas por el cliente de AWS específicas para sus casos de uso a fin de reducir aún más los permisos. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía de usuario de IAM.
- Use condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo,

puede escribir una condición de política para especificar que todas las solicitudes deben enviarse utilizando SSL. También puede usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado, como por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política JSON de IAM: condición en la Guía del usuario de IAM.

- Use el Analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el Analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. IAM Access Analyzer proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para obtener más información, consulte la política de validación del Analizador de acceso de IAM en la Guía de usuario de IAM.
- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesita usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de MFA a sus políticas. Para obtener más información, consulte Configuración de acceso a una API protegida por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía de usuario de IAM.

Uso de la consola y la API de Resource Groups

Para acceder a la consola de Tag Editor y la API de AWS Resource Groups, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle registrar y consultar los detalles acerca de los recursos de Resource Groups en su cuenta de AWS. Si crea una política basada en identidades que es más restrictiva que los permisos mínimos requeridos, la consola no funcionará según lo previsto para las entidades principales (usuarios o roles de IAM) con esa política.

Para asegurarse de que esas entidades puedan seguir usando Resource Groups, asocie la siguiente política (o una política que contenga los permisos enumerados en la siguiente política) a las entidades. Para obtener más información, consulte Agregar de permisos a un usuario en la Guía del usuario de 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 obtener acerca de cómo conceder acceso a Resource Groups, consulte Otorgar permisos para usar AWS Resource Groups un editor de etiquetas en esta guía.

Permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se adjuntan a la identidad de sus usuarios. Esta política incluye permisos para llevar a cabo esta acción en la consola o mediante programación con la AWS CLI o la API de 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": "*"
        }
    ]
}
```

Visualización de grupos basados en etiquetas

Puede utilizar las condiciones de su política basada en la identidad para controlar el acceso a los recursos de Resource Groups basados en etiquetas. Este ejemplo muestra cómo puede crear una política que permita ver un recurso, en este ejemplo, un grupo de recursos. Sin embargo, el permiso solo se concede si la etiqueta `project` de grupo tiene el mismo valor que la etiqueta `project` adjunta a la entidad principal que realiza la llamada.

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

```
        }
    ]
}
```

También puede adjuntar esta política a las entidades entidad principales en su cuenta. Si una entidad principal con la clave `project` y el valor de la etiqueta `alpha` intenta ver un grupo de recursos, también debe etiquetarlo como `project=alpha`. De lo contrario, se deniega el acceso al usuario. La clave de la etiqueta de condición `project` coincide con los nombres de las claves de condición `Project` y `project` porque no distinguen entre mayúsculas y minúsculas. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condition en la Guía del usuario de IAM.

Solución de problemas AWS Resource Groups de identidad y acceso

Utilice la siguiente información para ayudar a diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Resource Groups e IAM.

Temas

- No tengo autorización para realizar una acción en Resource Groups
- No estoy autorizado a realizar lo siguiente: PassRole
- Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis Resource Groups

No tengo autorización para realizar una acción en Resource Groups

Si AWS Management Console le indica que no está autorizado a realizar una acción, debe ponerse en contacto con su administrador para obtener ayuda. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

En el siguiente ejemplo, el error se produce cuando el usuario `mateojackson` intenta utilizar la consola para ver detalles de un grupo, pero no tiene permisos `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
```

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso `my-test-group` mediante la acción `resource-groups:ListGroups`.

No estoy autorizado a realizar lo siguiente: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, se deben actualizar las políticas a fin de permitirle pasar un rol a Resource Groups.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando una usuaria de IAM llamada `marymajor` intenta utilizar la consola para realizar una acción en Resource Groups. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

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

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis Resource Groups

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si Resource Groups admite estas funciones, consulte Cómo funciona Resource Groups con IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a través de los Cuentas de AWS que eres propietario, consulta Cómo proporcionar acceso a un usuario de IAM en otro de tu Cuenta de AWS propiedad en la Guía del usuario de IAM.

- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para obtener información acerca del uso de roles y políticas basadas en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Registro y supervisión en Resource Groups

Todas las acciones de AWS Resource Groups se registran en AWS CloudTrail.

Registrar llamadas a la API de AWS Resource Groups con AWS CloudTrail

AWS Resource Groups y Tag Editor están integrados con AWS CloudTrail, un servicio que registra las acciones de usuarios, de roles o de servicios de AWS en Resource Groups o Tag Editor. CloudTrail captura todas las llamadas a la API de Resource Groups como eventos, incluidas las llamadas procedentes de la consola de Resource Groups o Tag Editor y de las llamadas de código a las API de Resource Groups. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos para Resource Groups. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Historial de eventos. Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Resource Groups, la dirección IP desde la que se realizó, quién la realizó y cuándo, etc.

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

Información de Resource Groups en CloudTrail

CloudTrail se habilita en su cuenta de AWS cuando la crea. Cuando se produce actividad en Resource Groups o en la consola de Tag Editor, esta se registra en un evento de CloudTrail junto con otros eventos de servicio de AWS en el Historial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de los eventos en su cuenta de AWS, incluidos los eventos de Resource Groups, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail

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

- Introducción a la creación de registros de seguimiento
- Servicios e integraciones compatibles con CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de registro de CloudTrail de varias regiones y Recibir archivos de registro de CloudTrail de varias cuentas

Todas las acciones de Resource Groups las registra CloudTrail y se documentan en la Referencia de la API de AWS Resource Groups. Las acciones de Resource Groups en CloudTrail se muestran como eventos con el punto de conexión de la API `resource-groups.amazonaws.com` como fuente. Por ejemplo, las llamadas a las acciones `CreateGroup`, `GetGroup` y `UpdateGroupQuery` generan entradas en los archivos de log de CloudTrail. CloudTrail registra las acciones de Tag Editor en la consola y se muestran como eventos con el punto de conexión interno de la API `resource-explorer` como fuente.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales raíz o del usuario de IAM.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte Elemento `userIdentity` de CloudTrail.

Comprensión de las entradas de archivos de registro de Resource Groups

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que especifique. Los archivos log de CloudTrail pueden contener una o varias entradas de log. Un evento representa una única solicitud de cualquier origen

e incluye información acerca de la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etcétera. Los archivos de registro de CloudTrail no son un rastro de pila ordenado de las llamadas a las API públicas, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail que ilustra la acción `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"
}
```


Validación de cumplimiento en Resource Groups

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

> **Note**
>
> No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en Resource Groups

AWS Resource Groups realiza copias de seguridad automatizadas en los recursos del servicio interno. Estas copias de seguridad no pueden ser configuradas por el usuario. Las copias de seguridad están cifradas, tanto en reposo como en tránsito. Resource Groups almacena datos de clientes en Amazon DynamoDB.

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

Ni siquiera la pérdida total de los grupos de recursos de usuarios provocaría la pérdida de datos de los clientes, ya que la mayoría de los datos de los clientes se replican en todas las zonas de disponibilidad (AZ) de AWS. Si elimina grupos accidentalmente, póngase en contacto con el Centro AWS Support.

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

Seguridad de la infraestructura en Resource Groups

Resource Groups no ofrece ninguna forma adicional de aislar el tráfico de red o de servicio. Si corresponde, utilice un aislamiento específico de AWS. Puede usar la API y la consola de Resource Groups en una VPC para maximizar la privacidad y la seguridad de la infraestructura.

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

Puede utilizar llamadas a la API publicadas de AWS para acceder a Resource Groups a través de la red. Los clientes deben admitir lo siguiente:

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

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

Resource Groups no admite políticas basadas en recursos.

Prácticas recomendadas de seguridad para Resource Groups

Las siguientes prácticas recomendadas son directrices generales y no suponen una solución de seguridad completa. Puesto que es posible que estas prácticas recomendadas no sean adecuadas o suficientes para el entorno, considérelas como consideraciones útiles en lugar de como normas.

- Utilice el principio de privilegio mínimo para permitir el acceso a grupos. Resource Groups admite permisos a nivel de recursos. Conceda acceso a grupos específicos solo cuando sea necesario para usuarios específicos. Evite el uso de asteriscos en las declaraciones de política que asignan permisos a todos los usuarios o a todos los grupos. Para obtener más información sobre el privilegio mínimo, consulte Conceder privilegios mínimos en la Guía del usuario de IAM.
- Mantenga la información privada fuera de los campos públicos. El nombre de un grupo se trata como metadatos de servicio. Los nombres de los grupos no están cifrados. No incluya información confidencial en los nombres de los grupos. Las descripciones de los grupos son privadas.

  No coloque información privada o confidencial en las claves o valores de las etiquetas.
- Utilice la autorización basada en el etiquetado siempre que sea apropiado. Resource Groups es compatible con la autorización basada en etiquetas. Puede etiquetar grupos y, a continuación, actualizar las políticas asociadas a sus entidades principales de IAM, como los usuarios y las funciones, para establecer su nivel de acceso en función de las etiquetas que se apliquen a un grupo. Para obtener más información sobre el uso de la autorización basada en etiquetas, consulte Control de acceso a los recursos de AWS en la Guía del usuario de IAM.

  Muchos servicios de AWS admiten la autorización basada en etiquetas para sus recursos. Tenga en cuenta que la autorización basada en etiquetas puede configurarse para los recursos de los miembros de un grupo. Si el acceso a los recursos de un grupo está restringido por etiquetas, es posible que los usuarios o grupos no autorizados no puedan realizar acciones o automatizaciones en esos recursos. Por ejemplo, si una instancia de Amazon EC2 de uno de sus grupos está etiquetada con una clave de etiqueta `Confidentiality` y un valor de etiqueta de `High` y no está autorizado a ejecutar comandos en los recursos etiquetados `Confidentiality:High`, las acciones o automatizaciones que realice en la instancia de EC2 fallarán, incluso si las acciones se

realizan correctamente para otros recursos del grupo de recursos. Para obtener más información sobre qué servicios admiten la autorización basada en etiquetas para sus recursos, consulte AWSServicios que funcionan con IAM en la Guía del usuario de IAM.

Para obtener más información sobre cómo desarrollar una estrategia de etiquetado para sus AWS recursos, consulte Estrategias de etiquetado de AWS.

Cuotas de servicio para Resource Groups

En la siguiente tabla se describen los límites de AWS Resource Groups (Resource Groups). Puede solicitar que se aumenten algunos de estos límites. Para solicitar un aumento del límite, vaya a la consola de Service Quotas. Para obtener más información acerca de los límites que pueden cambiarse, consulte Service Quotas.

> **Note**
>
> Las siguientes definiciones se aplican a la descripción de las cuotas a continuación:
>
> - Grupo de recursos: conjunto de recursos de AWS de que se encuentra en la misma Región de AWS y que coincide con los criterios especificados en la consulta del grupo.

Recurso	Límite predeterminado
Número máximo de recursos por grupo por Cuenta de AWS por Región de AWS	100

Referencia de AWS Resource Groups

Consulte los temas de esta sección para encontrar información de referencia de distintos aspectos de AWS Resource Groups.

Cuotas de servicio para Resource Groups

Nombre	Valor predeterminado	Ajusta	Descripción
Grupos de recursos por cada cuenta	Cada región admitida: 100	Sí	Número máximo de grupos de recursos que puede crear en esta cuenta. Un grupo de recursos es un conjunto de recursos de AWS que cumplen un criterio específico.

> **Note**
>
> Puede solicitar cambios en las cuotas marcadas como ajustables mediante la página de AWS Resource Groups de la consola Service Quotas.

Políticas administradas de AWS disponibles para su uso con AWS Resource Groups

Las políticas de permisos de IAM administradas por AWS le permiten conceder permisos preconfigurados a las entidades principales de IAM, como las funciones y los usuarios, de su cuenta. Las políticas administradas por AWS se prueban y siguen las recomendaciones de las prácticas recomendadas, por lo que puede utilizarlas de forma fiable en los escenarios para los que están definidas. A medida que los nuevos tipos de recursos se admiten como miembros de los grupos de recursos y los nuevos tipos de recursos admiten el etiquetado, AWS actualiza automáticamente estas políticas para adaptarlos. No tiene que hacer nada.

En la siguiente tabla se enumeran las políticas de permisos de IAM administradas por AWS que puede utilizar para conceder permisos a AWS Resource Groups.

Nombre de la política y ARN	Descripción
AWSResourceGroupsReadOnlyAccess arn:aws:iam::aws:policy/AWSResourceGroupsReadOnlyAccess	Concede acceso de solo lectura a la consola de administración de AWS Resource Groups. Incluye el permiso para ver los detalles de un recurso, incluida la lista de etiquetas adjuntas. Esta política no concede permiso para realizar cambios en los grupos de recursos o las etiquetas.
ResourceGroupsandTagEditorReadOnlyAccess arn:aws:iam::aws:policy/ResourceGroupsandTagEditorReadOnlyAccess	Concede acceso de solo lectura a la consola de administración de AWS Resource Groups, lo que incluye Tag Editor. Incluye el permiso para ver los detalles de un recurso, incluidas las etiquetas. Puede usar Tag Editor para ver los recursos que coinciden con las consultas de etiquetas. Esta política no concede permiso para realizar cambios en los grupos de recursos o las etiquetas.
ResourceGroupsandTagEditorFullAccess arn:aws:iam::aws:policy/ResourceGroupsandTagEditorFullAccess	Otorga acceso administrativo completo a la consola de administración de AWS Resource Groups. Incluye permisos para ver, crear y modificar grupos de recursos. También incluye permisos para ver, establecer y modificar las etiquetas de cualquier recurso compatible con Tag Editor.

AWS Resource Groups historial de documentos

Cambio	Descripción	Fecha
Compatibilidad con más tipos de recursos	Resource Groups y Tag Editor ahora admiten más tipos de recursos.	30 de mayo de 2024
Políticas AWS gestionadas actualizadas y ResourceGroupsandTagEditorFullAccess ResourceGroupsandTagEditorReadOnlyAccess	Resource Groups actualizó dos políticas AWS administradas para añadir AWS CloudFormation permisos adicionales.	10 de agosto de 2023
Cuotas de servicio de Resource Groups	Ahora puede ver los límites de cuota de Resource Groups mediante Service Quotas.	29 de junio de 2023
Actualización de las prácticas recomendadas de IAM	Guía actualizada para implementar las prácticas recomendadas de IAM. Para obtener más información, consulte prácticas recomendadas de seguridad en IAM.	3 de enero de 2023
La información de Tag Editor se ha trasladado a su propia guía	La documentación de Tag Editor se ha eliminado de esta guía y se ha trasladado a la nueva Guía del usuario de Tag Editor.	13 de diciembre de 2022
Los grupos de recursos ahora pueden incluir recursos de Amazon Keyspaces (para Apache Cassandra)	AWS Resource Groups ahora admite la inclusión de recursos para Amazon Keyspaces (para Apache Cassandra) en un grupo de recursos.	20 de octubre de 2022

Discontinuidad de los tipos de recursos	Tag Editor ya no admite los siguientes tipos de recursos: `AWS::RoboMaker::Robot` , `AWS::RoboMaker::Fleet` y `AWS::RoboMaker::DeploymentJob` .	17 de mayo de 2022
Nueva política AWS gestionada - ResourceGroupsServiceRolePolicy	Resource Groups agregó una nueva política AWS administrada en AWS Identity and Access Management (IAM) para respaldar la función vinculada al servicio del servicio.	12 de enero de 2022
Eventos del ciclo de vida de un grupo	Resource Groups ahora puede generar eventos en Amazon CloudWatch Events para avisarle cuando se produzcan cambios en sus grupos de recursos.	12 de enero de 2022
Amazon VPC Network Access Analyzer ahora puede utilizar los grupos de recursos para supervisar el tráfico de red no deseado que se dirige a sus recursos. AWS	Puede utilizarlos AWS Resource Groups para especificar las fuentes y los destinos según sus requisitos de acceso a la red.	3 de diciembre de 2021
Se agregó soporte para los recursos de AWS Resilience Hub	AWS Resource Groups ahora admite la inclusión de recursos para AWS Resilience Hub en un grupo de recursos.	18 de noviembre de 2021

Se añadió soporte para los recursos de Amazon Pinpoint	AWS Resource Groups ahora admite la inclusión de recursos para Amazon Pinpoint en un grupo de recursos.	11 de noviembre de 2021
Se agregó soporte para grupos de recursos configurados y administrados por AppRegistry	AWS Resource Groups ahora admite grupos de recursos que contienen configuraciones de servicio para los recursos de las aplicaciones que se crean mediante el uso de ellas AWS Service Catalog AppRegistry. Para obtener más información, consulte Configuraciones de servicio en la Referencia de la API de AWS Resource Groups .	15 de septiembre de 2021
Se agregó soporte para los recursos de Amazon OpenSearch Service	AWS Resource Groups ahora permite incluir recursos para Amazon OpenSearch Service en un grupo de recursos.	11 de agosto de 2021
Se agregó soporte para los recursos de AWS Braket	AWS Resource Groups ahora permite incluir recursos para AWS Braket en un grupo de recursos.	30 de junio de 2021
Se añadió soporte para recursos de Amazon EMR Containers	AWS Resource Groups ahora admite la inclusión de recursos para contenedores de Amazon EMR en un grupo de recursos.	27 de abril de 2021

Se agregó soporte para recursos de servicios adicionales AWS	AWS Resource Groups ahora permite incluir recursos para los siguientes servicios en un grupo de recursos: Amazon CodeGuru Reviewer, Amazon Elastic Inference, Amazon Forecast, Amazon Fraud Detector y Service Quotas.	25 de febrero de 2021
Se añadió un capítulo sobre seguridad y cumplimiento.	Analiza cómo Resource Groups protege su información y cumple con los estándares regulatorios.	30 de julio de 2020

Se añadió soporte para los grupos de recursos que están configurados para los servicios de AWS	Ahora puede crear grupos de recursos que estén asociados a un AWS servicio y que configuren la forma en que el servicio puede interactuar con los recursos del grupo. En esta primera versión de esta característica, puede crear un grupo de recursos que contenga reservas de capacidad de Amazon EC2 y luego introducir instancias de Amazon EC2 en el grupo. Si hay capacidad en una o más de las reservas del grupo que coincide con su instancia, esa instancia usará la reserva. Si la instancia no coincide con ninguna reserva disponible en el grupo, se introduce como una instancia bajo demanda. Para obtener más información, consulte Trabajar con grupos de reserva de capacidad en la Guía del usuario de Amazon EC2.	29 de julio de 2020
Se agregó soporte para AWS IoT Greengrass recursos.	El editor de etiquetas ahora admite más tipos de recursos. AWS Resource Groups	25 de marzo de 2020

Vea los datos de operaciones de AWS Resource Groups	En la AWS Systems Manager consola, la AWS Resource Groups página muestra los datos de operaciones de un grupo seleccionado en cuatro pestañas: Details, Config CloudTrail, OpsItems. Estas pestañas no están disponibles cuando esté viendo un grupo en la consola de Resource Groups. Puede utilizar la información de estas pestañas para ayudarle a comprender qué recursos de un grupo son admitidos y funcionan correctamente y qué recursos requieren acción. Si necesita realizar acciones en un recurso, puede utilizar los manuales de procedimientos de Systems Manager Automation para realizar tareas comunes de mantenimiento y solución de problemas. Para obtener más información, consulte Visualización de los datos de operaciones para AWS Resource Groups en la Guía del usuario de AWS Systems Manager .	16 de marzo de 2020

Compruebe el cumplimiento con políticas de etiquetas	Después de crear y adjuntar políticas de etiquetas a las cuentas que utilice AWS Organizations, podrá encontrar etiquetas no conformes en los recursos de las cuentas de su organizac ión.	26 de noviembre de 2019
Compatibilidad con más tipos de recursos	El editor de etiquetas ahora admite más tipos de AWS Resource Groups recursos.	4 de octubre de 2019
Los nuevos tipos de recursos son compatibles con AWS Resource Groups	Ahora se admiten más tipos de recursos AWS Resource Groups, especialmente para los grupos basados en una AWS CloudFormation pila.	5 de agosto de 2019
Los nuevos tipos de recursos son compatibles con AWS Resource Groups	Las API REST de Amazon API Gateway, CloudWatc h los eventos de Amazon Events y los temas de Amazon SNS ahora son tipos de recursos compatibles en. AWS Resource Groups	27 de junio de 2019
Tag Editor ahora permite buscar recursos sin etiquetas	Ahora puede buscar recursos en el editor de etiquetas que no tengan valores de etiqueta aplicados para una clave de etiqueta específica.	18 de junio de 2019

Los nuevos tipos de recursos son compatibles con un AWS Resource Groups editor de etiquetas	Se han agregado más de 50 tipos de recursos nuevos AWS Resource Groups y es compatible con el editor de etiquetas.	6 de junio de 2019
AWS Resource Groups y la consola de Tag Editor sale de la AWS Systems Manager consola	La consola AWS Resource Groups and Tag Editor ahora es independiente de la consola de Systems Manager. Aunque todavía puede encontrar los punteros a la AWS Resource Groups consola en la barra de navegación izquierda de Systems Manager, puede abrir la consola Resource Groups and Tag Editor directamente desde el menú desplegable de la parte superior izquierda del AWS Management Console.	5 de junio de 2019
Nuevas características de autorización y control de acceso de Resource Groups	Resource Groups admite ahora políticas basadas en acciones, permisos de nivel de recursos y autorizaciones basadas en etiquetas.	24 de mayo de 2019
Las herramientas antiguas y heredadas de Resource Groups y Tag Editorya no están disponibles	Se han eliminado las menciones a las herramien tas Resource Groups y Tag Editor anteriores, clásicas o heredadas. Estas herramien tas ya no están disponibles en AWS. En su lugar AWS Resource Groups , utilice un editor de etiquetas.	14 de mayo de 2019

El editor de etiquetas ahora admite el etiquetado de recursos en varias regiones	El editor de etiquetas ahora le permite buscar y administrar las etiquetas de recursos en varias regiones, con su región actual añadida a las consultas de recursos por defecto.	2 de mayo de 2019
El editor de etiquetas ahora admite la exportación de resultados de consultas a un archivo CSV	Puede exportar los resultados de una consulta en la página Buscar recursos para etiquetar a un archivo con formato CSV. Se muestra una nueva columna de región en los resultados de la consulta del editor de etiquetas. El editor de etiquetas ahora le permite buscar los recursos que tienen valores vacíos para una clave de etiqueta específica. Los valores de clave se completan de forma automática a medida que escribe un valor único entre las claves existentes.	2 de abril de 2019

El editor de etiquetas ahora admite la adición de todos los tipos de recursos a una consulta	Puede aplicar etiquetas hasta a un máximo de 20 tipos de recursos individuales en una única operación o puede elegir Todos los tipos de recursos para consultar todos los tipos de recursos de una región. Se ha añadido la finalización automática al campo Clave de etiqueta de una consulta para ayudar a habilitar claves de etiquetas consistentes entre recursos. Si los cambios de etiqueta fallan en algunos recursos, puede volver a intentar los cambios de etiquetas solo en los recursos en los que han fallado los cambios de etiqueta.	19 de marzo de 2019
El editor de etiquetas ahora admite varios tipos de recursos en una búsqueda	Puede aplicar etiquetas a un máximo de 20 tipos de recursos en una sola operación. También puede elegir que columnas que le aparecen en los resultado s de búsqueda, incluidas las columnas de cada clave de etiqueta única que aparecen en sus resultados de búsqueda o en los recursos seleccionados de los resultado s.	26 de febrero de 2019

Documentation añadida para el nuevo Tag Editor	En la sección «Trabajar con Tag Editor» se describe cómo utilizar la nueva experiencia de consola de AWS Tag Editor.	13 de febrero de 2019
Nuevos tipos de recursos admitidos para grupos en Resource Groups	Se han añadido nuevos tipos de recursos que se admiten ahora en Resource Groups.	4 de febrero de 2019
Experiencia de usuario mejorada a la hora de añadir etiquetas a consultas de Resource Groups basadas en etiquetas	Pequeños cambios en la experiencia de usuario de la consola para la adición de etiquetas en una consulta basada en etiquetas.	17 de diciembre de 2018
AWS CloudFormation Se agregó soporte para consultas basadas en pilas a Resource Groups	Puede crear grupos de recursos en los que la consulta se base en una AWS CloudFormation pila. Después de que elija una pila, puede elegir qué tipos de recursos de la pila desea que aparezcan en la consulta de grupo.	13 de noviembre de 2018
Resource Groups y CloudTrail	Resource Groups ahora ofrece AWS CloudTrail soporte. Puede ver los registros de todas las llamadas a la API Resource Groups y trabajar con ellos CloudTrail.	29 de junio de 2018

- Versión de la API: 27-11-2017
- Última actualización de la documentación: 24 de septiembre de 2019

Actualizaciones anteriores

En la siguiente tabla, se describen los cambios importantes de cada versión de la Guía del usuario de AWS Resource Groups anteriores a junio de 2018.

Cambio	Descripción	Fecha
Versión inicial	Versión inicial de la próxima generación de AWS Resource Groups	29 de noviembre de 2017

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.