



Guía del usuario

# AWS Resource Groups



# AWS Resource Groups: Guía del usuario

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

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

---

# Table of Contents

¿Qué son los grupos de recursos? .....	1
Los recursos y sus tipos de grupos .....	1
Casos de uso de los grupos de recursos .....	3
AWS Resource Groups y permisos .....	4
AWS Resource Groups recursos .....	4
Cómo funciona el etiquetado .....	4
Introducción .....	5
Requisitos previos .....	6
Autorización y control de acceso de Resource Groups .....	12
AWS servicios que funcionan con AWS Resource Groups .....	13
Configuraciones del servicio .....	17
Acceso .....	18
Sintaxis y estructura .....	18
Tipos de configuración y parámetros .....	19
Creación de grupos .....	36
Tipos de consultas de grupos de recursos .....	36
Construir una consulta basada en etiquetas y crear un grupo .....	41
Cree un grupo AWS CloudFormation basado en pilas .....	43
Actualización de grupos .....	46
Actualizar grupos de consultas basados en etiquetas .....	46
Actualice un grupo AWS CloudFormation basado en pilas .....	49
Supervisión de los grupos de recursos para detectar cambios .....	53
Activación de los eventos del ciclo de vida de los grupos .....	55
Crear una regla de eventos del ciclo de vida de un grupo .....	57
Crear una regla para capturar solo tipos de eventos específicos del ciclo de vida de un grupo .....	60
Desactivar los eventos del ciclo de vida del grupo .....	61
Estructura y sintaxis de los eventos .....	63
Estructura del campo <code>detail</code> .....	64
Ejemplo de patrones de eventos personalizados .....	72
Eliminación de grupos .....	76
Tipos de recursos admitidos .....	77
Amazon API Gateway .....	79
Amazon API Gateway V2 .....	79

---

Analizador de acceso de IAM .....	80
AWS Amplify .....	80
AWS App Mesh .....	80
Amazon AppStream .....	81
AWS AppSync .....	81
Amazon Athena .....	82
AWS Backup .....	82
AWS Batch .....	83
AWS Billing Conductor .....	83
Amazon Braket .....	84
AWS Certificate Manager .....	84
AWS Certificate Manager Autoridad de certificación privada .....	84
AWS Cloud9 .....	85
AWS CloudFormation .....	85
Amazon CloudFront .....	85
AWS Cloud Map .....	86
AWS CloudTrail .....	87
Amazon CloudWatch .....	87
Amazon CloudWatch Logs .....	88
Amazon CloudWatch Synthetics .....	88
AWS CodeArtifact .....	88
AWS CodeBuild .....	89
AWS CodeCommit .....	89
AWS CodeDeploy .....	90
CodeGuru Revisor de Amazon .....	90
Amazon CodeGuru Profiler .....	91
AWS CodePipeline .....	91
AWS CodeConnections .....	92
Amazon Cognito .....	92
Amazon Comprehend .....	92
AWS Config .....	93
Amazon Connect .....	94
Amazon Connect Wisdom .....	94
AWS Data Exchange .....	95
AWS Data Pipeline .....	95
AWS DataSync .....	95

AWS Database Migration Service .....	96
AWS Device Farm .....	96
Amazon DynamoDB .....	97
Amazon EMR .....	97
Contenedores de Amazon EMR .....	97
Amazon EMR sin servidor .....	98
Amazon ElastiCache .....	98
AWS Elastic Beanstalk .....	99
Amazon Elastic Compute Cloud (Amazon EC2) .....	99
Amazon Elastic Container Registry .....	104
Amazon Elastic Container Service .....	105
Amazon Elastic File System .....	105
Amazon Elastic Inference .....	106
Amazon Elastic Kubernetes Service (Amazon EKS) .....	106
Elastic Load Balancing .....	107
OpenSearch Servicio Amazon .....	107
CloudWatch Eventos de Amazon .....	108
EventBridge Esquemas de Amazon .....	108
Amazon FSx .....	109
Amazon Forecast .....	109
Amazon Fraud Detector .....	110
Amazon GameLift .....	111
AWS Global Accelerator .....	112
AWS Glue .....	112
AWS Glue DataBrew .....	113
AWS Ground Station .....	113
Amazon GuardDuty .....	114
Amazon Interactive Video Service .....	114
AWS Identity and Access Management .....	115
Generador de Imágenes de EC2 .....	116
Amazon Inspector .....	116
AWS IoT .....	117
AWS IoT Analytics .....	118
AWS IoT Events .....	118
AWS IoT FleetWise .....	119
AWS IoT Greengrass .....	119

AWS IoT Greengrass Version 2 .....	120
Consola de AWS IoT SiteWise .....	121
AWS IoT Wireless .....	121
AWS Key Management Service .....	122
Amazon Keyspaces (para Apache Cassandra) .....	123
Amazon Kinesis .....	123
Amazon Managed Service para Apache Flink .....	123
Amazon Data Firehose .....	124
AWS Lambda .....	124
Amazon Lightsail .....	125
Amazon MQ .....	126
Amazon Macie .....	126
Amazon Managed Blockchain .....	127
Transmisión gestionada de Amazon para Apache Kafka .....	127
AWS Elemental MediaConnect .....	127
AWS Elemental MediaPackage .....	128
AWS Network Manager .....	129
OpenSearch Servicio Amazon OpenSearch .....	129
AWS OpsWorks .....	130
AWS Organizations .....	130
Amazon Pinpoint .....	131
API de SMS y voz de Amazon Pinpoint .....	131
Amazon Quantum Ledger Database (Amazon QLDB) .....	132
Amazon Redshift .....	132
Amazon Relational Database Service (Amazon RDS) .....	133
AWS Resource Access Manager .....	135
AWS Resource Groups .....	135
AWS Robomaker .....	135
Amazon Route 53 .....	136
Amazon Route 53 Resolver .....	137
Amazon S3 Glacier .....	138
Amazon SageMaker .....	138
AWS Secrets Manager .....	140
AWS Service Catalog .....	140
AWS Service Catalog AppRegistry .....	141
Service Quotas .....	141

Amazon Simple Email Service .....	142
Amazon Simple Notification Service .....	142
Amazon Simple Queue Service .....	143
Amazon Simple Storage Service (Amazon S3) .....	143
AWS Step Functions .....	144
Storage Gateway .....	144
AWS Systems Manager .....	145
AWS Systems Manager para SAP .....	145
Amazon Timestream .....	146
AWS Transfer Family .....	146
AWS WAF .....	147
Amazon WorkSpaces .....	147
AWS X-Ray .....	148
Tipos de recursos obsoletos .....	148
Crear grupos con AWS CloudFormation recursos .....	149
Resource Groups y AWS CloudFormation plantillas .....	149
Obtenga más información sobre AWS CloudFormation .....	149
Seguridad .....	150
Protección de datos .....	151
Cifrado de datos .....	152
Privacidad del tráfico entre redes .....	152
Administración de identidades y accesos .....	153
Público .....	153
Autenticación con identidades .....	154
Administración de acceso mediante políticas .....	157
Cómo funciona Resource Groups con IAM .....	160
Políticas administradas de AWS .....	164
Uso de roles vinculados a servicios .....	167
Ejemplos de políticas basadas en identidad .....	170
Resolución de problemas .....	175
Registro y supervisión .....	177
Integración de CloudTrail .....	177
Validación de conformidad .....	180
Resiliencia .....	181
Seguridad de la infraestructura .....	182
Prácticas recomendadas de seguridad .....	183

---

Cuotas de servicio .....	184
Historial de documentos .....	185
Actualizaciones anteriores .....	196
.....	cxcvii

## ¿Qué son los grupos de recursos?

Puede usar los grupos de recursos para organizar AWS los recursos. AWS Resource Groups es el servicio que le permite gestionar y automatizar tareas en un gran número de recursos a la vez. 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 AWS servicio que utilice. Para obtener una lista de los servicios compatibles 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 el uso de Resource GroupsAPI, en AWS CLI comandos o lenguajes AWS SDK de programación. Consulte la [AWS Resource Groups APIreferencia](#) para obtener más información.

Para trabajar con grupos de recursos en el AWS Management Console hogar

1. Inicie sesión en 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.

## Los recursos y sus tipos de grupos

En AWS, un recurso es una entidad con la que puede trabajar. Los ejemplos incluyen una EC2 instancia de Amazon, una AWS CloudFormation pila o un bucket de Amazon S3. Si trabaja con varios recursos, puede resultarle útil administrarlos en grupo en lugar de pasar de un AWS servicio a otro para cada tarea. Si administra una gran cantidad de recursos relacionados, como EC2 las instancias que forman una capa de aplicación, es probable que necesite realizar acciones masivas en estos recursos al mismo tiempo. 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 AWS recursos que están todos en el mismo Región de AWS lugar y que cumplen 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 ningún otro tipo de información confidencial o delicada en las etiquetas. Utilizamos etiquetas para prestarle servicios de facturación y administración. Las etiquetas no se han diseñado para usarse con información privada o confidencial.

- AWS CloudFormation basado en pilas

Un grupo de recursos AWS CloudFormation basado en pilas basa su pertenencia a una consulta que especifica una AWS CloudFormation pila 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 la consulta en una sola AWS CloudFormation pila.

## Grupos de recursos vinculados a servicios

Algunos Servicios de AWS definen grupos de recursos que solo se pueden crear y administrar mediante la consola de ese servicio y APIs. 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 servicios para grupos de recursos](#) en la Guía de AWS Resource Groups API referencia.

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, AWS Management Console se organiza por AWS servicio. 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 en los recursos de una AWS CloudFormation pila. 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.
- Conjunto de AWS recursos que se utilizan juntos para un proyecto común o que se desean administrar o supervisar como 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. Siempre que IAM los responsables, como los roles y los usuarios, que comparten su cuenta tengan los IAM permisos correctos, podrán trabajar con los grupos de recursos que usted cree.

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.

## AWS Resource Groups recursos

En Resource Groups, el único recurso disponible son los grupos. Los grupos tienen nombres de recursos de Amazon (ARNs) exclusivos asociados a ellos. Para obtener más información sobre ARNs, consulte [Amazon Resource Names \(ARN\) y AWS Service Namespaces](#) en Referencia general de Amazon Web Services

Tipo de recurso	ARN Formato
Grupo de recursos	<code>arn:aws:resource-groups: <i>region</i>:<i>account</i>:group/<i>group-name</i></code>

## Cómo funciona el etiquetado

Las etiquetas son pares de claves y valores que actúan como metadatos para organizar AWS los recursos. Con la mayoría de AWS los recursos, tiene la opción de añadir etiquetas al crear el recurso, ya sea una EC2 instancia de Amazon, un bucket de Amazon S3 u otro recurso. No obstante, también puede añadir etiquetas a varios recursos admitidos a la vez mediante el editor de etiquetas. 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 ningún otro tipo de información confidencial o delicada en las etiquetas. Utilizamos etiquetas para prestarle 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.

## Empezar con AWS Resource Groups

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

En esta sección se muestra cómo empezar a utilizarlos AWS Resource Groups. En primer lugar, organice AWS los recursos etiquetándolos en el editor de etiquetas. 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.

Después de crear grupos de recursos en Resource Groups, utilice AWS Systems Manager herramientas como Automation para simplificar las tareas de administración de los grupos de recursos.

Para obtener más información sobre cómo empezar a utilizar AWS Systems Manager las funciones y herramientas, consulte la [Guía del AWS Systems Manager usuario](#).

### Temas

- [Requisitos previos para trabajar con AWS Resource Groups](#)
- [Más información sobre la AWS Resource Groups autorización y el control de acceso](#)

# Requisitos previos para trabajar con AWS Resource Groups

Antes de empezar a trabajar con grupos de recursos, asegúrese de tener un grupo activo AWS cuenta con los recursos existentes y los derechos correspondientes para etiquetar los recursos y crear grupos.

## Temas

- [Registrarse en AWS](#)
- [Crear recursos de](#)
- [Configuración de permisos](#)

## Registrarse en AWS

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

Para suscribirte a una Cuenta de AWS

1. Abrir <https://portal.aws.amazon.com/billing/registro>.
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, un Usuario raíz de la cuenta de AWS se crea. El usuario root tiene acceso a todos Servicios de AWS y los recursos de la 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 el AWS Resource Groups consola yAPI.

Si es administrador, puede proporcionar permisos a sus usuarios mediante la creación de políticas a través del AWS Identity and Access Management servicio (IAM). Primero debe crear sus funciones principales, como las IAM funciones o los usuarios, o bien asociar identidades externas a su AWS entorno mediante un servicio como AWS IAM Identity Center. A continuación, aplica las políticas con los permisos que necesitan los usuarios. Para obtener información sobre cómo crear y adjuntar IAM políticas, consulte [Trabajar con políticas](#).

## Permisos para servicios individuales

### Important

En esta sección se describen los permisos necesarios para etiquetar recursos de otras consolas de servicio y APIs agregar esos recursos a grupos de recursos.

Como se describe en [Los recursos y sus tipos de grupos](#), 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 EC2 instancias de Amazon, debes tener permisos para las acciones de etiquetado de ese servicioAPI, como las que se enumeran en la [Guía del EC2 usuario de Amazon](#).

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 AmazonEC2, consulta [Ejemplos de políticas para trabajar en la EC2 consola de Amazon](#) en la Guía del EC2 usuario de Amazon.

## Permisos obligatorios para Resource Groups y Tag Editor

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

### Utilización AWS políticas gestionadas para los permisos de Resource Groups y Tag Editor

AWS Resource Groups y Tag Editor admiten lo siguiente AWS políticas gestionadas que puede utilizar para proporcionar un conjunto predefinido de permisos a sus 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 IAM rol o 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 otorga al IAM rol o usuario adjunto permiso para llamar a cualquier operación de Resource Groups y a las operaciones de etiquetas de lectura y escritura 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 AWS-la política administrada [ReadOnlyAccess](#) otorga permisos a las operaciones de solo lectura para los recursos de cada servicio. AWS mantiene esta política actualizada automáticamente con las nuevas AWS servicios a medida que estén disponibles.
- Muchos servicios proporcionan un servicio de solo lectura específico AWS-políticas gestionadas que puede utilizar para limitar el acceso únicamente a los recursos proporcionados por ese servicio. Por ejemplo, Amazon EC2 proporciona [Amazon EC2ReadOnlyAccess](#).
- 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 de uso AWS Resource Groups y Tag Editor

Para añadir una política de uso AWS Resource Groups y Tag Editor a un usuario, haga lo siguiente.

1. Abra la [IAMconsola](#).
2. En el panel de navegación, seleccione Usuarios.
3. Busca el usuario al que quieres conceder AWS Resource Groups y permisos de editor de etiquetas. 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 JSONpestaña, pegue la siguiente declaración de política.

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

#### Note

En este ejemplo de declaración de política se conceden permisos únicamente para AWS Resource Groups y las acciones del editor de etiquetas. No permite el acceso a AWS Systems Manager tareas en el AWS Resource Groups console. 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 sobre la concesión de acceso a Systems

Manager, consulte [Configuración del acceso a Systems Manager](#) en AWS Systems Manager Guía del usuario.

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 adjuntarla a otros usuarios. Para obtener más información sobre cómo añadir una política a un usuario, consulte [Añadir permisos adjuntando políticas directamente al usuario en la](#) Guía del IAM usuario.

## 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. Resource Groups [ARNs](#) permite 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 a AWS Resource Groups las operaciones.

Resource Groups no admite políticas basadas en recursos.

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](#)
- [Acciones, recursos y claves de condición para AWS Resource Groups](#)
- [Control del acceso mediante políticas](#)

# AWS servicios que funcionan con AWS Resource Groups

Puede utilizar los siguientes AWS servicios con AWS Resource Groups.

AWS servicio	Uso con Resource Groups
<p><a href="#">AWS CloudFormation</a>— Cree grupos de recursos AWS CloudFormation mediante una plantilla de pila.</p>	<p>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.</p> <p>Para obtener más información, consulte la <a href="#">referencia sobre ResourceGroups los tipos de recursos</a> en la Guía del AWS CloudFormation usuario.</p>
<p><a href="#">CloudTrail</a>— Capture todas las acciones del grupo de recursos utilizando AWS CloudTrail.</p>	<p>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.</p> <p>Para obtener más información, consulte <a href="#">Visualización de eventos con el historial de CloudTrail eventos</a>.</p>
<p><a href="#">Amazon CloudWatch</a>: habilite la supervisión en tiempo real de sus AWS recursos y las aplicaciones en las que se ejecuta AWS.</p>	<p>Puede centrar su vista para ver estadísticas y alarmas desde un único grupo de recursos.</p> <p>Para obtener más información, consulte <a href="#">Centrarse en las métricas y las alarmas de un</a></p>

AWS servicio	Uso con Resource Groups
	<p><a href="#">grupo de recursos</a> en la Guía del CloudWatch usuario de Amazon.</p>
<p>Información sobre las <a href="#">CloudWatch aplicaciones de Amazon</a>: detecte problemas comunes con sus aplicaciones basadas en SQL Server y .NET.</p>	<p>Supervise los recursos de .NET y SQL Server que pertenecen a un grupo de recursos.</p> <p>Para obtener más información, consulte <a href="#">Componentes de aplicaciones compatibles</a> en la Guía del CloudWatch usuario de Amazon.</p>
<p><a href="#">Grupos de tablas de Amazon DynamoDB</a>: organice las tablas de DynamoDB en agrupaciones lógicas para poder administrar sus recursos con mayor facilidad.</p>	<p>Cree, edite y elimine grupos de tablas de DynamoDB desde el menú de acciones de DynamoDB.</p> <p>Para obtener más información, consulte la <a href="#">Guía del desarrollador de Amazon DynamoDB</a>.</p>
<p><a href="#">Hosts dedicados de Amazon EC2</a>: use las licencias de software existentes por conector, por núcleo o por VM, incluido Windows Server, Microsoft SQL Server, SUSE y Linux Enterprise Server.</p>	<p>Lance instancias de Amazon EC2 en grupos de recursos de host para maximizar el uso de hosts dedicados.</p> <p>Para obtener más información, consulte <a href="#">Trabajar con hosts dedicados</a> en la Guía del usuario de Amazon EC2.</p>

AWS servicio	Uso con Resource Groups
<p><a href="#">Reservas de capacidad de Amazon EC2</a>: 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.</p>	<p>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.</p> <p>Para obtener más información, consulte <a href="#">Trabajar con grupos de reserva de capacidad</a> en la Guía del usuario de Amazon EC2.</p>
<p><a href="#">AWS License Manager</a>: simplifica el proceso de llevar licencias de proveedores de software a la nube.</p>	<p>Configure un grupo de recursos de hosts para permitir que License Manager administre sus hosts dedicados.</p> <p>Para obtener más información, consulte <a href="#">Grupos de recursos de host en License Manager</a> en la Guía del usuario de License Manager.</p>
<p><a href="#">AWS Resilience Hub</a>: prepare y proteja sus aplicaciones de las interrupciones.</p>	<p>Descubra las aplicaciones que se definen mediante Resource Groups.</p> <p>Para obtener más información, consulte <a href="#">Mida y mejore la resiliencia de sus aplicaciones con AWS Resilience Hub</a> en el blog de noticias de AWS .</p>

AWS servicio	Uso con Resource Groups
<p><a href="#">AWS Resource Access Manager</a>— Comparta AWS los recursos específicos de su propiedad con otras cuentas.</p>	<p>Comparta los grupos de recursos del anfitrión mediante AWS RAM.</p> <p>Para obtener más información, consulte <a href="#">Recursos compartibles</a> en la Guía del usuario de AWS RAM .</p>
<p><a href="#">AWS Service Catalog AppRegistry</a>: Defina y gestione sus aplicaciones y metadatos.</p>	<p>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.</p> <p>Para obtener más información, consulte <a href="#">Utilización AppRegistry</a> en la Guía del AWS Service Catalog administrador.</p>

AWS servicio	Uso con Resource Groups
<p><a href="#">AWS Systems Manager</a>— Habilite la visibilidad y el control de sus AWS recursos.</p>	<p>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 ayudarlo a determinar qué recursos de una aplicación son conformes y funcionan correctamente y qué recursos requieren una acción.</p> <p>Para obtener más información, consulte <a href="#">Uso de aplicaciones en Application Manager</a> en la Guía del usuario de AWS Systems Manager .</p>
<p><a href="#">Analizador de acceso a la red Amazon VPC</a>: identifique el acceso no deseado a los recursos de la red en AWS.</p>	<p>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.</p> <p>Para obtener más información, consulte <a href="#">Utilizar Resource Groups con Network Access Scopes</a> en la Guía del usuario de Amazon Virtual Private Cloud.</p>

## 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 la configuración que

se aplicará a los miembros del grupo como una configuración en forma de estructura de [JSON](#) datos 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](#)
- [JSONsintaxis 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 . AWS SDK Algunos servicios administran por completo sus grupos vinculados a servicios y no se pueden modificar de ninguna manera excepto según lo permitan la consola o los comandos proporcionados por el servicio propietario. AWS Sin embargo, en algunos casos, puede interactuar con la configuración del servicio mediante las siguientes API operaciones en AWS SDKs o sus equivalentes: AWS CLI

- Puede adjuntar su propia configuración a un grupo al crear el grupo mediante la [CreateGroup](#) operación.
- Puede modificar la configuración actual adjunta a un grupo mediante la [PutGroupConfiguration](#) operación.
- Puede ver la configuración actual de un grupo de recursos llamando a la [GetGroupConfiguration](#) operación.

## JSONsintaxis 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 [JSON](#) objeto. 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 *placeholders* 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.

```
[
  {
    "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::HostManagement`.

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 `HostManagement` grupo solo pueda contener `hosts EC2` dedicados de Amazon.
- `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 `CapacityReservation` grupo solo pueda contener la capacidad de reserva `EC2` de capacidad de Amazon.

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 que solo `EC2` alojen instancias de Amazon.

```
[
  {
    "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.

```

[
  {
    "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 [Amazon Resource Name \(ARN\)](#) de la aplicación asignada por AppRegistry.

Tipo de datos de valores: cadena

Valores permitidos: válidosARN.

Obligatorio: sí

#### Note

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

Este grupo de recursos de la aplicación incluye automáticamente como miembros del grupo [los grupos de recursos creados para las AWS CloudFormation pilas](#) asociadas a la AppRegistry aplicación. Puede usar la [ListGroupResources](#) operación 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`.

```
[
  {
    "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 [Amazon Resource Name \(ARN\)](#) de la AWS CloudFormation pila adjunta a la aplicación en AppRegistry.

Tipo de datos de valores: cadena

Valores permitidos: a válidosARN.

Obligatorio: sí

 **Note**

Para cambiar cualquiera de estos elementos, debe modificar la aplicación mediante la AppRegistry consola o un dispositivo equivalente AWS SDK y AWS CLI las operaciones.

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

```
[
  {
    "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 EC2 capacidad de Amazon. 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 te permite lanzar una EC2 instancia de Amazon 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, consulta [Cómo trabajar con grupos de reserva de capacidad](#) en la Guía del EC2 usuario de Amazon.

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 EC2 de capacidad de Amazon 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.

```

[
  {
    "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 para la administración de EC2 hosts de Amazon 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 anfitriones EC2 dedicados de Amazon 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, consulta [Cómo entender la colocación automática y la afinidad](#) en la Guía del EC2 usuario de Amazon.

Tipo de datos de valores: booleano

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

Obligatorio: no

```
[
  {
    "Type": "AWS::EC2::HostManagement",
    "Parameters": [
      {
        "Name": "auto-allocate-host",
        "Values": [ "true" ]
      },
      {
        "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" ]
      }
    ]
  }
]
```

- **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, consulta la [sección Liberar hosts dedicados](#) en la Guía del EC2 usuario de Amazon.

Tipo de datos de valores: booleano

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

Obligatorio: no

```
[
  {
    "Type": "AWS::EC2::HostManagement",
    "Parameters": [
      {
        "Name": "auto-release-host",
        "Values": [ "false" ]
      },
      {
        "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" ]
      }
    ]
  }
]
```

- **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 EC2 instancias de Amazon](#) válido C4, como 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.

```
[
  {
    "Type": "AWS::EC2::HostManagement",
    "Parameters": [
      {
        "Name": "allowed-host-families",
        "Values": ["c5", "m5"]
      },
      {
        "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"]
      }
    ]
  }
]
```

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

Este parámetro especifica las rutas de [Amazon Resource Name \(ARN\)](#) 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. ARNs

Valores permitidos: cada uno debe ser una [configuración de License Manager](#) válidaARN.

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.

```
[
  {
    "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.

```
[
  {
    "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.

```
[
  {
    "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 grupo

ARN 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 AWS SDK operación.

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"  
  }  
}
```

# Crear grupos basados en consultas en AWS Resource Groups

## 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 contenga todas las EC2 instancias de Amazon y los buckets de Amazon S3 que utiliza para ejecutar la fase de prueba de una aplicación y tiene instancias y buckets etiquetados de esta manera, elija los tipos de recursos y los tipos de `AWS::S3::Bucket` recursos de la lista desplegable `AWS::EC2::Instance` 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. Contiene una representación en cadena de una JSON estructura 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 admitidos por 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 JSON elementos deben combinarse en una representación de cadena de una sola línea de la JSON estructura. Por ejemplo, considere a Query con la siguiente JSON estructura de ejemplo. Esta consulta debe coincidir únicamente con las EC2 instancias de Amazon que tengan la etiqueta «Stage» con el valor «Test».

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

Esto se JSON puede representar como la siguiente cadena de una sola línea y se puede usar como el valor del Query elemento. Como el valor de una JSON estructura debe ser una cadena

entre comillas dobles, debe evitar los caracteres incrustados entre comillas dobles o barras diagonales y colocarlos delante de una barra invertida, como se muestra a continuación:

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

A continuación, la ResourceQuery cadena completa se representa como parámetro de comando, tal y como se muestra a continuación: 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 AWS CloudFormation basada en pilas, eliges una AWS CloudFormation pila de tu cuenta en la región actual y, a continuación, eliges los tipos de recursos de la pila que quieres que formen parte del grupo. Puede basar la consulta en una sola AWS CloudFormation pila.

#### Note

Una AWS CloudFormation pila puede contener otras pilas 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 AWS CloudFormation pilas 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 AWS CloudFormation pila no se convierten en miembros del grupo. Por ejemplo, si un grupo de autoescalado es creado AWS CloudFormation como parte de la pila, entonces ese grupo de autoescalado es miembro del grupo. Sin embargo, una EC2 instancia de Amazon creada por ese grupo de autoscalamiento como parte de su operación no es miembro del grupo de recursos basado en AWS CloudFormation pilas.

Si creas un grupo basado en una AWS CloudFormation pila y el estado de la pila cambia a uno que ya no se admite como base para una consulta de grupo, por ejemplo, el grupo de recursos sigue existiendo, pero no tiene recursos de miembros. DELETE\_COMPLETE

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

La sintaxis del `ResourceQuery` parámetro de un grupo de recursos CloudFormation basado en una pila 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 una pila, 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 en cadena de una JSON estructura 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 del recurso de Amazon (ARN) de la AWS CloudFormation pila cuyos recursos desea incluir en el grupo.

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

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

Esto se JSON puede representar como la siguiente cadena de una sola línea y se puede usar como el valor del Query elemento. Como el valor de una JSON estructura debe ser una cadena entre comillas dobles, debe evitar los caracteres incrustados entre comillas dobles o barras diagonales y colocarlos delante de 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\" }
```

A continuación, la ResourceQuery cadena completa se representa como parámetro de comando, tal y como se muestra a continuación: 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 página Crear 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:::Instance yEC2::S3 AWS:::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. Aún en Criterios de agrupación, selecciona Vista previa de los recursos del grupo para ver la lista de EC2 instancias y depósitos de S3 de tu cuenta que coinciden con la clave o claves de etiqueta especificadas.
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, añade 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 AWS CLI sesión, escribe lo siguiente y, a continuación, presiona Entrar y reemplaza los valores del nombre del grupo, la descripción, los tipos de recursos, las claves y los valores de las etiquetas por los tuyos. 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, utilice `AWS::AllSupported` como el valor de `ResourceTypeFilters`.

```
$ aws resource-groups create-group \
  --name resource-group-name \
  --resource-query '{"Type":"TAG_FILTERS_1_0","Query":{"ResourceTypeFilters": [{"ResourceType": "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\n":["AWS::EC2::Instance"],\n"TagFilters":{"Key":"Stage","Values":["Test"]}}}'
```

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

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

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 AWS CloudFormation basado en pilas

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 CloudFormation pilas.
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. 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. Seleccione Ver recursos de grupo para obtener la lista de recursos de la AWS CloudFormation pila que coinciden con los tipos de recursos seleccionados.
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 AWS CloudFormation basado en pilas se basa en un tipo de consulta.

`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.

La *stack\_identifier* es la pilaARN, 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 AWS CloudFormation basado en una pila, 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 que están disponibles en la pila, actualice la AWS CloudFormation plantilla utilizada para crear la pila y, a continuación, actualice la pila en ella. AWS CloudFormation Para obtener más información sobre cómo actualizar una AWS CloudFormation pila, consulta [las actualizaciones de AWS CloudFormation pilas](#) en la Guía del AWS CloudFormation usuario.

En el AWS CLI, se actualizan los grupos mediante dos comandos.

- `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.

En la consola, no se puede cambiar un grupo AWS CloudFormation basado en pilas a un grupo de consultas basado en etiquetas ni viceversa. Sin embargo, puede hacerlo mediante los Resource GroupsAPI, incluidos los AWS CLI.

## Actualizar grupos de consultas basados en etiquetas

Los siguientes procedimientos muestran cómo actualizar un grupo de consultas basado 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 en AWS License Manager todos los grupos con un propietario de cuenta distinto del grupo en el que has iniciado sesión. Para obtener más información, consulte [Grupos de recursos de host de AWS 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, agregamos 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. Selecciona Vista previa de los recursos del grupo para recuperar la lista actualizada de EC2 instancias, buckets S3 e instancias de RDS bases de datos de Amazon de tu cuenta que

coinciden 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 el AWS CLI, se actualiza la consulta de un grupo y se actualiza la descripción de un grupo de recursos mediante dos comandos diferentes. No se puede editar el nombre de un grupo existente. En el AWS CLI, puede cambiar un grupo basado en etiquetas a un grupo CloudFormation basado en pilas o viceversa.

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

```
$ 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.

## Actualice un grupo AWS CloudFormation basado en pilas

Los siguientes procedimientos muestran cómo actualizar un grupo basado en CloudFormation pilas.

### Console

No puede cambiar un grupo basado en AWS CloudFormation pilas a un grupo basado en etiquetas en el. 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 en AWS License Manager todos los grupos con un propietario de cuenta distinto del grupo en el que has iniciado sesión. Para obtener más información, consulte [Grupos de recursos de host en AWS 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. Seleccione Vista previa de los recursos del grupo para recuperar la lista de recursos de la AWS CloudFormation pila que coinciden con los tipos de recursos seleccionados.
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 finalizado, elija Guardar cambios.

## AWS CLI & AWS SDKs

En el AWS CLI, se actualiza la consulta de un grupo y se actualiza la descripción de un grupo de recursos mediante dos comandos diferentes. No se puede editar el nombre de un grupo existente. En el AWS CLI, puede cambiar un grupo basado en etiquetas a un grupo CloudFormation basado en pilas 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.

- 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.

La *stack\_identifier* es la pilaARN, 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 monitorizar esos grupos para detectar cambios que se le 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 tus grupos de recursos, permites que Amazon capture los eventos relacionados con los cambios en tus grupos EventBridge y los ponga a disposición de todos los distintos servicios de destino EventBridge compatibles. A continuación, puede configurar esos servicios de destino para que realicen automáticamente las acciones que requiera su situación. Estos objetivos incluyen una variedad de AWS servicios como Amazon Simple Notification Service (AmazonSNS), Amazon Simple Queue Service (AmazonSQS) y AWS Lambda. Con servicios como Lambda, sus eventos pueden disparar respuestas programáticas que utilizan código para realizar cualquier acción que necesite. Para ver una lista de los AWS servicios con los que puedes segmentar EventBridge, consulta [Amazon EventBridge Targets](#) en la Guía del EventBridge usuario de Amazon.

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

- Un rol AWS Identity and Access Management (IAM) vinculado al servicio que tiene permiso para supervisar tus recursos para detectar cualquier cambio en sus etiquetas y tus AWS CloudFormation pilas para detectar cualquier cambio en los recursos que forman parte de una pila.
- Una EventBridge regla gestionada por Resource Groups que captura los detalles de cualquier cambio en las etiquetas o pilas de los recursos. EventBridge usa esta regla para notificar dichos cambios a Resource Groups. A continuación, Resource Groups genera eventos de membresía EventBridge para enviarlos a los que se procesen las 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. También se puede producir un cambio de membresía cuando cambian las etiquetas o cuando cambia una AWS CloudFormation pila.

#### Important

- Para recibir y responder correctamente a los eventos grupales, debe realizar cambios en Resource Groups y EventBridge. Puede realizar los cambios en cualquier orden, pero no se publicará ningún evento de grupo en EventBridge los destinos hasta que no haya realizado 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 EventBridge regla que utilice la `aws.tag` fuente, en lugar de la `aws.resource-groups` fuente. Para obtener más información, consulte [Etiquetar eventos de cambio en AWS los recursos](#) en la Guía del EventBridge usuario de Amazon.

#### Temas

- [Activación de eventos del ciclo de vida del grupo en Resource Groups](#)
- [Crear una EventBridge regla para capturar los eventos del ciclo de vida del grupo y publicar las notificaciones](#)

- [Desactivar los eventos del ciclo de vida del grupo](#)
- [Estructura y sintaxis de los eventos del ciclo de vida de Resource Groups](#)

## 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, [PutRule](#) y [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

## Temas

- [Estructura del campo detail](#)
- [Ejemplos de patrones de eventos EventBridge personalizados para diferentes casos de uso](#)

Los eventos del ciclo de vida AWS Resource Groups adoptan la forma de cadenas de [JSON](#) objetos en 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:

Nombre del campo	Tipo	Descripción
		<ul style="list-style-type: none"> <li>• <a href="#">ResourceGroups Group State Change</a> : representa los cambios en el estado general del grupo y sus propiedades.</li> <li>• <a href="#">ResourceGroups Group Membership Change</a>: representa los cambios en la composición del grupo.</li> </ul>
source	Cadena	En el caso de Resource Groups, este valor es siempre "aws.resource-groups" .
resources	Un conjunto de nombres de recursos de Amazon (ARNs)	<p>Este campo siempre incluye el <a href="#">nombre del recurso de Amazon (ARN)</a> del grupo con el cambio que desencadenó este evento.</p> <p>Este campo también puede incluir ARNs los recursos añadidos o retirados del grupo, si corresponde.</p>
detail	JSONcadena de objetos	Esta es la carga del evento. El contenido del campo detail depende del valor del campo detail-type . <a href="#">Para obtener más información, consulte la siguiente sección.</a>

## 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 grupo ARN y un "unique-id" campo 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 identificador único ARN y el identificador único como clave del grupo de sus programas que interactúa 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
<code>event-sequence</code>	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.
<code>group</code>	<a href="#">Group</a> JSONObjeto	El objeto de grupo asociado al evento por su ARN nombre e identificador único.
<code>state-change</code>	Cadena	El tipo de cambio de estado que se ha producido. Puede ser cualquiera de los siguientes valores: <ul style="list-style-type: none"> <li>• <a href="#">create</a></li> <li>• <a href="#">update</a></li> <li>• <a href="#">delete</a></li> </ul>
<code>old-state</code>	<a href="#">GroupState</a> JSONObjeto	El estado del grupo antes del cambio. El objeto incluye solo los valores de las propiedades que han cambiado.

Nombre del campo	Tipo	Descripción
new-state	<a href="#">GroupState</a> e_JSONobjeto	El estado del grupo después del cambio. El objeto incluye solo los valores de las propiedades que han cambiado.

El group JSON objeto 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 GUID valor único que distingue entre un grupo que se eliminó y un grupo diferente que se creó posteriormente con el mismo nombre yARN. Usa la concatenación de ARN y este valor como clave única para el grupo cuando consumas estos eventos en tu código.

Los GroupState JSON objetos 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	ResourceQuery JSONobjeto	Una JSON representación 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 <a href="#">tipo ResourceQuery API de datos</a> .

Nombre del campo	Tipo	Descripción
		Se incluyen ejemplos de esto en los ejemplos de eventos de <a href="#">Create</a> y <a href="#">Update</a> .
group-configuration	Configuración JSON Objeto	Una JSON representación de los parámetros de configuración asociados a un grupo vinculado a un servicio. Para obtener más información, consulte <a href="#">Configuraciones de servicios para grupos de recursos</a> en la AWS Resource Groups API Referencia.

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 coincide únicamente con las instancias de Amazon Elastic Compute Cloud (AmazonEC2) 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-6c4a10fccee"
      },
      "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 EC2 volumen de Amazon 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-6c4a10fccea"
    },
    "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-6c4a10fccee"
      }
    }
  }
}

```

## 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. Si `detail-type` se especifica esto, el `resources` campo de nivel superior incluye el ARN del grupo cuya membresía se cambió y ARNs los recursos que se agregaron o eliminaron 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
<code>event-sequence</code>	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.

Nombre del campo	Tipo	Descripción
group	GroupJSONObjeto	Identifica el objeto de grupo asociado al evento por su ARN nombre e identificador único.
resources	Matriz de ResourceChange JSON objetos	<p>Conjunto de recursos cuya pertenencia a un grupo ha cambiado.</p> <p>Este objeto ResourceChange incluye los siguientes campos para cada recurso:</p> <ul style="list-style-type: none"> <li>• membership-change : el valor es "add" o "remove".</li> <li>• arn— El ARN del recurso añadido o eliminado.</li> <li>• resource-type : el tipo de recurso agregado o eliminado.</li> </ul>

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-6c4a10fccee"
    }
  }
}
```

```

    },
    "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, sustituya cada uno *user input placeholder* con tu propia 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 ARNs 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 [AWS Resource Groups consola](#) 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 [Resource Groups 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* con el nombre de su grupo.

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

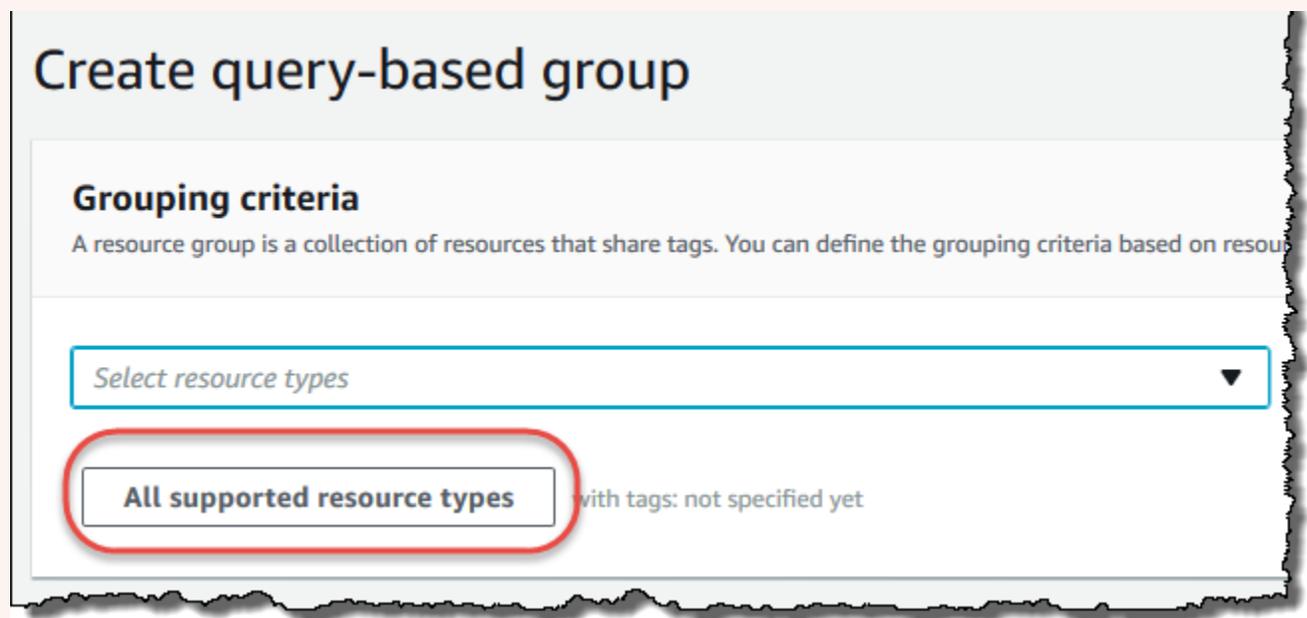
2. Cuando se le pida que confirme la eliminación, escriba yes y, a continuación, pulse Intro.

# 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	X No	X No	✓ Sí
AWS::ApiGateway::ApiKey	X No	✓ Sí	✓ Sí
AWS::ApiGateway::ClientCertificate	X No	✓ Sí	X No
AWS::ApiGateway::DomainName	X No	X No	✓ Sí
AWS::ApiGateway::RestApi	X No	✓ Sí	✓ Sí
AWS::ApiGateway::Stage	X No	✓ Sí	X No
AWS::ApiGateway::UsagePlan	X 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	X No	✓ Sí	X No

## Analizador de acceso de IAM

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

## AWS Amplify

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

## AWS App Mesh

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::AppMesh::Mesh	X No	✓ Sí	X 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
<code>AWS::Batch::ComputeEnvironment</code>	X No	✓ Sí	X No
<code>AWS::Batch::JobQueue</code>	X No	✓ Sí	X No
<code>AWS::Batch::SchedulingPolicy</code>	X No	✓ Sí	X No

## AWS Billing Conductor

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
<code>AWS::BillingConductor::BillingGroup</code>	X No	✓ Sí	✓ Sí
<code>AWS::BillingConductor::CustomLineItem</code>	X No	✓ Sí	✓ Sí
<code>AWS::BillingConductor::PricingPlan</code>	X No	✓ Sí	✓ Sí
<code>AWS::BillingConductor::PricingRule</code>	X 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 <sup>1</sup>	✓ Sí <sup>2</sup>	✓ Sí <sup>2</sup>

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en Stack
AWS::CloudFront::StreamingDistribution	✓ Sí <sup>1</sup>	✓ Sí <sup>2</sup>	✓ Sí <sup>2</sup>

<sup>1</sup> 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.

<sup>2</sup> 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 una 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	× No

## AWS CodeCommit

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

## AWS CodeDeploy

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
<code>AWS::CodeDeploy::Application</code>	X No	✓ Sí	✓ Sí
<code>AWS::CodeDeploy::DeploymentConfig</code>	X No	X No	✓ Sí

## CodeGuru Revisor de Amazon

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en Stack
<code>AWS::CodeGuruReviewer::RepositoryAssociation</code>	✓ 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
<code>AWS::CodeStarConnections::Connection</code>	✗ No	✓ Sí	✗ No

## Amazon Cognito

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
<code>AWS::Cognito::IdentityPool</code>	✓ Sí	✓ Sí	✓ Sí
<code>AWS::Cognito::UserPool</code>	✓ Sí	✓ Sí	✓ Sí

## Amazon Comprehend

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
<code>AWS::Comprehend::DocumentClassifier</code>	✓ 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
<code>AWS::Connect::Instance</code>	X No	✓ Sí	X No
<code>AWS::Connect::PhoneNumber</code>	X No	✓ Sí	X No

## Amazon Connect Wisdom

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
<code>AWS::Wisdom::Assistant</code>	X No	✓ Sí	✓ Sí
<code>AWS::Wisdom::AssistantAssociation</code>	X No	✓ Sí	✓ Sí
<code>AWS::Wisdom::Content</code>	X No	✓ Sí	X No
<code>AWS::Wisdom::KnowledgeBase</code>	X No	✓ Sí	✓ Sí
<code>AWS::Wisdom::Session</code>	X No	✓ Sí	X 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	X No	✓ Sí	✓ Sí
AWS::EMRServerless::JobRun	X No	✓ Sí	X 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	X No	✓ Sí	X No
AWS::ElastiCache::SecurityGroup	X No	✓ Sí	X No
AWS::ElastiCache::Snapshot	✓ Sí	✓ Sí	X No
AWS::ElastiCache::SubnetGroup	X No	✓ Sí	X No
AWS::ElastiCache::User	X No	✓ Sí	X No
AWS::ElastiCache::UserGroup	X No	✓ Sí	X 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	X No	✓ Sí	X No
AWS::EC2::IPv6Pool	X No	✓ Sí	X No
AWS::EC2::KeyPair	X No	✓ Sí	X No
AWS::EC2::LaunchTemplate	X No	✓ Sí	✓ Sí
AWS::EC2::LocalGateway	X No	✓ Sí	X No
AWS::EC2::LocalGatewayRouteTable	X No	✓ Sí	X No
AWS::EC2::LocalGatewayRouteTableVirtualInterfaceGroupAssociation	X No	✓ Sí	X No
AWS::EC2::LocalGatewayRouteTableVPASSOCIATION	X No	✓ Sí	X No
AWS::EC2::LocalGatewayVirtualInterface	X No	✓ Sí	X No
AWS::EC2::LocalGatewayVirtualInterfaceGroup	X No	✓ Sí	X No
AWS::EC2::NatGateway	✓ Sí	✓ Sí	✓ Sí
AWS::EC2::NetworkACL	✓ Sí	✓ Sí	✓ Sí
AWS::EC2::NetworkInsightsAccessScope	X No	✓ Sí	X No
AWS::EC2::NetworkInsightsAccessScopeAnalysis	X No	✓ Sí	X No

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

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::EC2::TransitGateway	X No	✓ Sí	X No
AWS::EC2::TransitGatewayAttachment	X No	✓ Sí	X No
AWS::EC2::TransitGatewayConnectPeer	X No	✓ Sí	X No
AWS::EC2::TransitGatewayMulticastDomain	X No	✓ Sí	X No
AWS::EC2::TransitGatewayPolicyTable	X No	✓ Sí	X No
AWS::EC2::TransitGatewayRouteTable	X No	✓ Sí	X No
AWS::EC2::TransitGatewayRouteTableAnnouncement	X No	✓ Sí	X No
AWS::EC2::VerifiedAccessEndpoint	X No	✓ Sí	X No
AWS::EC2::VerifiedAccessGroup	X No	✓ Sí	X No
AWS::EC2::VerifiedAccessInstance	X No	✓ Sí	X No
AWS::EC2::VerifiedAccessTrustProvider	X No	✓ Sí	X No
AWS::EC2::Volume	✓ Sí	✓ Sí	✓ Sí
AWS::EC2::VPC	✓ Sí	✓ Sí	✓ Sí
AWS::EC2::VPCEndpoint	X No	✓ Sí	X No
AWS::EC2::VPCEndpointConnection	X No	✓ Sí	X No
AWS::EC2::VPCEndpointService	X No	✓ Sí	X 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	X No	✓ Sí	X No
AWS::ECS::Cluster	✓ Sí	✓ Sí	X No
AWS::ECS::ContainerInstance	X No	✓ Sí	X No
AWS::ECS::Service	X No	✓ Sí	X No
AWS::ECS::Task	X No	✓ Sí	X No
AWS::ECS::TaskDefinition	✓ Sí	✓ Sí	X No
AWS::ECS::TaskSet	X No	✓ Sí	X 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	X No	✓ Sí	X 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	X No	✓ Sí	X No
AWS::EventSchemas::Registry	X No	✓ Sí	X No
AWS::EventSchemas::Schema	X No	✓ Sí	X 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	X No	✓ Sí	X No

## AWS Glue

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::Glue::Crawler	✓ Sí	✓ Sí	X No
AWS::Glue::Database	X No	✓ Sí	✓ Sí
AWS::Glue::Job	✓ Sí	✓ Sí	X No
AWS::Glue::MLTransform	X No	✓ Sí	X No
AWS::Glue::Registry	X No	✓ Sí	X No
AWS::Glue::Trigger	✓ Sí	✓ Sí	X No
AWS::Glue::Workflow	X No	✓ Sí	X 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::DataflowEndpoint Group	× 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	X No	✓ Sí	✓ Sí
AWS::GuardDuty::Filter	X No	✓ Sí	X No
AWS::GuardDuty::IPSet	X No	✓ Sí	X No
AWS::GuardDuty::ThreatIntelSet	X No	✓ Sí	X No

## Amazon Interactive Video Service

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::IVS::Channel	X No	✓ Sí	X No
AWS::IVS::RecordingConfiguration	X No	✓ Sí	X No
AWS::IVS::StreamKey	X No	✓ Sí	X 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 <sup>1</sup>	✓ Sí <sup>2</sup>	× No
AWS::IAM::ManagedPolicy	✓ Sí <sup>1</sup>	✓ Sí <sup>2</sup>	× No
AWS::IAM::OpenIDConnectProvider	✓ Sí <sup>1</sup>	✓ Sí <sup>2</sup>	× No
AWS::IAM::Role	× No	× No	✓ Sí <sup>2</sup>
AWS::IAM::SAMLProvider	✓ Sí <sup>1</sup>	✓ Sí <sup>2</sup>	× No
AWS::IAM::ServerCertificate	✓ Sí <sup>1</sup>	✓ Sí <sup>2</sup>	× No
AWS::IAM::VirtualMFADevice	✓ Sí <sup>1</sup>	✓ Sí <sup>2</sup>	× No

<sup>1</sup> 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.

<sup>2</sup> 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	X No	✓ Sí	X No
AWS::ImageBuilder::ContainerRecipe	X No	✓ Sí	X No
AWS::ImageBuilder::DistributionConfiguration	X No	✓ Sí	X No
AWS::ImageBuilder::Image	X No	✓ Sí	X No
AWS::ImageBuilder::ImagePipeline	X No	✓ Sí	X No
AWS::ImageBuilder::ImageRecipe	X No	✓ Sí	X No
AWS::ImageBuilder::InfrastructureConfiguration	X No	✓ Sí	X No

## Amazon Inspector

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

# AWS IoT

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::IoT::Authorizer	X No	✓ Sí	X No
AWS::IoT::BillingGroup	X No	✓ Sí	X No
AWS::IoT::CACertificate	X No	✓ Sí	X No
AWS::IoT::CustomMetric	X No	✓ Sí	X No
AWS::IoT::Dimension	X No	✓ Sí	X No
AWS::IoT::JobTemplate	X No	✓ Sí	X No
AWS::IoT::MitigationAction	X No	✓ Sí	X No
AWS::IoT::Policy	X No	✓ Sí	X No
AWS::IoT::RoleAlias	X No	✓ Sí	X No
AWS::IoT::ScheduledAudit	X No	✓ Sí	X No
AWS::IoT::SecurityProfile	X No	✓ Sí	X No
AWS::IoT::ThingGroup	X No	✓ Sí	X No
AWS::IoT::ThingType	X No	✓ Sí	X No
AWS::IoT::TopicRule	X 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::IoT FleetWise::Campaign	× No	✓ Sí	✓ Sí
AWS::IoT FleetWise::DecoderManifest	× No	✓ Sí	✓ Sí
AWS::IoT FleetWise::Fleet	× No	✓ Sí	✓ Sí
AWS::IoT FleetWise::ModelManifest	× No	✓ Sí	✓ Sí
AWS::IoT FleetWise::SignalCatalog	× No	✓ Sí	✓ Sí
AWS::IoT FleetWise::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	X No	✓ Sí	X No
AWS::IoTSiteWise::AssetModel	X No	✓ Sí	X No
AWS::IoTSiteWise::Dashboard	X No	✓ Sí	X No
AWS::IoTSiteWise::Gateway	X No	✓ Sí	X No
AWS::IoTSiteWise::Portal	X No	✓ Sí	X No
AWS::IoTSiteWise::Project	X No	✓ Sí	X No

## AWS IoT Wireless

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::IoTWireless::Destination	X No	✓ Sí	X No
AWS::IoTWireless::DeviceProfile	X No	✓ Sí	X No
AWS::IoTWireless::FuotaTask	X No	✓ Sí	X No
AWS::IoTWireless::MulticastGroup	X No	✓ Sí	X 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	X No	✓ Sí	✓ Sí
AWS::Cassandra::Table	X No	✓ Sí	X 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 gestionada 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	X No	✓ Sí	X No
AWS::NetworkManager::Device	X No	✓ Sí	X No
AWS::NetworkManager::GlobalNetwork	X No	✓ Sí	X No
AWS::NetworkManager::Link	X No	✓ Sí	X No
AWS::NetworkManager::Site	X No	✓ Sí	X No
AWS::NetworkManager::VpcAttachment	X No	✓ Sí	X 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	X No	✓ Sí	✓ Sí
AWS::OpsWorks::Layer	X No	✓ Sí	✓ Sí
AWS::OpsWorks::Stack	X 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	X No
AWS::Organizations::OrganizationalUnit	X No	✓ Sí	X No
AWS::Organizations::Policy	X No	✓ Sí	X No
AWS::Organizations::Root	✓ Sí	✓ Sí	X No

## Amazon Pinpoint

Recursos	Etiquetado de Tag Editor	Grupos basados en etiquetas	AWS CloudFormation Grupos basados en pilas
AWS::Pinpoint::App	X No	✓ Sí	✓ Sí
AWS::Pinpoint::EmailTemplate	X No	✓ Sí	✓ Sí
AWS::Pinpoint::PushTemplate	X No	✓ Sí	✓ Sí
AWS::Pinpoint::SmsTemplate	X No	✓ Sí	✓ Sí
AWS::Pinpoint::VoiceTemplate	X No	✓ Sí	X 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	X No	✓ Sí	X 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 <sup>1</sup>	✓ Sí <sup>2</sup>	✗ No
AWS::Route53::HealthCheck	✓ Sí <sup>1</sup>	✓ Sí <sup>2</sup>	✓ Sí <sup>2</sup>
AWS::Route53::HostedZone	✓ Sí <sup>1</sup>	✓ Sí <sup>2</sup>	✓ Sí <sup>2</sup>

<sup>1</sup> 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.

<sup>2</sup> 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	X No	✓ Sí <sup>2</sup>	X No
AWS::Route53Resolver::FirewallRuleGroup	X No	✓ Sí <sup>2</sup>	X No
AWS::Route53Resolver::FirewallRuleGroupAssociation	X No	✓ Sí <sup>2</sup>	X No
AWS::Route53Resolver::ResolverEndpoint	✓ Sí <sup>1</sup>	✓ Sí <sup>2</sup>	X No
AWS::Route53Resolver::ResolverQueryLoggingConfig	X No	✓ Sí <sup>2</sup>	X No
AWS::Route53Resolver::ResolverRule	✓ Sí <sup>1</sup>	✓ Sí <sup>2</sup>	X No

<sup>1</sup> 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.

<sup>2</sup> 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	X No	✓ Sí	X No
AWS::SageMaker::Image	X No	✓ Sí	X No
AWS::SageMaker::LabelingJob	X No	✓ Sí	X No
AWS::SageMaker::Model	X No	✓ Sí	✓ Sí
AWS::SageMaker::ModelPackageGroup	X No	✓ Sí	✓ Sí
AWS::SageMaker::NotebookInstance	✓ Sí	✓ Sí	✓ Sí
AWS::SageMaker::Pipeline	X No	✓ Sí	X No
AWS::SageMaker::Project	X No	✓ Sí	✓ Sí
AWS::SageMaker::TrainingJob	X No	✓ Sí	X No
AWS::SageMaker::TransformJob	X No	✓ Sí	X No
AWS::SageMaker::Workteam	X No	✓ Sí	X 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	× No	✓ Sí	× No
AWS::S3::StorageLens	× No	✓ Sí	× 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	× No
AWS::StorageGateway::Volume	× No	✓ Sí	× 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	<a href="#">AWS::RoboMaker::Robot</a>	Tag Editor ya no lo admite.	2 de mayo de 2022
AWS RoboMaker	<a href="#">AWS::RoboMaker:: Fleet</a>	Tag Editor ya no lo admite.	2 de mayo de 2022
AWS RoboMaker	<a href="#">AWS::RoboMaker::DeploymentJob</a>	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 AWS recursos para que pueda dedicar menos tiempo a crear y administrar sus recursos e infraestructura. Crea una plantilla que describe todos los AWS recursos que desea (como los grupos de recursos) y AWS CloudFormation aprovisiona y configura esos recursos por usted.

Cuando la utilice AWS CloudFormation, podrá reutilizar la plantilla para configurar los grupos de recursos de forma coherente y repetida. Describa sus grupos de recursos una vez y, a continuación, aprovisiona los mismos grupos de recursos una y otra vez en varias Cuentas de AWS regiones.

## Resource Groups y AWS CloudFormation plantillas

Para suministrar y configurar recursos para Resource Groups y sus servicios relacionados, debe entender las [plantillas de AWS CloudFormation](#). Las plantillas son archivos de texto formateados en JSON oYAML. Estas plantillas describen los recursos que deseas aprovisionar en tus AWS CloudFormation pilas. Si no estás familiarizado con JSON ellasYAML, puedes usar AWS CloudFormation Designer para ayudarte a empezar con AWS CloudFormation las plantillas. Para obtener más información, consulta [¿Qué es AWS CloudFormation Designer?](#) en la Guía AWS CloudFormation del usuario.

Resource Groups permite crear grupos de recursos en AWS CloudFormation. Para obtener más información, incluidos ejemplos JSON y YAML plantillas de grupos de recursos, consulte la [referencia sobre los tipos de AWS Resource Groups recursos](#) en la Guía del AWS CloudFormation usuario.

## Obtenga más información sobre AWS CloudFormation

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

- [AWS CloudFormation](#)
- [AWS CloudFormation Guía del usuario](#)
- [AWS CloudFormation APIReferencia](#)
- [AWS CloudFormation Guía del usuario de la interfaz de línea de comandos](#)

# 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 datos en AWS Resource Groups](#)
- [Gestión de identidad y acceso para AWS Resource Groups](#)
- [Registro y supervisión en Resource Groups](#)
- [Validación de cumplimiento en Resource Groups](#)
- [Resiliencia en Resource Groups](#)
- [Seguridad de la infraestructura en Resource Groups](#)
- [Prácticas recomendadas de seguridad para Resource Groups](#)

# Protección de datos en AWS Resource Groups

La AWS modelo de [responsabilidad compartida modelo](#) de se aplica a la protección de datos en AWS Resource Groups. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido que está alojado en esta infraestructura. También es responsable de las tareas de configuración y administración de la seguridad del Servicios de AWS que utilices. Para obtener más información sobre la privacidad de los datos, consulte la sección [Privacidad de datos FAQ](#). Para obtener información sobre la protección de datos en Europa, consulte la [AWS Modelo de responsabilidad compartida y entrada de GDPR](#) blog sobre AWS Blog de seguridad.

Para fines de protección de datos, le recomendamos que proteja Cuenta de AWS credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactorial (MFA) con cada cuenta.
- Utilice SSL/TLS para comunicarse con AWS recursos. Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Configure API y registre la actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte [Trabajar con CloudTrail senderos](#) en la AWS CloudTrail Guía del usuario.
- Use AWS soluciones de cifrado, junto con todos los controles de seguridad predeterminados 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 entre FIPS 140 y 3 módulos criptográficos validados para acceder AWS a través de una interfaz de línea de comandos o API, utilice un FIPS punto final. Para obtener más información sobre los FIPS puntos finales disponibles, consulte la [Norma Federal de Procesamiento de Información \(FIPS\) 140-3](#).

Se recomienda encarecidamente no introducir nunca 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. Esto incluye cuando trabaja con Resource Groups u otros Servicios

de AWS mediante la consolaAPI, AWS CLI, o AWS SDKs. Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, le recomendamos encarecidamente que no incluya información sobre las credenciales URL para validar su solicitud a ese servidor.

## Cifrado de datos

En comparación con otros AWS servicios, AWS Resource Groups tiene una superficie de ataque mínima, ya que no proporciona una forma de cambiar, agregar o eliminar AWS recursos, excepto 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 AWS-aislamiento específico. Puede usar Resource Groups API y la consola en un VPC para maximizar la privacidad y la seguridad de la infraestructura.

## Cifrado en tránsito

AWS Resource Groups los datos se cifran en tránsito a la base de datos interna del servicio para su copia 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 AWS KMS keys.

## Privacidad del tráfico entre redes

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

# Gestión de identidad y acceso para AWS Resource Groups

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS recursos. IAM los administradores controlan quién puede autenticarse (iniciar sesión) y quién está autorizado (tiene permisos) para usar los recursos de Resource Groups. IAM es un Servicio de AWS que puede utilizar sin coste adicional.

## Temas

- [Público](#)
- [Autenticación con identidades](#)
- [Administración de acceso mediante políticas](#)
- [Cómo funciona Resource Groups con IAM](#)
- [Políticas administradas de AWS para AWS Resource Groups](#)
- [Uso de roles vinculados a servicios para Resource Groups](#)
- [Ejemplos de políticas basadas en identidad de AWS Resource Groups](#)
- [Solución de problemas AWS Resource Groups de identidad y acceso](#)

## Público

Cómo se usa AWS Identity and Access Management (IAM) varía según el trabajo que 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. A continuación, debe enviar solicitudes a su IAM administrador para cambiar los permisos de los usuarios del servicio. Revise la información de esta página para comprender los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM Resource Groups, consulte [Cómo funciona Resource Groups con IAM](#).

IAM administrador: si es IAM administrador, puede que desee obtener más información sobre cómo escribir políticas para administrar el acceso a Resource Groups. Para ver ejemplos de políticas basadas en la identidad de Resource Groups que puede utilizar IAM, consulte [Ejemplos de políticas basadas en identidad de AWS Resource Groups](#)

## Autenticación con identidades

La autenticación es la forma de iniciar sesión en AWS utilizando tus credenciales de identidad. Debe estar autenticado (iniciar sesión en AWS) como Usuario raíz de la cuenta de AWS, como IAM usuario o asumiendo un IAM rol.

Puede iniciar sesión en AWS como identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios de (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, el administrador configuró previamente la federación de identidades mediante roles. IAM Cuando accedes AWS al usar la federación, está asumiendo indirectamente un rol.

Según el tipo de usuario que sea, puede iniciar sesión en AWS Management Console o el AWS portal de acceso. Para obtener más información sobre cómo iniciar sesión en AWS, consulta [Cómo iniciar sesión en tu Cuenta de AWS](#) en la AWS Sign-In Guía del usuario.

Si accedes 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 usa AWS herramientas, debe firmar las solicitudes usted mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte [Firmar AWS APIsolicitudes](#) en la Guía IAM del usuario.

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

## Cuenta de AWS usuario raíz

Al crear un Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos los Servicios de AWS y los recursos de la cuenta. Esta identidad se denomina Cuenta de AWS usuario root y se accede a él iniciando sesión con la dirección de correo electrónico y la contraseña que utilizó 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 tareas que requieren que inicie sesión como usuario root, consulte [Tareas que requieren credenciales de usuario root](#) en la Guía del IAM usuario.

## Usuarios y grupos de IAM

Un [IAMusuario](#) es una identidad dentro de su Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos utilizar credenciales temporales en lugar de crear IAM usuarios con credenciales de larga duración, como contraseñas y claves de acceso. Sin embargo, si tiene casos de uso específicos que requieren credenciales a largo plazo con IAM los usuarios, le recomendamos que rote las claves de acceso. Para obtener más información, consulte [Rotar las claves de acceso con regularidad para los casos de uso que requieran credenciales de larga duración](#) en la Guía del IAM usuario.

Un [IAMgrupo](#) es una identidad que especifica un conjunto de IAM usuarios. 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 para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdmins y concederle permisos para administrar IAM los recursos.

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 de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte [Cuándo crear un IAM usuario \(en lugar de un rol\)](#) en la Guía del IAM usuario.

## IAMroles

Un [IAMrol](#) es una identidad dentro de tu Cuenta de AWS que tiene permisos específicos. Es similar a un IAM usuario, pero no está asociado a una persona específica. Puede asumir temporalmente un IAM rol en el AWS Management Console [cambiando de rol](#). Puede asumir un rol llamando a un AWS CLI o AWS API operación o mediante una operación personalizada URL. Para obtener más información sobre los métodos de uso de roles, consulte [Uso de IAM roles](#) en la Guía del IAM usuario.

IAMlos roles 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 sobre los roles para la federación, consulte [Creación de un rol para un proveedor de identidad externo](#) en la Guía del IAM usuario.

Si usa IAM Identity Center, configura un conjunto de permisos. Para controlar a qué pueden acceder sus identidades después de autenticarse, IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM. Para obtener información sobre los conjuntos de permisos, consulte los [conjuntos de permisos](#) en la AWS IAM Identity Center Guía del usuario.

- **Permisos de IAM usuario temporales:** un IAM usuario o rol puede asumir un IAM rol para asumir temporalmente diferentes permisos para una tarea específica.
- **Acceso multicuenta:** puedes usar un IAM rol para permitir que alguien (un responsable de confianza) de una cuenta diferente acceda a los recursos de tu cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunos Servicios de AWS, puede adjuntar una política directamente a un recurso (en lugar de utilizar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso multicuenta, consulta el tema sobre el acceso a los [recursos entre cuentas IAM en](#) la Guía del IAM usuario.
- **Acceso entre servicios:** algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realizas una llamada en un servicio, es habitual 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 IAM usuario o un rol para realizar acciones en AWS, se le considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del director que llama a un Servicio de AWS, combinado con la solicitud Servicio de AWS para realizar solicitudes a los servicios intermedios. FAS las solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completar. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre la política a la hora de realizar FAS solicitudes, consulte [Reenviar las sesiones de acceso](#).
- **Función de servicio:** una función de servicio es una [IAM función](#) que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentro de IAM. Para obtener más información, consulte [Crear un rol para delegar permisos a un Servicio de AWS](#) en la Guía del usuario de IAM.
- **Función vinculada a un 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 la función de realizar

una acción en su nombre. Los roles vinculados al servicio aparecen en su Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver, pero no editar, los permisos de las funciones vinculadas al servicio.

- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un IAM rol para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y se están creando AWS CLI o AWS APIsolicitudes. Esto es preferible a almacenar las claves de acceso en la EC2 instancia. Para asignar un AWS Un rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia que se adjunte a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulte [Uso de un IAM rol para conceder permisos a aplicaciones que se ejecutan en EC2 instancias de Amazon](#) en la Guía del IAM usuario.

Para saber si se deben usar IAM roles o IAM usuarios, consulte [Cuándo crear un IAM rol \(en lugar de un usuario\)](#) en la Guía del IAM usuario.

## Administración de acceso mediante políticas

Usted controla el acceso en AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto en 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 en AWS como JSON documentos. Para obtener más información sobre la estructura y el contenido de los documentos de JSON políticas, consulte [Descripción general de JSON las políticas](#) en la Guía del IAM usuario.

Los administradores pueden utilizar AWS JSONpolíticas 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. Para conceder a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

IAMlas políticas definen los 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 su función en AWS Management Console, el AWS CLI, o el AWS API.

## Políticas basadas en identidad

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, 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 información sobre cómo crear una política basada en la identidad, consulte [Creación de IAM políticas](#) en la Guía del usuario. 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 funciones de su Cuenta de AWS. Las políticas gestionadas incluyen AWS las políticas gestionadas y las políticas gestionadas por el cliente. Para saber cómo elegir entre una política gestionada o una política en línea, consulte [Elegir entre políticas gestionadas y políticas integradas en la Guía](#) del IAM usuario.

## Políticas basadas en recursos

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles 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 AWS políticas gestionadas desde una política basada IAM en recursos.

## Listas de control de acceso ( ) ACLs

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

Amazon S3, AWS WAF, y Amazon VPC son ejemplos de servicios que admiten ACLs. Para obtener más información ACLs, consulte la [descripción general de la 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 función avanzada en la que se establecen los permisos máximos que una política basada en la identidad puede conceder a una IAM entidad (IAMusuario o rol). 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 los [límites de los permisos para IAM las entidades](#) en la Guía del IAMusuario.
- **Políticas de control de servicios (SCPs):** SCPs son JSON políticas que especifican los permisos máximos para una organización o unidad organizativa (OU) en AWS Organizations. AWS Organizations es un servicio para agrupar y administrar de forma centralizada múltiples Cuentas de AWS que es propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar las políticas de control de servicios (SCPs) a cualquiera de tus cuentas o a todas ellas. SCPLimita los permisos de las entidades en las cuentas de los miembros, incluidas todas Usuario raíz de la cuenta de AWS. Para obtener más información acerca de OrganizationsSCPs, consulte [Políticas de control de servicios](#) en AWS Organizations Guía del usuario.
- **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 obtener más información, consulte [las políticas de sesión](#) en la Guía del IAM usuario.

## Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para obtener información sobre cómo AWS determina si se permite una solicitud cuando se trata de varios tipos de políticas, consulte la [lógica de evaluación de políticas](#) en la Guía del IAM usuario.

## Cómo funciona Resource Groups con IAM

Antes de administrar el acceso IAM a Resource Groups, debe comprender qué IAM funciones están disponibles para su uso con Resource Groups. Para obtener una visión general del funcionamiento de Resource Groups y otros AWS servicios IAM, consulte [AWS Services That Work with IAM](#) en la Guía del IAM usuario.

### Temas

- [Políticas basadas en identidad de Resource Groups](#)
- [Políticas basadas en recursos](#)
- [Autorización basada en etiquetas de Resource Groups](#)
- [IAM Funciones de Resource Groups](#)

### Políticas basadas en identidad de Resource Groups

Con las políticas IAM basadas en la identidad, puede especificar las acciones y los 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 más información sobre todos los elementos que se utilizan en una JSON política, consulte la [Referencia sobre los elementos IAM JSON de la política](#) en la Guía del IAM usuario.

### Acciones

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

El `Action` elemento de una JSON política describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de política suelen tener el mismo nombre que la AWS API operación asociada. Hay algunas excepciones, como las acciones que solo permiten permisos y que no tienen una operación coincidente. API 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 permiso a alguien para crear un grupo Resource Groups con la `CreateGroup` API operación Resource Groups, debe incluir la `resource-groups:CreateGroup` acción 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 las acciones de Resource Groups, consulte [Actions, Resources and Condition Keys for AWS Resource Groups](#) en la Guía del IAM usuario.

## Recursos

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

El elemento `Resource` JSON de política especifica el objeto o los objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso mediante su [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 grupo tiene ARN el siguiente formato:

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

Para obtener más información sobre el formato de ARNs, consulte [Amazon Resource Names \(ARNs\) y AWS Service Namespaces](#).

Por ejemplo, para especificar el grupo `my-test-group` de recursos en su declaración, utilice lo 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 API acciones de Resource Groups pueden incluir 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 sola sentencia, sepárelos ARNs con comas.

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

Para ver una lista de los tipos de recursos de Resource Groups y sus correspondientes acciones ARNs, y saber con qué acciones puede especificar cada recurso, consulte [Acciones, recursos y claves de condición AWS Resource Groups](#) en la Guía del IAM usuario. ARN

## Claves de condición

Los administradores pueden usar AWS JSON políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en 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 mediante una OR operación lógica. 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 a un IAM usuario permiso para acceder a un recurso solo si está etiquetado con su nombre de IAM usuario. Para obtener más información, consulte [los elementos IAM de la política: variables y etiquetas](#) en la Guía del IAM usuario.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de [contexto de condición AWS globales](#) en la Guía del IAM usuario.

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 AWS globales, consulte las [claves de contexto de condición AWS globales](#) en la Guía del IAM usuario.

Para ver una lista de las claves de condición de Resource Groups y saber con qué acciones y recursos puede utilizar una clave de condición, consulte [Acciones, recursos y claves de condición AWS Resource Groups](#) en la Guía del IAM usuario.

## 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](#).

## IAM Funciones de Resource Groups

Un [IAMrol](#) es una entidad de su AWS cuenta que tiene permisos específicos. Resource Groups no tiene ni utiliza roles de servicio.

### Uso de credenciales temporales con Resource Groups

En Resource Groups, puede usar credenciales temporales para iniciar sesión con la federación, asumir un IAM rol o asumir un rol multicuenta. Para obtener credenciales de seguridad temporales, puede llamar a AWS STS API operaciones como [AssumeRole](#) o [GetFederationToken](#).

### Roles vinculados al servicio

Las [funciones vinculadas al servicio](#) permiten a AWS los servicios acceder 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 una 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, suscríbese a la fuente RSS en la página de [historial de documentos de Resource Groups](#).

Cambio	Descripción	Fecha
Actualización de política: <a href="#">ResourceGroupsandTagEditorFullAccess</a>	Resource Groups actualizó una política para incluir permisos de AWS CloudFormation adicionales.	10 de agosto de 2023

Cambio	Descripción	Fecha
Actualización de política: <a href="#">ResourceGroupsandTagEditorReadOnlyAccess</a>	Resource Groups actualizó una política para incluir permisos de AWS CloudFormation adicionales.	10 de agosto de 2023
Nueva política: <a href="#">ResourceGroupsServiceRolePolicy</a>	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 las 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](#)
- [Uso de la consola y la API de Resource Groups](#)
- [Permitir a los usuarios consultar sus propios permisos](#)
- [Visualización de grupos basados en etiquetas](#)

## 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 de uso AWS Resource Groups y Tag Editor](#) 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:ListGroupsWithUser",
        "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:ListGroup",
      "Resource": "arn:aws:resource-groups::region:account_ID:group/group_name"
    },
    {
      "Effect": "Allow",
      "Action": "resource-groups:ListGroup",
      "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:ListGroup`s.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
perform: resource-groups:ListGroup 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:ListGroup`s.

### 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.

Algunos 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-8081-7zz0386fbc6",  
"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.
- [Diseñando una arquitectura basada en la HIPAA seguridad y el cumplimiento en Amazon Web Services](#): en este documento técnico se describe cómo pueden utilizar las empresas AWS para crear HIPAA aplicaciones aptas.

### Note

No todos son aptos. Servicios de AWS HIPAA Para obtener más información, consulta la [Referencia de servicios HIPAA aptos](#).

- [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. En las guías se resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y se orientan a 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](#)— Este 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, por ejemplo PCIDSS, cumpliendo 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 consumo 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 AWS específico. Puede usar Resource Groups API y la consola en un VPC para maximizar la privacidad y la seguridad de la infraestructura.

Como servicio gestionado, AWS Resource Groups está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se protege la infraestructura, consulte [Seguridad AWS en la nube](#). Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte [Protección de infraestructuras en un marco](#) de buena AWS arquitectura basado en el pilar de la seguridad.

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

- Seguridad de la capa de transporte (TLS). Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Cifre suites con perfecto secreto (PFS), como (Ephemeral Diffie-Hellman) o DHE 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 firmarse con un identificador de clave de acceso y una clave de acceso secreta que esté asociada a un director. 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 [AWS Servicios 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 las cuotas dentro de AWS Resource Groups (Resource Groups). Para ajustar la cuota, puedes solicitar un aumento en la [consola de Service Quotas](#).

Nombre	Valor predeterminado	Ajuste	Descripción
Grupos de recursos por cada cuenta	Cada región admitida: 100	<a href="#">Sí</a>	Número máximo de grupos de recursos que puede crear en esta cuenta. Un grupo de recursos es un conjunto de AWS recursos que cumplen un criterio específico.

# AWS Resource Groups historial de documentos

Cambio	Descripción	Fecha
<a href="#">Contenido actualizado</a>	Se han actualizado los títulos de los temas y se ha reorganizado el contenido para mejorar la legibilidad y la visibilidad.	1 de agosto de 2024
<a href="#">Compatibilidad con más tipos de recursos</a>	Resource Groups y Tag Editor ahora admiten más tipos de recursos.	30 de mayo de 2024
<a href="#">Políticas AWS gestionadas actualizadas y ResourceGroupsandTagEditorFullAccessResourceGroupsandTagEditorReadOnlyAccess</a>	Resource Groups actualizó dos políticas AWS administradas para añadir AWS CloudFormation permisos adicionales.	10 de agosto de 2023
<a href="#">Cuotas de servicio de Resource Groups</a>	Ahora puede ver los límites de cuota de Resource Groups mediante Service Quotas.	29 de junio de 2023
<a href="#">IAMactualización de las mejores prácticas</a>	Guía actualizada para alinearla con las IAM mejores prácticas. Para obtener más información, consulte <a href="#">las mejores prácticas de seguridad en IAM</a> .	3 de enero de 2023
<a href="#">La información de Tag Editor se ha trasladado a su propia guía</a>	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
<a href="#">Los grupos de recursos ahora pueden incluir recursos de</a>	AWS Resource Groups ahora admite la inclusión de recursos	20 de octubre de 2022

<a href="#"><u>Amazon Keyspaces (para Apache Cassandra)</u></a>	para Amazon Keyspaces (para Apache Cassandra) en un grupo de recursos.	
<a href="#"><u>Discontinuidad de los tipos de recursos</u></a>	Tag Editor ya no admite los siguientes tipos de recursos: AWS::RoboMaker::Robot , AWS::RoboMaker:: Fleet yAWS::RoboMaker::DeploymentJob .	17 de mayo de 2022
<a href="#"><u>Nueva política AWS gestionada - ResourceGroupsServiceRolePolicy</u></a>	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
<a href="#"><u>Eventos del ciclo de vida de un grupo</u></a>	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
<a href="#"><u>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 AWS recursos.</u></a>	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

<a href="#">Se agregó soporte para los recursos de AWS Resilience Hub</a>	AWS Resource Groups ahora admite la inclusión de recursos para AWS Resilience Hub en un grupo de recursos.	18 de noviembre de 2021
<a href="#">Se añadió soporte para los recursos de Amazon Pinpoint</a>	AWS Resource Groups ahora admite la inclusión de recursos para Amazon Pinpoint en un grupo de recursos.	11 de noviembre de 2021
<a href="#">Se agregó soporte para grupos de recursos configurados y administrados por AppRegistry</a>	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 AWS Service Catalog AppRegistry. Para obtener más información, consulte <a href="#">Configuraciones de servicio</a> en la AWS Resource Groups APIreferencia.	15 de septiembre de 2021
<a href="#">Se agregó soporte para los recursos de Amazon OpenSearch Service</a>	AWS Resource Groups ahora permite incluir recursos para Amazon OpenSearch Service en un grupo de recursos.	11 de agosto de 2021
<a href="#">Se agregó soporte para los recursos de AWS Braket</a>	AWS Resource Groups ahora permite incluir recursos para AWS Braket en un grupo de recursos.	30 de junio de 2021
<a href="#">Se agregó soporte para los recursos de Amazon EMR Containers</a>	AWS Resource Groups ahora admite la inclusión de recursos para EMR contenedores de Amazon en un grupo de recursos.	27 de abril de 2021

[Se agregó soporte para recursos de AWS servicios adicionales](#)

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 la función, puede crear un grupo de recursos que contenga las reservas de EC2 capacidad de Amazon y, a continuación, lanzar EC2 instancias de Amazon 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, consulta [Cómo trabajar con grupos de reservas de capacidad](#) en la Guía del EC2 usuario de Amazon.

29 de julio de 2020

[Se ha añadido soporte para AWS IoT Greengrass los 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: Detalles, 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

---

<a href="#">Compruebe el cumplimiento con políticas de etiquetas</a>	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 organización.	26 de noviembre de 2019
<a href="#">Compatibilidad con más tipos de recursos</a>	El editor de etiquetas ahora admite más tipos de AWS Resource Groups recursos.	4 de octubre de 2019
<a href="#">Los nuevos tipos de recursos son compatibles con AWS Resource Groups</a>	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
<a href="#">Los nuevos tipos de recursos son compatibles con AWS Resource Groups</a>	Los eventos de Amazon API Gateway REST APIs, CloudWatch los eventos de Amazon Events y SNS los temas de Amazon ahora son tipos de recursos compatibles en AWS Resource Groups.	27 de junio de 2019
<a href="#">Tag Editor ahora permite buscar recursos sin etiquetas</a>	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

[El editor de etiquetas admite nuevos tipos de recursos AWS Resource Groups](#)

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 Editor ya no están disponibles](#)

Se han eliminado las menciones a las herramientas Resource Groups y Tag Editor anteriores, clásicas o heredadas. Estas herramientas 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 permite exportar los resultados de las consultas a un CSV](#)

Puede exportar los resultados de una consulta de la página Buscar recursos para etiquetar a un archivo CSV con formato. 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 resultados 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 resultados.

26 de febrero de 2019

<a href="#">Documentation añadida para el nuevo Tag Editor</a>	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
<a href="#">Nuevos tipos de recursos admitidos para grupos en Resource Groups</a>	Se han añadido nuevos tipos de recursos que se admiten ahora en Resource Groups.	4 de febrero de 2019
<a href="#">Experiencia de usuario mejorada a la hora de añadir etiquetas a consultas de Resource Groups basadas en etiquetas</a>	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
<a href="#">AWS CloudFormation Se agregó soporte para consultas basadas en pilas a Resource Groups</a>	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
<a href="#">Resource Groups y CloudTrail</a>	Resource Groups ahora ofrece AWS CloudTrail soporte. Puede ver y trabajar con los registros de todas las API llamadas de Resource Groups CloudTrail.	29 de junio de 2018

- API versión: 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

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