



Guía del administrador

# AWS Service Catalog



# AWS Service Catalog: Guía del administrador

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 es Service Catalog? .....	1
Vídeo: introducción a AWS Service Catalog .....	2
Información general .....	2
Usuarios .....	2
Productos .....	3
HashiCorp Soporte para Terraform Open Source y Terraform Cloud .....	3
Productos aprovisionados .....	3
Carteras .....	4
Control de versiones .....	4
Permisos .....	4
Restricciones .....	5
Flujo de trabajo inicial del administrador .....	5
Flujo de trabajo inicial del usuario final .....	6
Cuotas .....	6
AWS Organizations .....	6
Cuotas de restricciones .....	6
Cuotas de cartera .....	6
Cuotas de productos .....	7
Cuotas de productos aaprovisionados .....	7
Cuotas regionales .....	7
Cuotas de acciones del servicio .....	7
TagOptions cuotas .....	7
Configuración .....	8
.....	8
Inscríbese en una Cuenta de AWS .....	8
Creación de un usuario con acceso administrativo .....	8
Concesión de permisos a los administradores .....	10
Concesión de permisos a los usuarios finales .....	13
Instalar y configurar el motor de aprovisionamiento Terraform .....	14
Determinación de cola .....	14
Agregar Confused Deputy a su motor de aprovisionamiento Terraform .....	15
Introducción .....	19
Biblioteca de introducción .....	19
Requisitos previos .....	20

Más información .....	20
Introducción a un producto de AWS CloudFormation .....	20
Paso 1: Descargar la plantilla .....	21
Paso 2: Crear un par de claves .....	25
Paso 3: Crear una cartera .....	26
Paso 4: Crear un nuevo producto en la cartera .....	27
Paso 5: agregar una restricción de plantilla .....	28
Paso 6: Agregar una restricción de lanzamiento .....	29
Paso 7: Conceder acceso a la cartera a los usuarios finales .....	32
Paso 4: Probar la experiencia del usuario final .....	32
Introducción a un producto Terraform .....	34
Actualizar a un tipo de producto externo .....	36
Requisito previo: Configurar su motor de aprovisionamiento Terraform .....	36
Paso16: Descargar el archivo de configuración Terraform .....	38
Paso 2: Crear un producto de Terraform .....	39
Paso 3: Crear una cartera .....	40
Paso 4: Añadir el producto a la cartera .....	41
Paso 5: Crear roles de lanzamiento .....	41
Paso 6: Agregar una restricción de lanzamiento .....	46
Paso 7: Conceder acceso al usuario final .....	47
Paso 8: Compartir la cartera con el usuario final .....	47
Paso 4: Probar la experiencia del usuario final .....	48
Paso 10: Monitorización de las operaciones de aprovisionamiento de Terraform .....	49
Seguridad .....	51
Protección de los datos .....	52
Protección de los datos con el cifrado .....	53
Identity and Access Management .....	53
Público .....	54
Ejemplos de políticas basadas en la identidad para AWS Service Catalog .....	54
AWS políticas gestionadas .....	60
Uso de roles vinculados a servicios .....	70
Solución de problemas AWS Service Catalog de identidad y acceso .....	75
Control de acceso .....	77
Registro y supervisión .....	78
Validación de la conformidad .....	78
Resiliencia .....	79

Seguridad de infraestructuras .....	80
Prácticas recomendadas de seguridad .....	80
Administración de catálogos .....	82
Administración de carteras .....	82
Creación, visualización y eliminación de carteras .....	83
Ver los detalles de la cartera .....	83
Crear y eliminar carteras .....	83
Adición de productos .....	84
Adición de restricciones .....	87
Conceder acceso a los usuarios .....	88
Uso compartido de carteras .....	89
Compartir e importar carteras .....	97
Administración de productos .....	101
Ver la página de productos .....	102
Creación de productos .....	102
Adición de productos a las carteras .....	106
Actualización de productos .....	106
Sincronizar productos con archivos de plantillas de repositorios externos .....	108
Eliminación de productos .....	116
Administración de versiones .....	125
Uso de las restricciones .....	126
Restricciones de lanzamiento .....	127
Restricciones de notificación .....	132
Restricciones de actualización de etiquetas .....	133
Restricciones de conjunto de pilas .....	134
Restricciones de plantilla .....	135
Uso de acciones de servicio .....	140
Requisitos previos .....	140
Paso 1: Configurar los permisos de usuario final .....	141
Paso 2: Crear una acción de servicio .....	142
Paso 3: Asociar la acción de servicio con una versión de producto .....	143
Paso 4: Probar la experiencia del usuario final .....	143
Paso 5: Administrar las acciones de servicio con AWS CloudFormation .....	144
Paso 6: Solución de problemas .....	144
Adición de productos de AWS Marketplace a la cartera .....	146
Administración de productos de AWS Marketplace mediante AWS Service Catalog .....	147

Administración y adición manual de productos de AWS Marketplace .....	147
Usando AWS CloudFormation StackSets .....	152
Diferencias entre conjuntos de pilas e instancias de pila .....	153
Restricciones de conjunto de pilas .....	153
Administración de presupuestos .....	153
Requisitos previos .....	154
Crear un presupuesto .....	156
Asociación de un presupuesto .....	157
Visualización de un presupuesto .....	157
Desasociación de un presupuesto .....	158
Administración de productos aprovisionados .....	159
Administración de todos los productos aprovisionados como administrador .....	159
Cambio del propietario del producto aprovisionado .....	160
Véase también .....	161
Actualizar plantillas para productos aprovisionados .....	161
Tutorial: Identificación de la asignación de recursos del usuario .....	162
Gestión de los errores de estado del producto Terraform Open Source .....	166
Ejemplos de errores de estado .....	166
Administrar el archivo de estado del producto de Terraform Open Source .....	168
Administración de etiquetas .....	169
AutoTags .....	169
TagOption Biblioteca .....	170
Lanzamiento de un producto con TagOptions .....	172
Gestionando TagOptions .....	175
Uso TagOptions con políticas AWS Organizations de etiquetas .....	177
Motores externos .....	182
Consideraciones .....	183
Análisis de parámetros .....	183
Aprovisionando .....	187
Actualización .....	190
Terminando .....	193
Etiquetado .....	195
Supervisión .....	197
Herramientas de monitorización .....	197
Herramientas automatizadas .....	198
CloudWatch Métricas .....	198

---

Habilitar CloudWatch las métricas .....	198
Métricas y dimensiones disponibles .....	199
Visualización de las métricas de AWS Service Catalog .....	200
CloudTrail registros .....	200
AWS Service Catalog información en CloudTrail .....	201
Descripción de las entradas de los archivos de registro de AWS Service Catalog .....	202
Marca de la consola .....	204
Compatibilidad de Región de AWS con la marca de la consola .....	205
Historial de documentos .....	207
Actualizaciones anteriores .....	208
.....	ccxiv

# ¿Qué es Service Catalog?

Service Catalog permite a las organizaciones crear y administrar catálogos de servicios de TI aprobados para su uso en AWS. Estos servicios de TI pueden incluir desde imágenes de máquinas virtuales, servidores, software, bases de datos y más para completar las arquitecturas de aplicaciones multinivel.

Service Catalog permite a las organizaciones administrar de forma centralizada los servicios de TI que se implementan con más frecuencia, y ayuda a las organizaciones a conseguir una gobernanza uniforme y a cumplir los requisitos de conformidad. Los usuarios finales pueden implementar rápidamente solo los servicios de TI aprobados que necesitan, de acuerdo con las limitaciones establecidas por su organización.

Service Catalog proporciona los siguientes beneficios:

- Normalización

Permite administrar los recursos aprobados restringiendo dónde se puede lanzar el producto, el tipo de instancia que se puede utilizar y muchas otras opciones de configuración. El resultado es un entorno estandarizado de provisionamiento de productos en toda la organización.

- Detección y lanzamiento en autoservicio

Los usuarios examinan los listados de productos (servicios o aplicaciones) a los que tienen acceso para localizar el producto que deseen utilizar y lanzarlo por su cuenta como producto provisionado.

- Control de acceso detallado

Los administradores reúnen carteras de productos del catálogo, agregan restricciones y etiquetas de recursos para su uso durante el provisionamiento y, a continuación, conceden acceso a la cartera mediante AWS Identity and Access Management usuarios y grupos de IAM .

- Extensibilidad y control de versiones

Los administradores pueden agregar un producto a cualquier cantidad de carteras y restringirlo sin necesidad de crear otra copia. Cuando se actualiza el producto a una nueva versión, la actualización se propaga a todos los productos de todas las carteras en las que se hace referencia a él.

Para obtener más información , [consulte la página de detalles del producto de](#) .

El API de Service Catalog proporciona control mediante programación de todas las acciones del usuario final como alternativa al uso de la AWS Management Console. Para obtener más información, consulte la [Guía del desarrollador de Amazon SES](#).

## Vídeo: introducción a AWS Service Catalog

En este vídeo (7:27) se describe cómo crear, organizar y gestionar un catálogo seleccionado de productos de AWS y cómo compartir productos con un nivel de permisos. Como resultado, los usuarios finales pueden aprovisionar rápidamente los recursos de TI aprobados sin acceso directo a los servicios de AWS subyacentes.

[Introducción a AWS Service Catalog](#)

## Información general de Service Catalog

Para comenzar a trabajar con Service Catalog, debe comprender sus componentes y los flujos de trabajo iniciales para los administradores y los usuarios finales.

## Usuarios

Service Catalog admite los siguientes tipos de usuarios:

- **Administradores de catálogos (administradores):** se encargan de administrar un catálogo de productos (aplicaciones y servicios), organizarlos en carteras y conceder acceso a los usuarios finales. Los administradores de catálogos preparan las plantillas de AWS CloudFormation, configuran las restricciones y administran las funciones de IAM de los productos para proporcionar una administración avanzada de los recursos.
- **Usuarios finales:** reciben las AWS credenciales del departamento o el administrador de TI y utilizan la AWS Management Console para lanzar los productos cuyo acceso se les ha concedido. A los usuarios finales (a quienes también se denominan simplemente usuarios) se les pueden conceder diferentes permisos en función de sus necesidades operativas. Por ejemplo, un usuario puede tener el máximo nivel de permisos (para lanzar y administrar todos los recursos que requieren los productos que utilizan), o bien permiso para utilizar tan solo determinadas características del servicio.

## Productos

Un producto es un servicio de TI que se desea que esté disponible para implementarlo en AWS. Un producto consta de uno o más recursos de AWS como, por ejemplo, instancias EC2, volúmenes de almacenamiento, bases de datos, configuraciones de monitorización y componentes de redes, o bien productos AWS Marketplace empaquetados. Un producto puede ser una instancia de computación sencilla con AWS Linux, una aplicación web de distintos niveles completamente equipada que se ejecuta en su propio entorno, o algo intermedio.

Crea un producto importando una AWS CloudFormation plantilla. Las AWS CloudFormation plantillas definen los AWS recursos que el producto necesita para funcionar, las relaciones entre los recursos y los parámetros que los usuarios finales puede introducir al lanzar el producto para configurar los grupos de seguridad, crear pares de claves y realizar otras personalizaciones.

## HashiCorp Soporte para Terraform Open Source y Terraform Cloud

AWS Service Catalog permite un aprovisionamiento rápido y de autoservicio con control integrado para sus configuraciones de Terraform Open Source y HashiCorp Terraform Cloud. AWS Puede usar Service Catalog como una herramienta única para organizar, gobernar y distribuir sus configuraciones de Terraform según las necesidades de AWS. Puede acceder a las características clave de Service Catalog, incluyendo la catalogación de plantillas de Terraform estandarizadas y preaprobadas, el control de acceso, el aprovisionamiento con privilegios mínimos, el control de versiones, el etiquetado y el uso compartido en miles de cuentas de AWS. Sus usuarios finales ven una lista sencilla de los productos y las versiones a los que tienen acceso y, a continuación, pueden implementar esos productos en una sola acción.

Para obtener más información y completar un tutorial sobre los productos de Terraform, consulte [Introducción a un producto Terraform](#).

## Productos aprovisionados

Las pilas e AWS CloudFormation facilitan la administración del ciclo de vida del producto porque le permiten provisionar, etiquetar, actualizar y terminar la instancia de su producto como una sola unidad. Una pila de AWS CloudFormation incluye una plantilla de AWS CloudFormation, escrita en formato JSON o YAML, así como su colección de recursos asociados. Un producto aprovisionado es una pila. Cuando un usuario final lanza un producto, la instancia del producto que se ha aprovisionado mediante es una pila con los recursos necesarios para ejecutar el producto. Si quiere obtener más información, consulte la [Guía del usuario de AWS CloudFormation](#).

## Carteras

Una cartera es una colección de productos junto con la información de configuración. Las carteras ayudan a administrar quién puede hacer uso de los productos y de qué manera. Con Service Catalog, puede crear una cartera de productos personalizada para cada tipo de usuario de su organización y conceder acceso de manera selectiva a la cartera de productos apropiada para cada uno de ellos. Cuando se agrega una nueva versión de un producto a una cartera, esta versión pasa automáticamente a estar disponible para todos los usuarios actuales.

También puede compartir las carteras con otras AWS cuentas de AWS y permitir a los administradores de estas cuentas distribuir las carteras con restricciones adicionales (por ejemplo, limitar qué instancias EC2 puede crear un usuario). Mediante las carteras, los permisos, el uso compartido y las restricciones, puede asegurarse de que los usuarios lancen productos que estén configurados correctamente según las necesidades y los estándares de la organización.

## Control de versiones

Service Catalog permite administrar varias versiones de los productos del catálogo. Este enfoque le permite añadir nuevas versiones de plantillas y recursos asociados en función de las actualizaciones de software o los cambios en la configuración.

Al crear una nueva versión de un producto, la actualización se distribuye automáticamente a todos los usuarios que tienen acceso al producto y les permite seleccionar la versión del producto que desean usar. Los usuarios pueden actualizar de manera rápida y sencilla las instancias en ejecución del producto a la nueva versión.

## Permisos

Cuando se concede a un usuario acceso a una cartera de productos, se le permite explorarla y lanzar los productos que contiene. Los permisos de IAM AWS Identity and Access Management se aplican para controlar quiénes pueden ver y modificar el catálogo. Es posible asignar permisos de IAM a usuarios, grupos y roles de IAM.

Cuando un usuario lanza un producto con una función de IAM asignado, utiliza dicha función para lanzar los recursos en la nube del producto mediante AWS CloudFormation . Asignar un rol de IAM a cada producto ayuda a evitar que se concedan permisos a los usuarios para que realicen operaciones sin aprobar; además, permite a estos últimos provisionar recursos mediante el catálogo.

# Restricciones

Las restricciones controlan cómo se pueden implementar los recursos de AWS específicos para un producto. Puede usarlas para aplicar límites a los productos para el control de costos o de dirección. Existen diferentes tipos de restricciones de AWS Service Catalog: las restricciones de lanzamiento, las restricciones de notificación y las restricciones de plantilla.

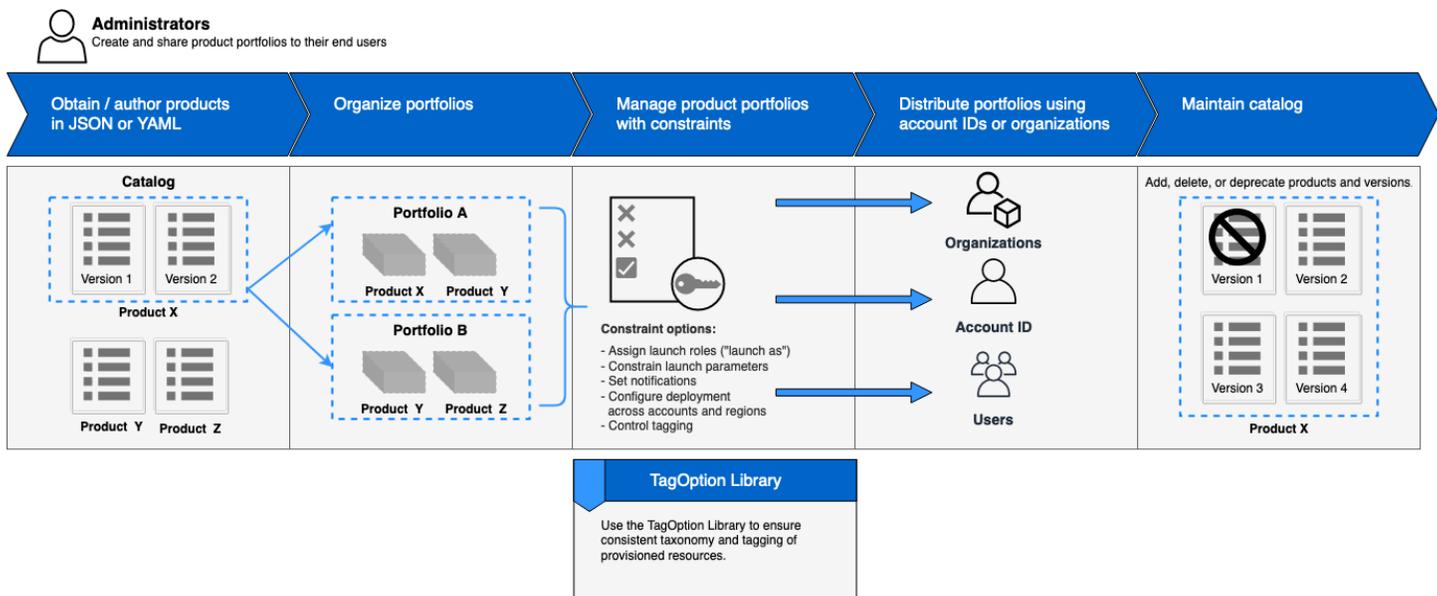
Las restricciones de lanzamiento permiten especificar una función de un producto en una cartera. Utilice este rol para provisionar los recursos durante el lanzamiento, de modo que pueda restringir los permisos del usuario sin que esto afecte a la capacidad de los usuarios de provisionar productos del catálogo.

Las restricciones de notificación permiten obtener notificaciones sobre los eventos de la pila mediante un tema de Amazon SNS.

Las restricciones de plantilla restringen los parámetros de configuración que hay disponibles para el usuario al lanzar el producto (por ejemplo, los tipos de instancia EC2 o los intervalos de direcciones IP). Las restricciones de plantilla permiten reutilizar las plantillas de AWS CloudFormation genéricas para productos, así como aplicar restricciones a las plantillas por producto o por cartera.

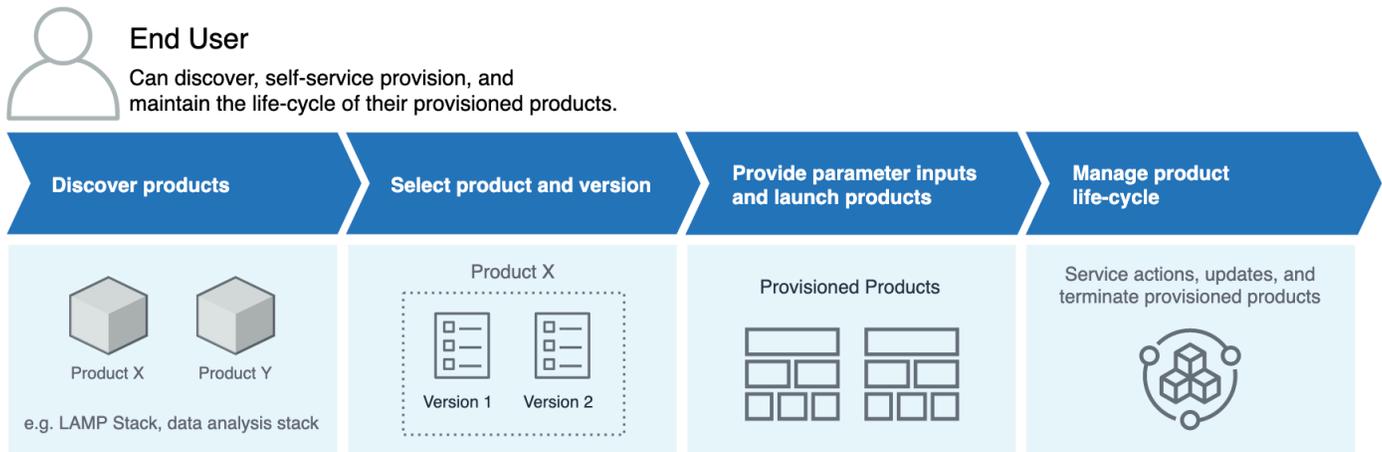
## Flujo de trabajo inicial del administrador

Este diagrama se muestra el flujo de trabajo inicial de un administrador para la creación de un catálogo.



## Flujo de trabajo inicial del usuario final

Este diagrama muestra el flujo de trabajo inicial de un usuario final.



## Cuotas de servicio predeterminadas de AWS Service Catalog

Su AWS cuenta tiene las siguientes cuotas predeterminadas para: restricción AWS Organizations, cartera, producto, producto aprovisionado, región, acción de servicio y. TagOptions

Puede utilizar Service Quotas para administrar sus cuotas o solicitar un aumento de las cuotas. Para obtener más información sobre Service Quotas, consulte [¿Qué son las cuotas de servicio?](#) en la Service Quotas Guía del usuario. Para solicitar un aumento de la cuota, consulte [Solicitar un aumento de cuota](#).

### AWS Organizations

- Administradores delegados de AWS Service Catalog por organización: 50

### Cuotas de restricciones

- Restricciones por producto y cartera: 100

### Cuotas de cartera

- Usuarios, grupos y roles por cartera: 100
- Productos por cartera: 150

- Etiquetas por cartera: 20
- Cuentas compartidas por cartera: 5000
- Valores de etiqueta por clave de etiqueta: 25

## Cuotas de productos

- Usuarios, grupos y roles por producto: 200
- Versiones de producto por producto: 100
- Etiquetas por producto: 20
- Valores de etiqueta por clave de etiqueta: 25

## Cuotas de productos aprovisionados

- Etiquetas por producto aprovisionado: 50

## Cuotas regionales

- Carteras: 100
- Productos: 350

## Cuotas de acciones del servicio

- Acciones del servicio por región: 200
- Asociaciones de acciones del servicio por versión del producto: 25

## TagOptions cuotas

- TagOptions por recurso: 25
- Valores por TagOption: 25

# Configuración AWS Service Catalog

Antes de empezar AWS Service Catalog, complete las siguientes tareas.

Temas

- [Inscríbase en una Cuenta de AWS](#)
- [Creación de un usuario con acceso administrativo](#)

## Inscríbase en una Cuenta de AWS

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

Para suscribirte a una Cuenta de AWS

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

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

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

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en <https://aws.amazon.com/> y seleccionando Mi cuenta.

## Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

## Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión [AWS Management Console](#) como propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

Para obtener ayuda para iniciar sesión con el usuario raíz, consulte [Signing in as the root user](#) en la Guía del usuario de AWS Sign-In .

2. Active la autenticación multifactor (MFA) para el usuario raíz.

Para obtener instrucciones, consulte [Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz \(consola\)](#) en la Guía del usuario de IAM.

## Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

Consulte las instrucciones en [Activar AWS IAM Identity Center](#) en la Guía del usuario de AWS IAM Identity Center .

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte [Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la](#) Guía del AWS IAM Identity Center usuario.

## Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte [Iniciar sesión en el portal de AWS acceso](#) en la Guía del AWS Sign-In usuario.

## Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

Para conocer las instrucciones, consulte [Create a permission set](#) en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

Para conocer las instrucciones, consulte [Add groups](#) en la Guía del usuario de AWS IAM Identity Center .

Para dar acceso, agregue permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

Cree un conjunto de permisos. Siga las instrucciones de [Creación de un conjunto de permisos](#) en la Guía del usuario de AWS IAM Identity Center .

- Usuarios administrados en IAM a través de un proveedor de identidades:

Cree un rol para la federación de identidades. Siga las instrucciones descritas en [Creación de un rol para un proveedor de identidad de terceros \(federación\)](#) en la Guía del usuario de IAM.

- Usuarios de IAM:

- Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en [Creación de un rol para un usuario de IAM](#) en la Guía del usuario de IAM.

- (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en [Adición de permisos a un usuario \(consola\)](#) de la Guía del usuario de IAM.

## Concesión de permisos a los administradores de AWS Service Catalog

El administrador de catálogos necesita acceso a la vista de la consola del administrador de AWS Service Catalog y permisos de IAM que le permitan realizar tareas como las siguientes:

- Crear y administrar carteras
- Crear y administrar productos
- Agregar restricciones de plantilla para controlar las opciones que los usuarios finales tienen a su disposición cuando lanzan productos

- Agregar restricciones de lanzamiento para definir las funciones de IAM que AWS Service Catalog asume cuando los usuarios finales lanzan productos
- Conceder a los usuarios finales acceso a los productos

Usted, o un administrador que administre los permisos de IAM, debe adjuntar al usuario, grupo o rol de IAM las políticas necesarias para llevar a cabo este tutorial.

Para conceder permisos a un administrador de catálogos

1. Abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación, amplíe Administración de acceso y, a continuación, seleccione Usuarios. Si ya ha creado un usuario de IAM que desea utilizar como administrador de catálogos, elija el nombre del usuario y seleccione Añadir permisos. De lo contrario, cree un usuario de la siguiente manera:
  - a. Elija Añadir usuario.
  - b. En User name, escriba **ServiceCatalogAdmin**.
  - c. Seleccione Programmatic access y AWS Management Console access.
  - d. Elija Siguiente: permisos.
3. Elija Adjuntar directamente políticas existentes.
4. Elija Create policy y haga lo siguiente:
  - a. Seleccione la pestaña JSON.
  - b. Copie el siguiente ejemplo de política y péguelo en Documento de política:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateKeyPair",
        "iam:AddRoleToInstanceProfile",
        "iam:AddUserToGroup",
        "iam:AttachGroupPolicy",
        "iam:CreateAccessKey",
        "iam:CreateGroup",
        "iam:CreateInstanceProfile",
```

```

        "iam:CreateLoginProfile",
        "iam:CreateRole",
        "iam:CreateUser",
        "iam:Get*",
        "iam:List*",
        "iam:PutRolePolicy",
        "iam:UpdateAssumeRolePolicy"
    ],
    "Resource": [
        "*"
    ]
}
]
}

```

- c. Elija Siguiente: etiquetas.
- d. (Opcional) Seleccione Añadir etiqueta para asociar un par clave-valor al recurso. Puede agregar un máximo de 50 etiquetas.

#### Note

Las etiquetas son pares clave-valor que puede añadir a los recursos. Esto ayuda a identificar, organizar y buscar recursos. Para obtener más información, consulte [Etiquetado de los AWS recursos](#) en la Referencia general de AWS Guía de referencia general.

- e. Elija Siguiente: Revisar.
- f. En Policy Name, escriba **ServiceCatalogAdmin-AdditionalPermissions**.

#### Important

Debe conceder a los administradores permisos de Amazon S3 para acceder a las plantillas que AWS Service Catalog almacena en Amazon S3. Para obtener más información, consulte [Ejemplo de políticas de usuario](#) en la Guía del usuario de Amazon Simple Storage Service.

- g. Seleccione Crear política.
5. Volver a la ventana del navegador donde está abierta la página de permisos y elija Refresh.
6. En el campo de búsqueda, escriba **ServiceCatalog** para filtrar la lista de políticas.

7. Seleccione la casilla que se encuentra junto a **AWSServiceCatalogAdminFullAccess** la política **ServiceCatalogAdmin-AdditionalPermissions** y después elija Siguiendo: Revisar.
8. Si va a actualizar a un usuario, elija Add permissions.  
  
Si va a crear un usuario, seleccione Create user. Puede descargar o copiar las credenciales. A continuación, elija Close.
9. Para iniciar sesión como administrador de catálogos, utilice la dirección URL específica de la cuenta. Para encontrar esta URL, elija Dashboard en el panel de navegación y seleccione Copy Link. Pegue el enlace en el navegador y utilizar el nombre y la contraseña del usuario de IAM que ha creado o actualizado en este procedimiento.

## Concesión de permisos a los usuarios finales de AWS Service Catalog

Para que el usuario final pueda utilizar AWS Service Catalog, debe concederle acceso a la vista de la consola del usuario final de AWS Service Catalog. Para conceder acceso, se adjuntan políticas al usuario, grupo o rol de IAM que el usuario final utiliza. En el siguiente procedimiento, adjuntamos la política **AWSServiceCatalogEndUserFullAccess** a un grupo de IAM.

Para conceder permisos a un grupo de usuarios finales

1. Abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación, elija User groups (Grupos de usuarios).
3. Elija Crear nuevo grupo y haga lo siguiente:
  - a. En Nombre de grupo, escriba **Endusers**.
  - b. En el campo de búsqueda, escriba **AWSServiceCatalog** para filtrar la lista de políticas.
  - c. Seleccione la casilla de verificación de la política **AWSServiceCatalogEndUserFullAccess** . También tiene la opción de elegir **AWSServiceCatalogEndUserReadOnlyAccess** en su lugar.
  - d. Elija Create Group.
4. En el panel de navegación, elija Usuarios.
5. Elija Añadir usuario y haga lo siguiente:

- a. En User name (Nombre de usuario), escriba un nombre para el usuario.
- b. Seleccione Contraseña - AWS Management Console access.
- c. Elija Siguiente: permisos.
- d. Elija Agregar usuario al grupo.
- e. Seleccione la casilla del grupo Endusers y elija Next: Tags (Siguiente: Etiquetas) y, después, Next: Review (Siguiente: Revisar).
- f. En la página Review, elija Create user. Descargue o copie las credenciales y, a continuación, elija Close (Cerrar).

## Instalar y configurar el motor de aprovisionamiento Terraform

Para utilizar correctamente los productos de Terraform con AWS Service Catalog, debe instalar y configurar un motor de aprovisionamiento de Terraform en la misma cuenta en la que administrará los productos de Terraform. Para empezar, puede utilizar el motor de aprovisionamiento de Terraform proporcionado por AWS, que instala y configura el código y la infraestructura necesarios para que funcione el motor de aprovisionamiento de Terraform con AWS Service Catalog. Esta configuración de una sola vez tarda aproximadamente 30 minutos. AWS Service Catalog proporciona un GitHub repositorio con instrucciones para [instalar y configurar el motor de aprovisionamiento Terraform](#).

### Determinación de cola

Cuando llama a una operación de aprovisionamiento, AWS Service Catalog prepara un mensaje de carga útil para enviarlo a la cola correspondiente del motor de aprovisionamiento. Para crear el ARN de la cola, AWS Service Catalog hace las siguientes suposiciones:

- El motor de aprovisionamiento se encuentra en la cuenta del propietario del producto
- El motor de aprovisionamiento se encuentra en la misma región en la que se realizó la llamada a AWS Service Catalog
- Las colas del motor de aprovisionamiento siguen el esquema de nomenclatura documentado que se detalla a continuación

Por ejemplo, si ProvisionProduct se llama us-east-1 desde la cuenta 1111111111 con un producto creado por la cuenta 000000000000, se AWS

Service Catalog supone que el ARN de SQS correcto es. `arn:aws:sqs:us-east-1:000000000000:ServiceCatalogTerraform0SProvisionOperationQueue`

La misma lógica se aplica a la función de Lambda llamada por `DescribeProvisioningParameters`.

## Agregar Confused Deputy a su motor de aprovisionamiento Terraform

Claves de contexto de Confused Deputy en los puntos de conexión para restringir el acceso a las operaciones **lambda:Invoke**

La función de Lambda del analizador de parámetros creada por los motores proporcionados por AWS Service Catalog tiene una política de acceso que otorga permisos de `lambda:Invoke` entre cuentas únicamente a la entidad principal del servicio AWS Service Catalog:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "servicecatalog.amazonaws.com"
      },
      "Action": "lambda:InvokeFunction",
      "Resource": "arn:aws:lambda:us-east-1:account_id:function:ServiceCatalogTerraform0SParameterParser"
    }
  ]
}
```

Este debería ser el único permiso necesario para que la integración con AWS Service Catalog funcione correctamente. Sin embargo, puede restringirlo aún más utilizando la clave de contexto `aws:SourceAccount` [Confused Deputy](#). Cuando AWS Service Catalog envía mensajes a estas colas, AWS Service Catalog rellena la clave con el ID de la cuenta de aprovisionamiento. Esto resulta útil si tiene intención de distribuir productos mediante el uso compartido de carteras y quiere asegurarse de que solo cuentas específicas utilicen su motor.

Por ejemplo, puede restringir su motor para que solo permita solicitudes que se originen entre `000000000000` y `111111111111` con la condición que se muestra a continuación:

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Principal": {
      "Service": "servicecatalog.amazonaws.com"
    },
    "Action": "lambda:InvokeFunction",
    "Resource": "arn:aws:lambda:us-
east-1:account_id:function:ServiceCatalogTerraformOSParameterParser",
    "Condition": {
      "StringLike": {
        "aws:SourceAccount": ["000000000000", "111111111111"]
      }
    }
  }
]
}

```

## Claves de contexto de Confused Deputy en los puntos de conexión para restringir el acceso a las operaciones **sqs:SendMessage**

Las colas de Amazon SQS de entrada a la operación de aprovisionamiento creadas por los motores proporcionados por AWS Service Catalog tienen una política de acceso que concede permisos de `sqs:SendMessage` entre cuentas (y el KMS asociado) únicamente a la entidad principal del servicio AWS Service Catalog:

```

{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "Enable AWS Service Catalog to send messages to the queue",
      "Effect": "Allow",
      "Principal": {
        "Service": "servicecatalog.amazonaws.com"
      },
      "Action": "sqs:SendMessage",
      "Resource": [
        "arn:aws:sqs:us-
east-1:account_id:ServiceCatalogTerraformOSProvisionOperationQueue"
      ]
    },
  ],
}

```

```

    {
      "Sid": "Enable AWS Service Catalog encryption/decryption permissions when
sending message to queue",
      "Effect": "Allow",
      "Principal": {
        "Service": "servicecatalog.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ReEncrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "arn:aws:kms:us-east-1:account_id:key/key_id"
    }
  ]
}

```

Este debería ser el único permiso necesario para que la integración con AWS Service Catalog funcione correctamente. Sin embargo, puede restringirlo aún más utilizando la clave de contexto `aws:SourceAccount` [Confused Deputy](#). Cuando AWS Service Catalog envía mensajes a estas colas, AWS Service Catalog rellena las claves con el ID de la cuenta de aprovisionamiento. Esto resulta útil si tiene intención de distribuir productos mediante el uso compartido de carteras y quiere asegurarse de que solo cuentas específicas utilicen su motor.

Por ejemplo, puede restringir su motor para que solo permita solicitudes que se originen entre 000000000000 y 111111111111 con la condición que se muestra a continuación:

```

{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "Enable AWS Service Catalog to send messages to the queue",
      "Effect": "Allow",
      "Principal": {
        "Service": "servicecatalog.amazonaws.com"
      },
      "Action": "sqs:SendMessage",
      "Resource": [
        "arn:aws:sqs:us-
east-1:account_id:ServiceCatalogTerraformOSProvisionOperationQueue"
      ],
    }
  ]
}

```

```
    "Condition": {
      "StringLike": {
        "aws:SourceAccount": ["000000000000", "111111111111"]
      }
    },
    {
      "Sid": "Enable AWS Service Catalog encryption/decryption permissions when
sending message to queue",
      "Effect": "Allow",
      "Principal": {
        "Service": "servicecatalog.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:Decrypt",
        "kms:ReEncrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "arn:aws:kms:us-east-1:account_id:key/key_id"
    }
  ]
}
```

# Introducción

Para empezar con AWS Service Catalog, utilice una de las plantillas de producto bien diseñadas de la biblioteca de introducción o siga los pasos de uno de los tutoriales de introducción.

En el tutorial realizará tareas como administrador del catálogo y usuario final. Como administrador del catálogo, usted crea una cartera y, a continuación, un producto. Como usuario final, debe verificar que puede acceder a la consola del usuario final y lanzar el producto. El producto es uno de los siguientes:

- Un entorno de desarrollo en la nube que se ejecuta en Amazon Linux y se basa en una plantilla de AWS CloudFormation que define los recursos de AWS que puede utilizar el producto.
- Un entorno de código abierto que se ejecuta en un motor de aprovisionamiento de Terraform y se basa en un archivo de configuración tar.gz que define los recursos de AWS que puede utilizar el producto.

## Note

Antes de comenzar, asegúrese de que ha realizado las acciones de [Configuración AWS Service Catalog](#).

## Temas

- [Biblioteca de introducción](#)
- [Introducción a un producto de AWS CloudFormation](#)
- [Introducción a un producto Terraform](#)

# Biblioteca de introducción

AWS Service Catalog proporciona una biblioteca de introducción de plantillas de productos de Well-Architected para que pueda comenzar rápidamente. Puede copiar cualquiera de los productos de las carteras de nuestra biblioteca de introducción en su cuenta y, a continuación, personalizarlo para que se adapte a sus necesidades.

## Temas

- [Requisitos previos](#)
- [Más información](#)

## Requisitos previos

Antes de utilizar las plantillas de nuestra biblioteca de introducción, asegúrese de contar con lo siguiente:

- Los permisos necesarios para utilizar las plantillas de AWS CloudFormation. Para obtener más información, consulte [Control del acceso con AWS Identity and Access Management](#).
- Los permisos de administrador necesarios para administrar AWS Service Catalog. Para obtener más información, consulte [the section called “Identity and Access Management”](#).

## Más información

Para obtener más información acerca del marco de Well-Architected, consulte [AWSWell-Architected](#).

## Introducción a un producto de AWS CloudFormation

Para empezar con AWS Service Catalog, utilice una de las plantillas de productos bien diseñadas de la biblioteca de introducción o siga los pasos del tutorial de introducción.

En el tutorial realizará tareas como administrador del catálogo y usuario final. Como administrador del catálogo, usted crea una cartera y, a continuación, un producto. Como usuario final, debe verificar que puede acceder a la consola de usuario final e iniciar el producto. El producto es un entorno de desarrollo en la nube que se ejecuta en Amazon Linux y se basa en una plantilla de AWS CloudFormation que define los recursos de AWS que puede utilizar el producto.

### Note

Antes de comenzar, asegúrese de que ha realizado las acciones que se detallan en [Configuración AWS Service Catalog](#).

## Temas

- [Paso 1: Descargar la plantilla de AWS CloudFormation](#)
- [Paso 2: Crear un par de claves](#)

- [Paso 3: Crear una cartera](#)
- [Paso 4: Crear un nuevo producto en la cartera](#)
- [Paso 5: agregar una restricción de plantilla para limitar el tamaño de instancia](#)
- [Paso 6: Agregar una restricción de lanzamiento para asignar un rol de IAM.](#)
- [Paso 7: Conceder acceso a la cartera a los usuarios finales](#)
- [Paso 4: Probar la experiencia del usuario final](#)

## Paso 1: Descargar la plantilla de AWS CloudFormation

Puede usar plantillas de AWS CloudFormation para configurar y aprovisionar carteras y productos. Las plantillas son archivos de texto con formato JSON o YAML que describen los recursos que desea aprovisionar. Para obtener más información, consulte [Formatos de plantilla](#) en la Guía del usuario de AWS CloudFormation. Puede utilizar el editor de AWS CloudFormation o cualquier editor de texto de su elección para crear y guardar plantillas. En este tutorial, hemos proporcionado una plantilla sencilla para comenzar. Esta plantilla lanza una única instancia de Linux configurada para el acceso SSH.

### Note

El uso de plantillas de AWS CloudFormation requiere permisos especiales. Antes de comenzar, confirme que cuenta con los siguientes permisos: Para obtener más información, consulte Requisitos previos en la [Biblioteca de introducción](#).

## Descarga de la plantilla

La plantilla de ejemplo proporcionada para este tutorial, `development-environment.template`, está disponible en <https://awsdocs.s3.amazonaws.com/servicecatalog/development-environment.template>.

## Descripción general de la plantilla

El texto de la plantilla de ejemplo se muestra a continuación:

```
{
  "AWSTemplateFormatVersion" : "2010-09-09",

  "Description" : "AWS Service Catalog sample template. Creates an Amazon EC2 instance
```



```

    "ParameterLabels" : {
      "InstanceType": {"default": "Server size:"},
      "KeyName": {"default": "Key pair:"},
      "SSHLocation": {"default": "CIDR range:"}
    }
  },
  "Mappings" : {
    "AWSRegionArch2AMI" : {
      "us-east-1"      : { "HVM64" : "ami-08842d60" },
      "us-west-2"      : { "HVM64" : "ami-8786c6b7" },
      "us-west-1"      : { "HVM64" : "ami-cfa8a18a" },
      "eu-west-1"      : { "HVM64" : "ami-748e2903" },
      "ap-southeast-1" : { "HVM64" : "ami-d6e1c584" },
      "ap-northeast-1" : { "HVM64" : "ami-35072834" },
      "ap-southeast-2" : { "HVM64" : "ami-fd4724c7" },
      "sa-east-1"      : { "HVM64" : "ami-956cc688" },
      "cn-north-1"     : { "HVM64" : "ami-ac57c595" },
      "eu-central-1"   : { "HVM64" : "ami-b43503a9" }
    }
  },
  "Resources" : {
    "EC2Instance" : {
      "Type" : "AWS::EC2::Instance",
      "Properties" : {
        "InstanceType" : { "Ref" : "InstanceType" },
        "SecurityGroups" : [ { "Ref" : "InstanceSecurityGroup" } ],
        "KeyName" : { "Ref" : "KeyName" },
        "ImageId" : { "Fn::FindInMap" : [ "AWSRegionArch2AMI", { "Ref" :
"AWS::Region" }, "HVM64" ] }
      }
    },
    "InstanceSecurityGroup" : {
      "Type" : "AWS::EC2::SecurityGroup",
      "Properties" : {
        "GroupDescription" : "Enable SSH access via port 22",
        "SecurityGroupIngress" : [ {
          "IpProtocol" : "tcp",
          "FromPort" : "22",
          "ToPort" : "22",

```

```

        "CidrIp" : { "Ref" : "SSHLocation"}
      } ]
    }
  },
  "Outputs" : {
    "PublicDNSName" : {
      "Description" : "Public DNS name of the new EC2 instance",
      "Value" : { "Fn::GetAtt" : [ "EC2Instance", "PublicDnsName" ] }
    },
    "PublicIPAddress" : {
      "Description" : "Public IP address of the new EC2 instance",
      "Value" : { "Fn::GetAtt" : [ "EC2Instance", "PublicIp" ] }
    }
  }
}

```

## Recursos de la plantilla

La plantilla declara recursos que deben crearse al lanzar el producto. Consta de las secciones siguientes:

- **AWSTemplateFormatVersion**(opcional): la versión del [formato de AWS plantilla](#) utilizada para crear esta plantilla. La última versión de formato de plantilla es 2010-09-09 y es en la actualidad el único valor válido.
- **Descripción** (opcional) – Descripción de la plantilla.
- **Parameters** (opcional) - Parámetros que el usuario debe especificar para lanzar el producto. Para cada parámetro, la plantilla incluye una descripción y las restricciones que el valor escrito debe cumplir. Para obtener más información acerca de las restricciones, consulte [Uso de las restricciones AWS Service Catalog](#).

El parámetro `KeyName` permite especificar el nombre del par de claves de Amazon Elastic Compute Cloud (Amazon EC2) que los usuarios finales deben proporcionar cuando utilizan AWS Service Catalog para lanzar el producto. El par de claves se crea en el siguiente paso.

- **Metadata** (opcional) – Objetos que proporcionan información adicional acerca de la plantilla. La clave [AWS:CloudFormation: :Interfaz](#) define cómo se muestran los parámetros en la vista de la consola del usuario final. La propiedad `ParameterGroups` define cómo se agrupan los parámetros y los encabezados de esos grupos. La propiedad `ParameterLabels` define los nombres intuitivos de los parámetros. Cuando un usuario especifica los parámetros para lanzar

un producto que se basa en esta plantilla, la vista de la consola del usuario final muestra el parámetro con la etiqueta `Server size`: bajo el encabezado `Instance configuration` y los parámetros con la etiqueta `Key pair`: y `CIDR range`:, bajo el encabezado `Security configuration`.

- **Mappings (opcional)** –Un mapeo de claves y valores asociados que puede utilizar para especificar valores de parámetros condicionales, similar a una tabla de búsqueda. Puede hacer coincidir una clave con el valor correspondiente mediante la función `FindInMap` intrínseca [Fn::](#) de las secciones `Recursos` y `Resultados`. La plantilla anterior incluye una lista de `AWSregiones` y la imagen de máquina de Amazon (AMI) que corresponde a cada una. `AWS Service Catalog` utiliza esta asignación para determinar qué AMI usar según la `AWSregion` que el usuario selecciona en el archivo `AWS Management Console`.
- **Recursos (obligatorio)** – Recursos de pila y sus propiedades. Puede consultar los recursos en las secciones `Recursos` y `Salidas` de la plantilla. En la plantilla anterior, especificamos una instancia de `EC2` que ejecute `Amazon Linux` y un grupo de seguridad que permita a `SSH` acceso a la instancia. La sección `Propiedades del recurso` de la instancia `EC2` utiliza la información que el usuario escribe para configurar el tipo de instancia y un nombre de clave para el acceso `SSH`.

`AWS CloudFormation` utiliza la región actual de `AWS` para seleccionar el identificador de AMI entre los mapeos definidos anteriormente y le asigna un grupo de seguridad. El grupo de seguridad está configurado para permitir el acceso entrante en el puerto `22` desde el rango de direcciones IP de `CIDR` que el usuario especifica.

- **Outputs: (opcional)** texto que indica al usuario cuándo se ha completado el lanzamiento de un producto. La plantilla proporcionada obtiene el nombre de `DNS` público de la instancia lanzada y se lo muestra al usuario. El usuario necesita el nombre de `DNS` para conectarse a la instancia mediante `SSH`.

Para obtener más información sobre la estructura de las plantillas, consulte [Referencia de las plantillas](#) en la `AWS CloudFormation Guía del usuario`.

## Paso 2: Crear un par de claves

Para que los usuarios finales puedan lanzar el producto que se basa en la plantilla de ejemplo de este tutorial, debe crear un par de claves de `Amazon EC2`. Un par de claves es una combinación de una clave pública que se utiliza para cifrar los datos y una clave privada que se utiliza para descifrarlos. Para obtener más información sobre los pares de claves, asegúrese de haber iniciado

sesión en la AWS consola y, a continuación, consulte los [pares de claves de Amazon EC2](#) en la Guía del usuario de Amazon EC2.

La AWS CloudFormation plantilla de este tutorial incluye `development-environment.template` el `KeyName` parámetro:

```
. . .
"Parameters" : {
  "KeyName": {
    "Description" : "Name of an existing EC2 key pair for SSH access to the EC2
instance.",
    "Type": "AWS::EC2::KeyPair::KeyName"
  },
. . .
```

Los usuarios finales deben especificar el nombre de un par de claves AWS Service Catalog al lanzar el producto basado en la plantilla.

Si ya tiene un par de claves en la cuenta que prefiere utilizar, puede ir directamente a [Paso 3: Crear una cartera](#). De lo contrario, lleve a cabo los pasos que figuran a continuación.

### Crear un par de claves

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, en Network & Security, seleccione Key Pairs.
3. En la página Key Pairs, elija Create Key Pair.
4. En Key pair name, escriba un nombre que sea fácil de recordar y, a continuación, seleccione Create.
5. Cuando la consola le pida que guarde el archivo de clave privada, guárdelo en un lugar seguro.

#### Important

Esta es la única oportunidad para guardar el archivo de clave privada.

## Paso 3: Crear una cartera

Para proporcionar productos a los usuarios, comience por crear una cartera para ellos.

## Para crear una cartera

1. Abra la consola de Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. En el panel de navegación izquierdo, elija Portfolios y luego, Crear cartera.
3. Escriba los siguientes valores:
  - Portfolio name: **Engineering Tools**
  - Descripción de la cartera – **Sample portfolio that contains a single product.**
  - Propietario – **IT (it@example.com)**
4. Seleccione Crear.

## Paso 4: Crear un nuevo producto en la cartera

Una vez que haya creado una cartera, estará listo para crear un producto dentro de la cartera. En este tutorial, creará un producto denominado Linux Desktop, un entorno de desarrollo en la nube que se ejecuta en Amazon Linux, dentro de la cartera Herramienta de ingeniería.

### Para crear un producto dentro de una cartera

1. Si acaba de completar el paso anterior, la página Portfolios ya está abierta. De lo contrario, abra <https://console.aws.amazon.com/servicecatalog/>.
2. Seleccione y abra la cartera de Herramientas de ingeniería que ha creado en el paso 2.
3. Seleccione Cargar un producto nuevo.
4. En la página Crear producto, en la sección detalles del producto, introduzca lo siguiente:
  - Product name: **Linux Desktop**
  - Descripción del producto – **Cloud development environment configured for engineering staff. Runs AWS Linux.**
  - Propietario – **IT**
  - Distribuidor – (en blanco)
5. En la página de detalles de la versión, selecciona Usar una CloudFormation plantilla. A continuación, seleccione Especificar una URL de plantilla de Amazon S3 e introduzca lo siguiente:
  - Select template: **<https://awsdocs.s3.amazonaws.com/servicecatalog/development-environment.template>**

- Título de versión – **v1.0**
  - Descripción: **Base Version**
6. En la página Support details, haga lo siguiente:
    - Contacto para correo electrónico – **ITSupport@example.com**
    - Enlace de soporte – **https://wiki.example.com/IT/support**
    - Descripción de soporte – **Contact the IT department for issues deploying or connecting to this product.**
  7. Seleccione Crear producto.

## Paso 5: agregar una restricción de plantilla para limitar el tamaño de instancia

Las restricciones suponen una capa de control adicional de los productos para toda la cartera. Las restricciones permiten controlar el contexto de lanzamiento de un producto (restricciones de lanzamiento) o agregar reglas a la plantilla de AWS CloudFormation (restricciones de plantilla). Para obtener más información, consulte [Uso de las restricciones AWS Service Catalog](#).

Agregue una restricción de plantilla al producto Linux Desktop que impedirá que los usuarios seleccionen los tipos de instancias grandes en el momento del lanzamiento. La plantilla del entorno de desarrollo permite al usuario elegir entre seis tipos de instancias. Esta restricción limita los tipos de instancias válidos a los dos tipos menores: `t2.micro` y `t2.small`. Para obtener más información, consulte [las instancias T2](#) en la Guía del usuario de Amazon EC2.

### Cómo agregar una restricción de plantilla al producto Linux Desktop

1. En la página Detalles de la cartera, elija la pestaña Restricciones y, a continuación, elija Crear restricción.
2. En la página Crear restricción, para Producto, seleccione Linux Desktop. A continuación, en Tipo de restricción, elija Plantilla.
3. En la sección Restricciones de plantillas, seleccione Editor de texto.
4. Pegue el siguiente contenido en el editor:

```
{
  "Rules": {
    "Rule1": {
```

```
    "Assertions": [  
      {  
        "Assert" : {"Fn::Contains": [["t2.micro", "t2.small"], {"Ref":  
"InstanceType"}]},  
        "AssertDescription": "Instance type should be t2.micro or t2.small"  
      }  
    ]  
  }  
}
```

5. Para la descripción de la restricción, introduzca **Small instance sizes**.
6. Seleccione Crear.

## Paso 6: Agregar una restricción de lanzamiento para asignar un rol de IAM.

Una restricción de lanzamiento designa una función del rol de IAM que AWS Service Catalog asume cuando un usuario final lanza un producto.

En este paso, agrega una restricción de lanzamiento al producto Linux Desktop para que AWS Service Catalog pueda utilizar los recursos que forman parte de la plantilla de AWS CloudFormation del producto.

El rol de IAM que se asigna a un producto como restricción de lanzamiento debe tener permisos para utilizar lo siguiente:

1. AWS CloudFormation
2. Los servicios en la plantilla de AWS CloudFormation del producto
3. Acceso de solo lectura a la plantilla de AWS CloudFormation en un bucket de Amazon S3 propiedad del servicio.

Esta restricción de lanzamiento permitirá que el usuario final lance el producto y, después de lanzarlo, lo administre como producto provisionado. Para obtener más información, consulte [Restricciones de lanzamiento de AWS Service Catalog](#).

Sin una restricción de lanzamiento, es preciso conceder permisos de IAM adicionales a los usuarios finales para que pudieran utilizar el producto Linux Desktop. Por ejemplo, la política `ServiceCatalogEndUserAccess` concede los permisos mínimos de IAM que se necesitan para tener acceso a la vista de la consola del usuario final de AWS Service Catalog.

El uso de una restricción de lanzamiento le permite seguir la práctica recomendada de IAM de reducir al mínimo los permisos de IAM de los usuarios finales. Para obtener más información, consulte [Conceder privilegios mínimos](#) en la Guía del usuario de IAM.

Para agregar una restricción de lanzamiento

1. Siga las instrucciones para [crear nuevas políticas en la pestaña JSON](#) de la Guía del usuario de IAM.
2. Pegue el siguiente documento de políticas JSON:
  - `cloudformation` – Concede a AWS Service Catalog todos los permisos para crear, leer, actualizar, eliminar, enumerar y etiquetar pilas de AWS CloudFormation.
  - `ec2` – Concede a AWS Service Catalog todos los permisos para enumerar, leer, escribir, aprovisionar y etiquetar los recursos de Amazon Elastic Compute Cloud (Amazon EC2) que forman parte del producto AWS Service Catalog. En función del recurso de AWS que desee implementar, este permiso puede cambiar.
  - `ec2` – Crea una nueva política administrada para su cuenta de AWS y adjunta la política administrada especificada al rol de IAM especificado.
  - `s3` - Permite el acceso a los buckets de Amazon S3 propiedad de AWS Service Catalog. Para implementar el producto, AWS Service Catalog requiere acceso a los artefactos de aprovisionamiento.
  - `servicecatalog` – Concede a AWS Service Catalog permisos para enumerar, leer, escribir, etiquetar y lanzar recursos en nombre del usuario final.
  - `sns` – Concede a AWS Service Catalog permisos para enumerar, leer, escribir y etiquetar temas de Amazon SNS para la restricción de lanzamiento.

 Note

En función de los recursos subyacentes que desee implementar, es posible que deba modificar la política de JSON de ejemplo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

    "Effect": "Allow",
    "Action": [
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStackEvents",
      "cloudformation:DescribeStacks",
      "cloudformation:GetTemplateSummary",
      "cloudformation:SetStackPolicy",
      "cloudformation:ValidateTemplate",
      "cloudformation:UpdateStack",
      "ec2:*",
      "servicecatalog:*",
      "sns:*"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetObject"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
      }
    }
  }
]
}

```

3. Elija Siguiente, Etiquetas.
4. Elija Siguiente, Etiquetas.
5. En la página Revisar política para el Nombre introduzca **linuxDesktopPolicy**.
6. Elija Crear política.
7. Seleccione Roles en el panel de navegación. Elija Crear role y haga lo siguiente:
  - a. En Seleccionar una entidad de confianza, seleccione AWSservicio y, a continuación, bajo Usar caso para otros servicios AWS, seleccione Service Catalog. Seleccione el caso de uso Service Catalog y, a continuación, elija Siguiente.
  - b. Busque la linuxDesktopPolicypolítica y, a continuación, active la casilla de verificación.

- c. Elija Siguiente.
  - d. En Role name, escriba **linuxDesktopLaunchRole**.
  - e. Elija Crear rol.
8. Abra la AWS Service Catalog consola en <https://console.aws.amazon.com/servicecatalog>.
  9. Elija la cartera Engineering Tools.
  10. En la página Detalles de la cartera, elija la pestaña Restricciones y, a continuación, elija Crear restricción.
  11. En Producto, elija Linux Desktop y en Restricción elija Cargar.
  12. Seleccione Seleccionar el rol de IAM. A continuación, elija linuxDesktopLaunchRol y, a continuación, elija Crear.

## Paso 7: Conceder acceso a la cartera a los usuarios finales

Ahora que ha creado una cartera de productos y ha agregado un producto, puede conceder acceso a los usuarios finales.

### Requisitos previos

Si no ha creado un grupo de IAM; para los usuarios finales, consulte [Concesión de permisos a los usuarios finales de AWS Service Catalog](#).

Para proporcionar acceso a la cartera

1. En la página de detalles de cartera, elija la tabla Acceso .
2. Elija Grant access (Conceder acceso).
3. En la pestaña Grupos, seleccione la casilla correspondiente al grupo de IAM de los usuarios finales.
4. Seleccione Añadir acceso.

## Paso 4: Probar la experiencia del usuario final

Para comprobar que el usuario final puede obtener acceso correctamente a la vista de la consola del usuario final y lanzar el producto, inicie sesión en AWS como ese usuario final y lleve a cabo las siguientes tareas.

Para comprobar que el usuario final puede obtener acceso a la consola del usuario final

1. Siga las instrucciones de [Iniciar sesión de un rol para un usuario de IAM](#) en la Guía del usuario de IAM.
2. En la barra de menús, seleccione la región AWS en la que ha creado la cartera Engineering Tools. Para este tutorial, seleccione la región us-east-1.
3. Abra la consola AWS Service Catalog en <https://console.aws.amazon.com/servicecatalog/> para ver:
  - Products: los productos que el usuario puede utilizar.
  - Provisioned products: los productos aprovisionados que el usuario ha lanzado.

Para comprobar que el usuario final puede lanzar el producto Linux Desktop

Tenga en cuenta que para este tutorial debe seleccionar la región us-east-1.

1. En la sección Productos de la consola, seleccione Linux Desktop.
2. Elija Lanzar producto con el fin de iniciar el asistente para configurar el producto.
3. En la página Lanzar: Linux Desktop, introduzca **Linux-Desktop** como nombre del producto aaprovisionado.
4. En la página Parámetros, escriba lo siguiente y, a continuación, elija Siguiente:
  - Server size Elija **t2.micro**.
  - Key pair: seleccione el par de claves que creó en [Paso 2: Crear un par de claves](#).
  - CIDR range: escriba un intervalo de CIDR válido para la dirección IP desde la que se conectará a la instancia. Puede introducir el valor predeterminado (0.0.0.0/0) para permitir el acceso desde cualquier dirección IP, su dirección IP seguida de **/32** para restringir el acceso a su dirección IP únicamente o una opción intermedia.
5. Seleccione Lanzar producto para lanzar la pila. La consola muestra la página de detalles de la pila de Linux-Desktop. El estado inicial del producto es En cambio. AWS Service Catalog tarda varios minutos en lanzar el producto. Para ver el estado actual, actualice el navegador. Una vez que el producto se ha lanzado, el estado es disponible.

# Introducción a un producto Terraform

AWS Service Catalog permite un aprovisionamiento rápido y de autoservicio con control interno para sus configuraciones de [HashiCorp Terraform](#). AWS puede utilizar AWS Service Catalog como una herramienta única para organizar, regular y distribuir sus configuraciones de Terraform según sea necesario dentro de AWS. AWS Service Catalog es compatible con Terraform en varias características clave, como la catalogación de plantillas de Terraform estandarizadas y previamente aprobadas, el control de acceso, el control de versiones, el etiquetado y el uso compartido con otras cuentas de AWS. En AWS Service Catalog, sus usuarios finales ven una lista sencilla de productos y versiones a los que tienen acceso y, a continuación, pueden implementar esos productos en una sola acción.

## Note

Para continuar con el soporte de HashiCorp las tecnologías, como resultado de los recientes cambios en las licencias de Terraform, AWS Service Catalog cambiamos cualquier referencia anterior a Terraform Open Source por la de External. El tipo de producto externo incluye soporte para Terraform Community Edition, anteriormente conocida como Terraform Open Source. Para obtener más información e instrucciones sobre cómo migrar sus productos de código abierto y los productos aprovisionados de Terraform existentes al tipo de producto externo, consulte [Actualizar los productos existentes de Terraform Open Source y los productos aprovisionados al tipo de producto externo](#).

Los pasos del siguiente tutorial lo ayudarán a empezar a utilizar un producto de Terraform en AWS Service Catalog.

Como administrador del catálogo, usted trabaja en una cuenta de administrador central (cuenta central). Tanto los productos de Terraform Community Edition como de Terraform Cloud requieren un motor de aprovisionamiento Terraform, sobre el que puede obtener más información en [Motor de aprovisionamiento para Terraform Community Edition \(tipo de producto externo\)](#) y [Motor de aprovisionamiento para Terraform Cloud](#).

Durante el tutorial, usted realiza las tareas siguientes en la cuenta de administrador:

- Cree un producto de Terraform utilizando el tipo de producto Terraform Cloud o Externo. Service Catalog utiliza el tipo de producto externo para respaldar los productos de Terraform Community Edition.

- Asocia el producto a una cartera.
- Cree una restricción de lanzamiento que permita a sus usuarios finales aprovisionar el producto
- Etiquetar el producto
- Comparta la cartera y el producto de Terraform con la cuenta de usuario final (cuenta radial)

En el tutorial, usted comparte un portafolio mediante la opción de compartir organizaciones desde la cuenta central de administración, que también es la cuenta de administración de la organización. Para obtener más información sobre el uso compartido de organizaciones, consulte [Uso compartido de carteras](#).

El recurso de AWS contenido en el producto de Terraform que ha creado en el tutorial es un bucket simple de Amazon S3.

#### Note

Antes de comenzar, asegúrese de que ha realizado las acciones de [Configuración AWS Service Catalog](#).

## Temas

- [Actualizar los productos existentes de Terraform Open Source y los productos aprovisionados al tipo de producto externo](#)
- [Requisito previo: Configurar su motor de aprovisionamiento Terraform](#)
- [Paso 1: Descargar el archivo de configuración Terraform](#)
- [Paso 2: Crear un producto de Terraform](#)
- [Paso 3: Crear una AWS Service Catalog cartera](#)
- [Paso 4: Añadir el producto a la cartera](#)
- [Paso 5: Crear roles de lanzamiento](#)
- [Paso 6: Añadir una restricción de lanzamiento a su producto de Terraform](#)
- [Paso 7: Conceder acceso al usuario final](#)
- [Paso 8: Compartir la cartera con el usuario final](#)
- [Paso 4: Probar la experiencia del usuario final](#)
- [Paso 10: Monitorización de las operaciones de aprovisionamiento de Terraform](#)

## Actualizar los productos existentes de Terraform Open Source y los productos aaprovisionados al tipo de producto externo

Para continuar con el soporte de HashiCorp las tecnologías, como resultado de los recientes cambios en las licencias de Terraform, AWS Service Catalog cambié cualquier referencia anterior de Terraform Open Source a External. El tipo de producto externo incluye soporte para Terraform Community Edition, anteriormente conocida como Terraform Open Source. AWS Service Catalog ya no es compatible con Terraform Open Source como tipo de producto válido para ningún producto nuevo o aaprovisionado. Solo podrá actualizar o cancelar los recursos de Terraform Open Source existentes, incluidos las versiones de los productos y los productos aaprovisionados.

Si aún no lo ha hecho, debe realizar la transición de todos los productos de Terraform Open Source y aaprovisionados existentes a productos externos, mediante las instrucciones de esta sección.

1. Actualice su motor de referencia de Terraform actual para que AWS Service Catalog incluya soporte para los tipos de productos tanto Externos como Terraform Open Source. [Para obtener instrucciones sobre cómo actualizar su motor de referencia de Terraform, consulte nuestro repositorio. GitHub](#)
2. Recree cualquier producto existente de Terraform Open Source utilizando el nuevo tipo de producto externo.
3. Elimine cualquier producto existente que utilice el tipo de producto Terraform Open Source.
4. Reaprovisione esos recursos restantes para utilizar el nuevo tipo de producto externo.
5. Cancele cualquier producto aaprovisionado existente que utilice el tipo de producto Terraform Open Source.

Tras realizar la transición de sus productos existentes, utilice el tipo de producto externo para cualquier producto nuevo que utilice un archivo de configuración tar.gz.

AWS Service Catalog apoyará a los clientes durante este cambio según sea necesario. Si estos cambios requieren un esfuerzo considerable para su cuenta o afectan a las cargas de trabajo esenciales de los productos, póngase en contacto con el representante de su cuenta para solicitar asistencia.

### Requisito previo: Configurar su motor de aprovisionamiento Terraform

Como requisito previo para crear productos de Terraform en AWS Service Catalog, debe instalar y configurar un motor de aprovisionamiento en su cuenta de administrador de Service Catalog

(cuenta central). El motor de aprovisionamiento es necesario tanto para los productos de Terraform Community Edition (que utilizan el tipo de producto externo) como para los productos de Terraform Cloud (que utilizan el tipo de producto Terraform Cloud).

 Note

La configuración del motor se realiza una sola vez y tarda aproximadamente 30 minutos.

## Motor de aprovisionamiento para Terraform Community Edition (tipo de producto externo)

AWS Service Catalog utiliza el tipo de producto externo para respaldar los productos de Terraform Community Edition. El tipo de producto externo también es compatible con otras herramientas de aprovisionamiento, como Pulumi, Ansible y Chef, entre otras, según la configuración del motor de aprovisionamiento.

Para AWS Service Catalog los productos que utilizan el tipo de producto externo con HashiCorp Terraform Community Edition, debe instalar y configurar un motor de aprovisionamiento de Terraform en su cuenta de AWS Service Catalog administrador (cuenta hub). AWS administra este motor y sus recursos.

AWS Service Catalog proporciona un GitHub repositorio con instrucciones sobre la [instalación y configuración del motor de aprovisionamiento Terraform AWS proporcionado por Terraform](#). La repo incluye la información siguiente:

- Herramientas necesarias para la instalación
- Construir el código
- Implementar en una cuenta de AWS
- Información adicional sobre los flujos de trabajo de aprovisionamiento, el control de calidad y las limitaciones

## Motor de aprovisionamiento para Terraform Cloud

En el AWS Service Catalog caso de los productos que utilizan el tipo de producto Terraform Cloud con HashiCorp Terraform Cloud, debe instalar y configurar un motor de aprovisionamiento de Terraform en su AWS Service Catalog cuenta de administrador (cuenta hub). HashiCorp administra este motor en un entorno remoto.

HashiCorp proporciona un GitHub repositorio con instrucciones sobre cómo configurar el [motor Terraform Cloud para AWS Service Catalog](#). La repo incluye la información siguiente:

- Herramientas necesarias para la instalación
- Construir el código
- Implementar en una cuenta de AWS
- Información adicional sobre los flujos de trabajo de aprovisionamiento, el control de calidad y las limitaciones

## Paso 1: Descargar el archivo de configuración Terraform

Puede usar un archivo de configuración de Terraform para crear y aprovisionar productos de HashiCorp Terraform. Estas configuraciones son archivos de texto sin formato y describen los recursos que desea aprovisionar. Puede usar el editor de texto que prefiera para crear, actualizar y guardar las configuraciones. Para la creación de productos, debe cargar las configuraciones de Terraform como un archivo tar.gz. En este tutorial, AWS Service Catalog proporciona un archivo de configuración sencillo para que pueda empezar. Para crear un bucket de Amazon S3 con la consola

### Descargar el archivo de configuración

AWS Service Catalog proporciona un ejemplo de archivo de configuración [simple-s3-bucket.tar.gz](#) para que lo utilice en este tutorial.

### Información general de la configuración

El texto del archivo de configuración de ejemplo es el siguiente:

```
variable "bucket_name" {
  type = string
}
provider "aws" {
}
resource "aws_s3_bucket" "bucket" {
  bucket = var.bucket_name
}
output regional_domain_name {
  value = aws_s3_bucket.bucket.bucket_regional_domain_name
}
```

## Configuración de recursos

El archivo de configuración declara los recursos que se crearán cuando AWS Service Catalog aprovisione el producto. Consta de las secciones siguientes:

- **Variable (opcional)** – Las definiciones de valores que un usuario administrador (administrador de cuenta central) puede asignar para personalizar la configuración. Las variables proporcionan una interfaz coherente para cambiar el comportamiento de una configuración determinada. La etiqueta que sigue a la palabra clave variable es el nombre de la variable, que debe ser único entre todas las variables del mismo módulo. Este nombre se usa para asignar un valor externo a la variable y para hacer referencia al valor de la variable desde el módulo.
- **Proveedor (opcional)** – El proveedor de servicios en la nube para el aprovisionamiento de recursos, que es AWS. AWS Service Catalog solo admite a AWS como proveedor. Como resultado, el motor de aprovisionamiento de Terraform reemplaza a cualquier otro proveedor que figure en la lista con AWS.
- **Recurso (obligatorio)** – El recurso de infraestructura de AWS para el aprovisionamiento. Para este tutorial, el archivo de configuración de Terraform especifica Amazon S3.
- **Salida (opcional)** – La información o el valor regresados, similar a los valores regresados en un lenguaje de programación. Puede usar los datos de salida para configurar el flujo de trabajo de la infraestructura con herramientas de automatización.

## Paso 2: Crear un producto de Terraform

Tras instalar el motor de aprovisionamiento de Terraform, estará listo para crear un producto de HashiCorp Terraform en AWS Service Catalog. En este tutorial, usted crea un producto de Terraform que contenga un bucket de Amazon S3 simple.

Cree un nuevo producto de Terraform

1. Inicie sesión como usuario administrador de IAM y abra la AWS Service Catalog consola de IAM en <https://console.aws.amazon.com/servicecatalog/>.
2. Vaya a la sección de Administración y, a continuación, seleccione Lista de productos.
3. Seleccione Crear producto.

4. En la página Crear producto, en la sección Detalles del producto, seleccione el tipo de producto Externo o Terraform Cloud. Service Catalog utiliza el tipo de producto externo para respaldar los productos de Terraform Community Edition.
5. Introduzca los siguientes detalles de productos:
  - Product name: **Simple S3 bucket**
  - Descripción del producto: producto de Terraform que contiene un bucket de Amazon S3.
  - Propietario – **IT**
  - Distribuidor – (en blanco)
6. En la página Detalles de la versión, seleccione Cargar un archivo de plantilla y elija el archivo. Edite el archivo que ha descargado en [Paso 1: Descargar el archivo de configuración Terraform](#).
7. Introduzca lo siguiente:
  - Nombre de la versión – **v1.0**
  - Descripción de la versión – **Base Version**
8. En la sección Detalles de soporte, introduzca lo siguiente y, a continuación, seleccione Crear producto.
  - Contacto para correo electrónico – **ITSupport@example.com**
  - Enlace de soporte – **https://wiki.example.com/IT/support**
  - Descripción de soporte – **Contact the IT department for issues deploying or connecting to this product.**
9. Seleccione Crear producto.

Tras crear correctamente el producto, AWS Service Catalog muestra un banner de confirmación en la página del producto.

## Paso 3: Crear una AWS Service Catalog cartera

Puede crear una cartera en su cuenta de administrador AWS Service Catalog (cuenta central) para organizar y distribuir fácilmente los productos a las cuentas de los usuarios finales (cuentas radiales).

Para crear una cartera

1. Inicie sesión como usuario administrador de IAM y abra la AWS Service Catalog consola de IAM en <https://console.aws.amazon.com/servicecatalog/>.

2. En el panel de navegación izquierdo, elija Carteras y luego, Crear cartera.
3. Escriba los siguientes valores:
  - Portfolio name: **S3 bucket**
  - Descripción de la cartera – **Sample portfolio for Terraform configurations.**
  - Propietario – **IT (it@example.com)**
4. Seleccione Crear.

## Paso 4: Añadir el producto a la cartera

Después de crear una cartera, puede añadir el producto HashiCorp Terraform que creó en el paso 2.

Para agregar el producto a una cartera de

1. Vaya a la página Lista de productos.
2. Seleccione el producto de Terraform de bucket Simple S3 que creó en el paso 2 y, a continuación, seleccione Acciones. En el menú desplegable, seleccione Añadir producto a la cartera. AWS Service Catalog muestra el panel Añadir un bucket de Simple S3 a la cartera.
3. Seleccione la cartera de bucket de S3 y, a continuación, desactive Crear restricción de lanzamiento. Creará la restricción de lanzamiento más adelante en el tutorial.
4. Seleccione Añadir producto a la cartera.

Tras añadir correctamente el producto a la cartera, AWS Service Catalog muestra un banner de confirmación en la página de lista de productos.

## Paso 5: Crear roles de lanzamiento

En este paso, creará un rol de IAM (rol de lanzamiento) que especificará los permisos que el motor de aprovisionamiento de Terraform AWS Service Catalog puede asumir cuando un usuario final lanza un HashiCorp producto de Terraform.

El rol de IAM (rol de lanzamiento) que asigne más adelante a su bucket simple de Amazon S3, producto de Terraform, como restricción de lanzamiento debe tener los siguientes permisos:

- Acceda a los recursos subyacentes de AWS de su producto Terraform. En este tutorial, esto incluye el acceso a las operaciones `s3:CreateBucket*`, `s3>DeleteBucket*`, `s3:Get*`, `s3:List*` y `s3:PutBucketTagging` de Amazon S3.

- Acceso de lectura a la plantilla de Amazon S3 en un bucket de Amazon S3 propiedad de AWS Service Catalog
- Acceso a las operaciones del grupo de recursos `CreateGroup`, `ListGroupResources`, `DeleteGroup` y `Tag` Estas operaciones permiten a AWS Service Catalog administrar los grupos de recursos y las etiquetas

Para crear un rol de lanzamiento en AWS Service Catalog en una cuenta de administrador

1. Mientras esté conectado a la cuenta de administrador AWS Service Catalog, siga las instrucciones para [Crear nuevas políticas en la pestaña JSON](#) en la Guía del usuario de IAM.
2. Cree una política para su producto de Terraform simple de bucket de Amazon S3. Esta política debe crearse antes de crear el rol de lanzamiento y consta de los siguientes permisos:
  - `s3` - Concede permisos completos AWS Service Catalog para enumerar, leer, escribir, aprovisionar y etiquetar el producto de Amazon S3.
  - `s3` - Permite el acceso a los buckets de Amazon S3 propiedad de AWS Service Catalog. Para implementar el producto, AWS Service Catalog requiere acceso a los artefactos de aprovisionamiento.
  - `resourcegroups` - Permite a AWS Service Catalog crear, enumerar, eliminar y etiquetar AWS Resource Groups.
  - `tag` - Concede permisos de etiquetado a AWS Service Catalog .

 Note

En función de los recursos subyacentes que desee implementar, es posible que deba modificar la política de JSON de ejemplo.

Pegue lo siguiente en el documento de política JSON:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "s3:GetObject",
```

```

    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
      }
    }
  },
  {
    "Action": [
      "s3:CreateBucket*",
      "s3>DeleteBucket*",
      "s3:Get*",
      "s3:List*",
      "s3:PutBucketTagging"
    ],
    "Resource": "arn:aws:s3:::*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "resource-groups:CreateGroup",
      "resource-groups:ListGroupResources",
      "resource-groups>DeleteGroup",
      "resource-groups:Tag"
    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "tag:GetResources",
      "tag:GetTagKeys",
      "tag:GetTagValues",
      "tag:TagResources",
      "tag:UntagResources"
    ],
    "Resource": "*",
    "Effect": "Allow"
  }
]
}

```

### 3. a. Elija Siguiente, Etiquetas.

- b. Elija Siguiente, Etiquetas.
  - c. En la página Revisar política para el Nombre introduzca **S3ResourceCreationAndArtifactAccessPolicy**.
  - d. Elija Crear política.
4. En el panel de navegación, seleccione Roles y luego seleccione Crear rol.
  5. En Seleccionar una entidad de confianza, seleccione Política de confianza personalizada y, a continuación, introduzca la siguiente política de JSON:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GivePermissionsToServiceCatalog",
      "Effect": "Allow",
      "Principal": {
        "Service": "servicecatalog.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account_id:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringLike": {
          "aws:PrincipalArn": [
            "arn:aws:iam::account_id:role/TerraformEngine/
            TerraformExecutionRole*",
            "arn:aws:iam::account_id:role/TerraformEngine/
            ServiceCatalogExternalParameterParserRole*",
            "arn:aws:iam::account_id:role/TerraformEngine/
            ServiceCatalogTerraformOSParameterParserRole*"
          ]
        }
      }
    }
  ]
}
```

6. Elija Siguiente.
7. En la lista de políticas, seleccione la `S3ResourceCreationAndArtifactAccessPolicy` que ha creado.
8. Elija Siguiente.
9. En Nombre del rol, ingrese **SCLaunch-S3product**.

 Important

Los nombres de los roles de lanzamiento deben empezar por “SCLaunch” seguido del nombre de rol deseado.

10. Elija Crear rol.

 Important

Tras crear el rol de lanzamiento en su cuenta de administrador AWS Service Catalog, también debe crear un rol de lanzamiento idéntico en la cuenta de usuario final AWS Service Catalog. El rol de la cuenta de usuario final debe tener el mismo nombre e incluir la misma política que el rol de la cuenta de administrador.

Para crear un rol de lanzamiento en la cuenta del usuario final AWS Service Catalog

1. Inicie sesión como administrador en la cuenta de usuario final y, a continuación, siga las instrucciones para [Crear nuevas políticas en la pestaña JSON](#) en la Guía del usuario de IAM.
2. Repita los pasos 2 a 10 descritos anteriormente en Para crear un rol de lanzamiento en la cuenta de administrador AWS Service Catalog.

 Note

Al crear un rol de lanzamiento en la cuenta del usuario final AWS Service Catalog, asegúrese de utilizar el mismo administrador de **AccountId** en la política de confianza personalizada.

Ahora que ha creado un rol de lanzamiento tanto en la cuenta de administrador como en la de usuario final, puede añadir una restricción de lanzamiento al producto.

## Paso 6: Añadir una restricción de lanzamiento a su producto de Terraform

### Important

Debe crear una restricción de lanzamiento para los productos HashiCorp Terraform. Sin una restricción de lanzamiento, los usuarios finales no pueden aprovisionar el producto.

Tras crear un rol de lanzamiento en su cuenta de administrador, estará listo para asociarlo a una restricción de lanzamiento en sus productos externos o de Terraform Cloud.

Esta restricción de lanzamiento permitirá que el usuario final lance el producto y, después de lanzarlo, lo administre como producto aprovisionado. Para obtener más información, consulte [Restricciones de lanzamiento de AWS Service Catalog](#).

El uso de una restricción de lanzamiento le permite seguir la práctica recomendada de IAM de reducir al mínimo los permisos de IAM de los usuarios finales. Para obtener más información, consulte [Conceder privilegios mínimos](#) en la Guía del usuario de IAM.

Para asignar una restricción de lanzamiento al producto

1. [Abra la AWS Service Catalog consola en https://console.aws.amazon.com/servicecatalog](https://console.aws.amazon.com/servicecatalog).
2. En el menú de navegación izquierdo, seleccione Carteras.
3. Seleccione la cartera de bucket de S3.
4. En la página de detalles de la cartera, elija la pestaña Restricciones y, a continuación, elija Crear restricción.
5. En Producto, seleccione un bucket Simple S3. AWS Service Catalog selecciona automáticamente el tipo de restricción de Lanzamiento.
6. Seleccione Introducir el nombre del rol y, a continuación, seleccione SCLaunch-S3product.
7. Seleccione Crear .

### Note

El nombre del rol especificado debe existir en la cuenta que creó la restricción de lanzamiento y la cuenta del usuario que lanza un producto con esta restricción de lanzamiento.

## Paso 7: Conceder acceso al usuario final

Tras aplicar la restricción de lanzamiento a su producto HashiCorp Terraform, estará listo para conceder acceso a los usuarios finales de la cuenta spoke.

En este tutorial, usted concede acceso a los usuarios finales mediante el uso compartido del nombre de entidad principal. Los nombres de entidad principal son nombres para grupos, roles y usuarios que los administradores pueden especificar en una cartera y luego compartirlos con la cartera. Al compartir la cartera, AWS Service Catalog verifica si esos nombres de entidad principal ya existen. Si existen, AWS Service Catalog asocia automáticamente las entidades principales de IAM coincidentes a la cartera compartida para conceder el acceso a los usuarios finales. Consulte [Compartir una cartera](#) para obtener más información.

### Requisitos previos

Si no ha creado un grupo de IAM; para los usuarios finales, consulte [Concesión de permisos a los usuarios finales de AWS Service Catalog](#).

Para proporcionar acceso a la cartera

1. Vaya a la página Carteras y, a continuación, elija la cartera S3 bucket.
2. Seleccione la pestaña Acceso y, a continuación, seleccione Conceder acceso.
3. En el panel Tipo de acceso, seleccione Nombre de entidad principal.
4. En el panel Nombre de entidad principal, seleccione el tipo de Nombre de entidad principal y, a continuación, introduzca el Nombre del usuario final deseado en la cuenta radial.
5. Elija Grant access (Conceder acceso).

## Paso 8: Compartir la cartera con el usuario final

El AWS Service Catalog administrador puede distribuir carteras con cuentas de usuario final mediante el uso account-to-account compartido o AWS Organizations compartido. En este tutorial compartirá su cartera con la organización desde la cuenta de administrador (cuenta central), que también es la cuenta de administración de la organización.

Para compartir el portafolio desde la cuenta central de administración

1. Abra la consola de AWS Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.

2. En la página Cartera, seleccione la cartera de bucket de S3. En el menú Accione, elija Compartir.
3. Seleccione AWS Organizations y, a continuación, filtre según su estructura organizativa.
4. En el panel Organización deAWS, seleccione la cuenta de usuario final (cuenta radial).

También puede seleccionar un Nodo raíz para compartir la cartera con toda la organización, una Unidad organizativa (OU) principal o una OU secundaria de la organización en función de la estructura de la organización. Para obtener más información, consulte [Uso compartido de carteras](#).

5. En el panel de Configuración de compartir, seleccione Compartir la entidad principal.
6. Elija Compartir.

Tras compartir correctamente la cartera con los usuarios finales, el siguiente paso consiste en verificar la experiencia del usuario final y aprovisionar el producto Terraform.

## Paso 4: Probar la experiencia del usuario final

Para comprobar que el usuario final puede obtener acceso correctamente a la vista de la consola del usuario final y lanzar el producto **Simple S3 bucket**, inicie sesión en AWS como ese usuario final y lleve a cabo las siguientes tareas.

Para comprobar que el usuario final puede obtener acceso a la consola del usuario final

- Abra la consola AWS Service Catalog en <https://console.aws.amazon.com/servicecatalog/> para ver:
  - Products: los productos que el usuario puede utilizar.
  - Provisioned products: los productos aprovisionados que el usuario ha lanzado.

Para verificar que el usuario final puede lanzar el producto Terraform

1. En la sección Productos de la consola, seleccione bucket Simple S3.
2. Elija Lanzar producto con el fin de iniciar el asistente para configurar el producto.
3. En la página Lanzar un bucket Simple S3, introduzca **Amazon S3 product** como nombre del producto aaprovisionado.
4. En la página Parámetros, escriba lo siguiente y, a continuación, elija Siguiente:

- `bucket_name` – Proporcione un nombre único para el bucket de Amazon S3. Por ejemplo, **terraform-s3-product**.
5. Seleccione Lanzar producto. La consola muestra la página de detalles de la pila para el lanzamiento del producto Amazon S3. El estado inicial del producto es Under change. AWS Service Catalog tarda varios minutos en lanzar el producto. Para ver el estado actual, actualice el navegador. Tras el lanzamiento exitoso del producto, el estado es Disponible.

AWS Service Catalog crea un nuevo bucket de Amazon S3 denominado **terraform-s3-product**.

## Paso 10: Monitorización de las operaciones de aprovisionamiento de Terraform

Si quieres supervisar las operaciones de aprovisionamiento, puedes revisar los CloudWatch registros de Amazon y cualquier flujo de trabajo AWS Step Functions de aprovisionamiento.

Hay dos máquinas de estados para el flujo de trabajo de aprovisionamiento:

- `ManageProvisionedProductStateMachine`: AWS Service Catalog invoca esta máquina de estados al aprovisionar un nuevo producto de Terraform y al actualizar un producto aprovisionado por Terraform existente.
- `TerminateProvisionedProductStateMachine` — AWS Service Catalog invoca esta máquina de estados al finalizar un producto aaprovisionado por Terraform existente.

Para ejecutar la máquina de estados de monitorización

1. Abra la consola de administración de AWS e inicie sesión como administrador en la cuenta central de administración donde está instalado el motor de aprovisionamiento Terraform.
2. Abra AWS Step Functions.
3. En el panel de navegación izquierdo, elija Máquinas de estado.
4. Elige. `ManageProvisionedProductStateMachine`
5. En la lista de Ejecuciones, introduzca el ID del producto aaprovisionado para localizar la ejecución.

 Note

AWS Service Catalog crea el ID del producto aprovisionado cuando usted aprovisiona el producto. El ID del producto aprovisionado tiene el siguiente formato: **pp-1111pwtn[ID number]**.

6. Elija un ID de ejecución.

En la página de Detalles de ejecución resultante, puede ver todos los pasos del flujo de trabajo de aprovisionamiento. También puede revisar los pasos fallidos para identificar la causa del error.

# Seguridad en AWS Service Catalog

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted 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 AWS los servicios en la AWS nube. AWS también le 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 cumplimiento aplicables AWS Service Catalog, consulte los [AWS servicios incluidos en el ámbito de aplicación por programa de cumplimiento](#)

- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted 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 le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS Service Catalog. Los siguientes temas muestran cómo configurarlo AWS Service Catalog para cumplir sus objetivos de seguridad y conformidad. También conocerá otros AWS servicios que le ayudan a supervisar y proteger sus AWS Service Catalog recursos.

## Temas

- [Protección de datos en AWS Service Catalog](#)
- [Administración de identidad y acceso en AWS Service Catalog](#)
- [Inicio de sesión y supervisión AWS Service Catalog](#)
- [Validación de conformidad para AWS Service Catalog](#)
- [Resiliencia en AWS Service Catalog](#)
- [Seguridad de la infraestructura en AWS Service Catalog](#)
- [Mejores prácticas de seguridad para AWS Service Catalog](#)

# Protección de datos en AWS Service Catalog

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

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las 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 multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS 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 módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte [Estándar de procesamiento de la información federal \(FIPS\) 140-2](#).

Se recomienda encarecidamente no 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 AWS Service Catalog o Servicios de AWS utiliza la consola, la API o los SDK. AWS CLI AWS 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, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

## Protección de los datos con el cifrado

### Cifrado en reposo

AWS Service Catalog utiliza buckets de Amazon S3 y bases de datos de Amazon DynamoDB cifradas en reposo mediante claves administradas por Amazon. Para obtener más información, consulte la información sobre cifrado en reposo proporcionada por Amazon S3 y Amazon DynamoDB.

### Cifrado en tránsito

AWS Service Catalog utiliza Transport Layer Security (TLS) y el cifrado por parte del cliente de la información en tránsito entre la persona que llama y AWS.

Puede acceder de forma privada a AWS Service Catalog las API desde su Amazon Virtual Private Cloud (Amazon VPC) mediante la creación de puntos de enlace de VPC. Con los puntos de enlace de la VPC, el enrutamiento entre la VPC y AWS Service Catalog lo gestiona la AWS red sin necesidad de una puerta de enlace a Internet, una puerta de enlace NAT o una conexión VPN.

La última generación de puntos de enlace de VPC que utiliza AWS Service Catalog está impulsada por AWS PrivateLink una AWS tecnología que permite la conectividad privada entre AWS servicios mediante interfaces de red elásticas con IP privadas en sus VPC.

## Administración de identidad y acceso en AWS Service Catalog

El acceso a las mismas requiere credenciales AWS Service Catalog. Esas credenciales deben tener permiso para acceder a AWS los recursos, como una AWS Service Catalog cartera o un producto. AWS Service Catalog se integra con AWS Identity and Access Management (IAM) para permitir conceder a AWS Service Catalog los administradores los permisos que necesitan para crear y gestionar productos, y conceder a los usuarios AWS Service Catalog finales los permisos que necesitan para lanzar productos y gestionar los productos aprovisionados. Estas políticas las crean y administran los administradores y los usuarios finales, AWS o de forma individual. Para controlar el acceso, se adjuntan las políticas a los usuarios, grupos y funciones que se utilizan con AWS Service Catalog.

## Público

Los permisos que tiene a través de AWS Identity and Access Management (IAM) pueden depender del rol que desempeñe en AWS Service Catalog.

Los permisos que tiene a través de AWS Identity and Access Management (IAM) pueden depender del rol que desempeñe en AWS Service Catalog.

Administrador: como AWS Service Catalog administrador, necesita acceso completo a la consola de administración y permisos de IAM que le permitan realizar tareas como la creación y administración de carteras y productos, la gestión de las restricciones y la concesión de acceso a los usuarios finales.

Usuario final: antes de que los usuarios finales puedan utilizar sus productos, debe concederles permisos que les permitan acceder a la consola de usuario AWS Service Catalog final. También pueden tener permiso para lanzar productos y administrar productos aprovisionados.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a AWS Service Catalog. Para ver ejemplos de políticas AWS Service Catalog basadas en la identidad que puede utilizar en IAM, consulte [the section called “AWS políticas gestionadas”](#)

## Ejemplos de políticas basadas en la identidad para AWS Service Catalog

### Temas

- [Acceso a la consola para los usuarios finales](#)
- [Acceso a los productos para los usuarios finales](#)
- [Ejemplos de políticas para administrar productos aprovisionados](#)

### Acceso a la consola para los usuarios finales

Las políticas **AWSServiceCatalogEndUserFullAccess** y **AWSServiceCatalogEndUserReadOnlyAccess** conceden acceso a la vista de consola de usuario final de AWS Service Catalog . Cuando un usuario que tiene alguna de estas políticas elige, AWS Service Catalog en la vista de la consola del usuario final AWS Management Console, los productos para los que tiene permiso de lanzamiento.

Antes de que los usuarios finales puedan lanzar correctamente un producto AWS Service Catalog al que les das acceso, debes proporcionarles permisos de IAM adicionales para que puedan utilizar

cada uno de los AWS recursos subyacentes de la AWS CloudFormation plantilla de un producto. Por ejemplo, si una plantilla de producto incluye Amazon Relational Database Service (Amazon RDS), debe conceder a los usuarios permisos de Amazon RDS para lanzar el producto.

Para obtener información sobre cómo permitir a los usuarios finales lanzar productos y, al mismo tiempo, aplicar los permisos de acceso mínimo a los recursos, consulte [AWS the section called “Uso de las restricciones”](#)

Si aplica la política **AWSServiceCatalogEndUserReadOnlyAccess**, los usuarios tendrán acceso a la consola del usuario final, pero no contarán con los permisos necesarios para lanzar productos y administrar productos aprovisionados. Puedes conceder estos permisos directamente a un usuario final mediante IAM, pero si quieres limitar el acceso de los usuarios finales a los AWS recursos, debes asociar la política a una función de lanzamiento. A continuación, se utiliza AWS Service Catalog para aplicar la función de lanzamiento a una restricción de lanzamiento del producto. Para obtener más información sobre la aplicación de funciones de lanzamiento, las limitaciones de estas últimas y un ejemplo de función de lanzamiento, consulte [Restricciones de lanzamiento AWS Service Catalog](#).

#### Note

Si concede a los usuarios permisos de IAM para los AWS Service Catalog administradores, aparecerá en su lugar la vista de la consola de administración. No conceda a los usuarios finales estos permisos a menos que desee que tengan acceso a la vista de la consola del administrador.

## Acceso a los productos para los usuarios finales

Antes de que los usuarios finales puedan utilizar un producto al que usted da acceso, debe proporcionarles permisos de IAM adicionales para que puedan utilizar cada uno de AWS los recursos subyacentes de la plantilla de AWS CloudFormation un producto. Por ejemplo, si una plantilla de producto incluye Amazon Relational Database Service (Amazon RDS), debe conceder a los usuarios permisos de Amazon RDS para lanzar el producto.

Si aplica la política **AWSServiceCatalogEndUserReadOnlyAccess**, los usuarios tendrán acceso a la vista de la consola del usuario final, pero no contarán con los permisos necesarios para lanzar productos y administrar productos aprovisionados. Puedes conceder estos permisos directamente a un usuario final en IAM, pero si quieres limitar el acceso de los usuarios finales a los AWS recursos, debes adjuntar la política a una función de lanzamiento. A continuación, se utiliza AWS Service

Catalog para aplicar la función de lanzamiento a una restricción de lanzamiento del producto. Para obtener más información sobre la aplicación de funciones de lanzamiento, las limitaciones de estas últimas y un ejemplo de función de lanzamiento, consulte [Restricciones de lanzamiento AWS Service Catalog](#).

## Ejemplos de políticas para administrar productos aprovisionados

Puede crear políticas personalizadas para ayudar a satisfacer los requisitos de seguridad de su organización. En los ejemplos siguientes se describe cómo personalizar el nivel de acceso a cada acción para los usuarios, roles y cuentas. Puede conceder acceso a los usuarios para consultar, actualizar, terminar y administrar solamente los productos aprovisionados que ha creado ese usuario o que otros han creado con su rol o desde la cuenta en la que han iniciado sesión. Este acceso es jerárquico, es decir, la concesión de acceso en el nivel de cuenta también concede acceso en los niveles de función y de usuario, mientras que agregar el acceso en el nivel de función también concede acceso en el nivel de usuario, pero no en el nivel de cuenta. Puede especificarlos en el JSON de la política mediante un bloque `Condition` como `accountLevel`, `roleLevel` o `userLevel`.

Estos ejemplos también se aplican a los niveles de acceso de las operaciones de escritura de la AWS Service Catalog API: `UpdateProvisionedProduct` y `TerminateProvisionedProduct`, y, las operaciones de lectura: `DescribeRecordScanProvisionedProducts`, y `ListRecordHistory`. Las operaciones `ScanProvisionedProducts` y `ListRecordHistory` de la API utilizan `AccessLevelFilterKey` como entrada y los valores de esa clave se corresponden con los niveles del bloque `Condition` que abordamos aquí (`accountLevel` equivale al valor "Account" de `AccessLevelFilterKey`, `roleLevel` al valor "Role" y `userLevel` al valor "User"). Para obtener más información, consulte la [Guía para desarrolladores de Service Catalog](#).

### Ejemplos

- [Acceso pleno de administración a los productos aprovisionados](#)
- [Acceso de usuario final a los productos aprovisionados](#)
- [Acceso parcial de administración a los productos aprovisionados](#)

### Acceso pleno de administración a los productos aprovisionados

La siguiente política permite acceso pleno de lectura y escritura a los productos aprovisionados y a los registros del catálogo en el nivel de cuenta.

```
{
```

```

"Version":"2012-10-17",
"Statement":[
  {
    "Effect":"Allow",
    "Action":[
      "servicelog:*"
    ],
    "Resource":"*",
    "Condition": {
      "StringEquals": {
        "servicelog:accountLevel": "self"
      }
    }
  }
]
}

```

Esta política equivale funcionalmente a la siguiente política:

```

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

```

No especificar un Condition bloque en ninguna política para AWS Service Catalog se trata de la misma manera que especificar el "servicelog:accountLevel" acceso. Tenga en cuenta que el acceso accountLevel incluye los accesos roleLevel y userLevel.

### Acceso de usuario final a los productos aprovisionados

La siguiente política restringe el acceso a las operaciones de lectura y escritura exclusivamente a los productos aprovisionados y a los registros asociados creados por el usuario actual.

```

{

```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "servicecatalog:DescribeProduct",
      "servicecatalog:DescribeProductView",
      "servicecatalog:DescribeProvisioningParameters",
      "servicecatalog:DescribeRecord",
      "servicecatalog:ListLaunchPaths",
      "servicecatalog:ListRecordHistory",
      "servicecatalog:ProvisionProduct",
      "servicecatalog:ScanProvisionedProducts",
      "servicecatalog:SearchProducts",
      "servicecatalog:TerminateProvisionedProduct",
      "servicecatalog:UpdateProvisionedProduct"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "servicecatalog:userLevel": "self"
      }
    }
  }
]
}

```

## Acceso parcial de administración a los productos aprovisionados

Las dos políticas que aparecen a continuación, si se aplican al mismo usuario, permiten lo que podríamos denominar un tipo de acceso de administrador "parcial", pues proporcionan acceso pleno de solo lectura y acceso de escritura limitado. Esto significa que el usuario puede consultar cualquier producto aprovisionado o registro asociado en la cuenta del catálogo, pero no puede realizar ninguna acción en ningún producto aprovisionado ni registro que no sean de su propiedad.

La primera política permite al usuario obtener acceso a las operaciones de escritura en los productos aprovisionados que el propio usuario actual ha creado, pero no a los que han creado otros usuarios. La segunda política agrega acceso pleno a las operaciones de lectura en los productos aprovisionados creados por todos (usuario, función o cuenta).

```

{
  "Version": "2012-10-17",

```

```

"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "servicecatalog:DescribeProduct",
      "servicecatalog:DescribeProductView",
      "servicecatalog:DescribeProvisioningParameters",
      "servicecatalog:ListLaunchPaths",
      "servicecatalog:ProvisionProduct",
      "servicecatalog:SearchProducts",
      "servicecatalog:TerminateProvisionedProduct",
      "servicecatalog:UpdateProvisionedProduct"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "servicecatalog:userLevel": "self"
      }
    }
  }
]
}

```

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "servicecatalog:DescribeRecord",
        "servicecatalog:ListRecordHistory",
        "servicecatalog:ScanProvisionedProducts"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "servicecatalog:accountLevel": "self"
        }
      }
    }
  ]
}

```

## AWS políticas administradas para AWS Service Catalog AppRegistry

### AWS política gestionada: **AWSServiceCatalogAdminFullAccess**

Puede adjuntarla `AWSServiceCatalogAdminFullAccess` a sus entidades de IAM. AppRegistry también vincula esta política a un rol de servicio que le permite AppRegistry realizar acciones en su nombre.

Esta política concede permisos *administrativos* que permiten el acceso total a la vista de la consola de administración y concede permisos para crear y administrar productos y carteras.

#### Detalles de los permisos

Esta política incluye los siguientes permisos.

- `servicecatalog`— Permite a los directores disponer de todos los permisos necesarios para acceder a la consola de administración y la posibilidad de crear y gestionar carteras y productos, gestionar las restricciones, conceder acceso a los usuarios finales y realizar otras tareas administrativas desde dentro. AWS Service Catalog
- `cloudformation`— Permite disponer de AWS Service Catalog todos los permisos necesarios para enumerar, leer, escribir y etiquetar AWS CloudFormation pilas.
- `config`— Permite permisos AWS Service Catalog limitados a carteras, productos y productos provisionados mediante. AWS Config
- `iam`: concede a las entidades principales todos los permisos necesarios para ver y crear los usuarios, grupos o roles del servicio necesarios para crear y administrar productos y carteras.
- `ssm`— Permite AWS Service Catalog AWS Systems Manager enumerar y leer los documentos de Systems Manager en la AWS cuenta corriente y AWS la región.

Ver la política: [AWSServiceCatalogAdminFullAccess](#).

### AWS política gestionada: **AWSServiceCatalogAdminReadOnlyAccess**

Puede adjuntarla `AWSServiceCatalogAdminReadOnlyAccess` a sus entidades de IAM. AppRegistry también vincula esta política a un rol de servicio que le permite AppRegistry realizar acciones en su nombre.

Esta política otorga permisos de *solo lectura* para acceder a la vista de la consola de administración. Esta política no concede acceso para crear ni administrar productos y carteras.

## Detalles de los permisos

Esta política incluye los siguientes permisos.

- `servicecatalog`: permite a las entidades principales permisos de solo lectura para acceder a la vista de la consola de administración.
- `cloudformation`— Permite permisos AWS Service Catalog limitados para enumerar y leer AWS CloudFormation pilas.
- `config`— Permite permisos AWS Service Catalog limitados a carteras, productos y productos aprovisionados mediante. AWS Config
- `iam`: permite a las entidades principales tener permisos limitados para ver los usuarios, grupos o roles del servicio necesarios para crear y administrar productos y carteras.
- `ssm`— Permite AWS Service Catalog AWS Systems Manager enumerar y leer los documentos de Systems Manager en la AWS cuenta corriente y AWS la región.

Ver la política: [AWSServiceCatalogAdminReadOnlyAccess](#).

## AWS política gestionada: **AWSServiceCatalogEndUserFullAccess**

Puede adjuntarla `AWSServiceCatalogEndUserFullAccess` a sus entidades de IAM. `AppRegistry` también vincula esta política a un rol de servicio que le permite `AppRegistry` realizar acciones en su nombre.

Esta política concede a los *colaboradores* permisos que permiten el acceso total a la vista de la consola del usuario final y concede permisos para lanzar productos y gestionar los productos aprovisionados.

## Detalles de los permisos

Esta política incluye los siguientes permisos.

- `servicecatalog`: concede acceso pleno a la vista de la consola del usuario final, así como permiso para lanzar los productos y administrar los productos aprovisionados.
- `cloudformation`— Permite permisos AWS Service Catalog completos para enumerar, leer, escribir y etiquetar AWS CloudFormation pilas.
- `config`— Permite permisos AWS Service Catalog limitados para enumerar y leer detalles sobre carteras, productos y productos aprovisionados a través de. AWS Config

- `ssm`— Permite AWS Service Catalog AWS Systems Manager leer documentos de Systems Manager en la AWS cuenta corriente y AWS la región.

Ver la política: [AWSServiceCatalogEndUserFullAccess](#).

### AWS política gestionada: **AWSServiceCatalogEndUserReadOnlyAccess**

Puede adjuntarla `AWSServiceCatalogEndUserReadOnlyAccess` a sus entidades de IAM. `AppRegistry` también vincula esta política a un rol de servicio que le permite `AppRegistry` realizar acciones en su nombre.

Esta política concede permisos de *solo lectura* que permiten el acceso de solo lectura a la vista de la consola del usuario final. Esta política no concede permiso para lanzar productos ni administrar productos aprovisionados.

#### Detalles de los permisos

Esta política incluye los siguientes permisos.

- `servicecatalog`: permite a las entidades principales permisos de solo lectura para acceder a la vista de la consola del usuario final.
- `cloudformation`— Permite permisos AWS Service Catalog limitados para enumerar y leer AWS CloudFormation pilas.
- `config`— Permite permisos AWS Service Catalog limitados para enumerar y leer detalles sobre carteras, productos y productos aprovisionados mediante. AWS Config
- `ssm`— Permite AWS Service Catalog AWS Systems Manager leer documentos de Systems Manager en la AWS cuenta corriente y AWS la región.

Ver la política: [AWSServiceCatalogEndUserReadOnlyAccess](#).

### AWS política gestionada: **AWSServiceCatalogSyncServiceRolePolicy**

AWS Service Catalog asocia esta política a la función

`AWSServiceRoleForServiceCatalogSync` vinculada al servicio (SLR), lo que permite AWS Service Catalog sincronizar las plantillas de un repositorio externo con los productos. AWS Service Catalog

Esta política concede permisos que permiten un acceso limitado a AWS Service Catalog las acciones (por ejemplo, las llamadas a la API) y a otras acciones de AWS servicio de las que dependa. AWS Service Catalog

## Detalles de los permisos

Esta política incluye los siguientes permisos.

- `servicecatalog`— Permite que la función de sincronización de AWS Service Catalog artefactos tenga acceso limitado a las API AWS Service Catalog públicas.
- `codeconnections`— Permite que la función de sincronización de AWS Service Catalog artefactos tenga acceso limitado a las API CodeConnections públicas.
- `cloudformation`— Permite que la función de sincronización de AWS Service Catalog artefactos tenga acceso limitado a las API AWS CloudFormation públicas.

Ver la política: [AWSServiceCatalogSyncServiceRolePolicy](#).

## Detalles del rol vinculado al servicio

AWS Service Catalog utiliza los detalles de permisos anteriores para el rol `AWSServiceRoleForServiceCatalogSync` vinculado al servicio que se crea cuando un usuario crea o actualiza un AWS Service Catalog producto que lo utiliza. CodeConnections Puede modificar esta política mediante la AWS CLI, la AWS API o mediante la AWS Service Catalog consola. Para obtener más información sobre cómo crear, editar y eliminar roles vinculados a servicios, consulte [Uso de funciones vinculadas a servicios \(SLR\) para AWS Service Catalog](#).

Los permisos incluidos en la función `AWSServiceRoleForServiceCatalogSync` vinculada al servicio permiten AWS Service Catalog realizar las siguientes acciones en nombre del cliente.

- `servicecatalog:ListProvisioningArtifacts`— Permite que la función de sincronización de AWS Service Catalog artefactos enumere los artefactos de aprovisionamiento de un AWS Service Catalog producto determinado que están sincronizados con un archivo de plantilla de un repositorio.
- `servicecatalog:DescribeProductAsAdmin`— Permite que la función de sincronización de AWS Service Catalog artefactos utilice la `DescribeProductAsAdmin` API para obtener detalles de un AWS Service Catalog producto y los artefactos aprovisionados asociados que se sincronizan con un archivo de plantilla de un repositorio. El rol de sincronización de artefactos

utiliza el resultado de esta llamada para verificar el límite de Service Quotas del producto para el aprovisionamiento de artefactos.

- `servicecatalog:DeleteProvisioningArtifact`— Permite que la función de sincronización de AWS Service Catalog artefactos elimine un artefacto aprovisionado.
- `servicecatalog:ListServiceActionsForProvisioningArtifact`— Permite que la función de sincronización de AWS Service Catalog artefactos determine si las acciones de servicio están asociadas a un artefacto de aprovisionamiento y garantizar que el artefacto de aprovisionamiento no se elimine si hay una acción de servicio asociada.
- `servicecatalog:DescribeProvisioningArtifact`— Permite que la función de sincronización de AWS Service Catalog artefactos recupere detalles de la `DescribeProvisioningArtifact` API, incluido el ID de confirmación, que se proporciona en el resultado. `SourceRevisionInfo`
- `servicecatalog>CreateProvisioningArtifact`— Permite que la función de sincronización de AWS Service Catalog artefactos cree un nuevo artefacto aprovisionado si se detecta un cambio (por ejemplo, si se confirma un git-push) en el archivo de plantilla fuente del repositorio externo.
- `servicecatalog:UpdateProvisioningArtifact`— Permite que la función de sincronización de AWS Service Catalog artefactos actualice el artefacto aprovisionado para un producto conectado o sincronizado.
- `codeconnections:UseConnection`— Permite que la función de sincronización de AWS Service Catalog artefactos utilice la conexión existente para actualizar y sincronizar un producto.
- `cloudformation:ValidateTemplate`— Permite que la función de sincronización de AWS Service Catalog artefactos tenga acceso limitado AWS CloudFormation para validar el formato de la plantilla que se está utilizando en el repositorio externo y AWS CloudFormation comprobar si es compatible con la plantilla.

AWS política gestionada:

### **AWSServiceCatalogOrgsDataSyncServiceRolePolicy**

AWS Service Catalog adjunta esta política a la función

`AWSServiceRoleForServiceCatalogOrgsDataSync` vinculada al servicio (SLR), lo que permite AWS Service Catalog sincronizarla con. AWS Organizations

Esta política concede permisos que permiten un acceso limitado a AWS Service Catalog las acciones (por ejemplo, las llamadas a la API) y a otras acciones de AWS servicio que dependan de ellas. AWS Service Catalog

## Detalles de los permisos

Esta política incluye los siguientes permisos.

- `organizations`— Permite que la función AWS Service Catalog de sincronización de datos limite el acceso a las API AWS Organizations públicas.

Ver la política: [AWSServiceCatalogOrgsDataSyncServiceRolePolicy](#).

## Detalles del rol vinculado al servicio

AWS Service Catalog utiliza los detalles de permisos anteriores para el rol `AWSServiceRoleForServiceCatalogOrgsDataSync` vinculado al servicio que se crea cuando un usuario habilita el acceso a una cartera AWS Organizations compartida o crea una cartera compartida. Puede modificar esta política mediante la AWS CLI, la AWS API o mediante la AWS Service Catalog consola. Para obtener más información sobre cómo crear, editar y eliminar roles vinculados a servicios, consulte [Uso de funciones vinculadas a servicios \(SLR\) para AWS Service Catalog](#).

Los permisos incluidos en la función `AWSServiceRoleForServiceCatalogOrgsDataSync` vinculada al servicio permiten AWS Service Catalog realizar las siguientes acciones en nombre del cliente.

- `organizations:DescribeAccount`— Permite que la AWS Service Catalog función de sincronización de datos de Organizations recupere información AWS Organizations relacionada con la cuenta especificada.
- `organizations:DescribeOrganization`— Permite que la función AWS Service Catalog Organizations Data Sync recupere información sobre la organización a la que pertenece la cuenta del usuario.
- `organizations:ListAccounts`— Permite que la función AWS Service Catalog Organizations Data Sync enumere las cuentas de la organización del usuario.
- `organizations:ListChildren`— Permite que la función AWS Service Catalog Organizations Data Sync enumere todas las unidades organizativas (UO) o cuentas que se encuentran en la OU principal o raíz especificada.
- `organizations:ListParents`— Permite que la AWS Service Catalog función de sincronización de datos de Organizations enumere la raíz o las unidades organizativas que actúan como matrices inmediatas de la unidad organizativa o cuenta secundaria especificada.

- `organizations:ListAWSServiceAccessForOrganization`— Permite que la AWS Service Catalog función de sincronización de datos de Organizations recupere una lista de los AWS servicios que el usuario ha permitido integrar con su organización.

## Políticas obsoletas

Las siguientes políticas administradas han quedado obsoletas:

- `ServiceCatalogAdminFullAccess`— Úselo `AWSServiceCatalogAdminFullAccess` en su lugar.
- `ServiceCatalogAdminReadOnlyAccess`— Úselo `AWSServiceCatalogAdminReadOnlyAccess` en su lugar.
- `ServiceCatalogEndUserFullAccess`— Úselo `AWSServiceCatalogEndUserFullAccess` en su lugar.
- `ServiceCatalogEndUserAccess`— Úselo `AWSServiceCatalogEndUserReadOnlyAccess` en su lugar.

Utilice el siguiente procedimiento para asegurarse de que se usan las políticas actuales para conceder permisos a los administradores y los usuarios finales.

Para migrar de las políticas obsoletas a las políticas actuales, consulte [Añadir y eliminar permisos de identidad de IAM](#) en la Guía del usuario de AWS Identity and Access Management .

## AppRegistry actualizaciones de las políticas AWS gestionadas

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas AppRegistry desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del AppRegistry documento.

Cambio	Descripción	Fecha
<a href="#">AWSServiceCatalogSyncServiceRolePolicy</a> — Actualizar la política gestionada	AWS Service Catalog actualizó la <code>AWSServiceCatalogSyncServiceRolePolicy</code> política para cambiarla <code>codestar-connections</code> a <code>codeconnections</code> .	7 de mayo de 2024

Cambio	Descripción	Fecha
<p><a href="#">AWSServiceCatalogAdminFullAccess</a>— Actualizar la política gestionada</p>	<p>AWS Service Catalog actualizó la <code>AWSServiceCatalogAdminFullAccess</code> política para incluir los permisos necesarios para que el AWS Service Catalog administrador pueda crear el rol <code>AWSServiceRoleForServiceCatalogOrgsDataSync</code> vinculado al servicio (SLR) en su cuenta.</p>	<p>14 de abril de 2023</p>
<p><a href="#">AWSServiceCatalogOrgsDataSyncServiceRolePolicy</a> – Nueva política administrada</p>	<p>AWS Service Catalog agregó el <code>AWSServiceCatalogOrgsDataSyncServiceRolePolicy</code>, que está asociado al rol <code>AWSServiceRoleForServiceCatalogOrgsDataSync</code> vinculado al servicio (SLR), lo que permite sincronizarlo con. AWS Service Catalog AWS Organizations Esta política permite el acceso limitado a AWS Service Catalog las acciones (por ejemplo, las llamadas a la API) y a otras acciones de AWS servicio que AWS Service Catalog dependan de ellas.</p>	<p>14 de abril de 2023</p>

Cambio	Descripción	Fecha
<p><a href="#">AWSServiceCatalogAdminFullAccess</a>— Actualizar la política gestionada</p>	<p>AWS Service Catalog actualizó la <code>AWSServiceCatalogAdminFullAccess</code> política para incluir todos los permisos del AWS Service Catalog administrador y crear compatibilidad con AppRegistry.</p>	<p>12 de enero de 2023</p>
<p><a href="#">AWSServiceCatalogSyncServiceRolePolicy</a> – Nueva política administrada</p>	<p>AWS Service Catalog agregó la <code>AWSServiceCatalogSyncServiceRolePolicy</code> política, que está asociada a la función <code>AWSServiceRoleForServiceCatalogSync</code> vinculada al servicio (SLR). Esta política permite sincronizar AWS Service Catalog las plantillas de un repositorio externo con los productos. AWS Service Catalog</p>	<p>18 de noviembre de 2022</p>
<p><a href="#">AWSServiceRoleForServiceCatalogSync</a>— Nuevo rol vinculado a un servicio</p>	<p>AWS Service Catalog agregó el rol <code>AWSServiceRoleForServiceCatalogSync</code> vinculado al servicio (SLR). Esta función es necesaria AWS Service Catalog para usar <code>CodeConnections</code> y crear, actualizar y describir los artefactos de AWS Service Catalog aprovisionamiento de un producto.</p>	<p>18 de noviembre de 2022</p>

Cambio	Descripción	Fecha
<a href="#">AWSServiceCatalogAdminFullAccess</a> — Política gestionada actualizada	<p>AWS Service Catalog actualizó la <code>AWSServiceCatalogAdminFullAccess</code> política para incluir todos los permisos necesarios para un AWS Service Catalog administrador. La política identifica las acciones específicas que el administrador puede realizar en todos AWS Service Catalog los recursos, como crear, describir, eliminar y más. Además, la política se modificó para admitir una función lanzada recientemente, el control de acceso basado en atributos (ABAC) para AWS Service Catalog. ABAC le permite utilizar la política <code>AWSServiceCatalogAdminFullAccess</code> como plantilla para permitir o denegar acciones en los recursos AWS Service Catalog en función de las etiquetas. Para obtener más información sobre ABAC, consulte <a href="#">¿Qué es ABAC para AWS?</a> en AWS Identity and Access Management.</p>	30 de septiembre de 2022

Cambio	Descripción	Fecha
AppRegistry comenzó a rastrear los cambios	AppRegistry comenzó a realizar un seguimiento de los cambios de sus políticas AWS gestionadas.	15 de septiembre de 2022

## Uso de roles vinculados a servicios de AWS Service Catalog

AWS Service Catalog [usa roles vinculados al AWS Identity and Access Management servicio \(IAM\)](#).

Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. AWS Service Catalog Los roles vinculados al servicio están predefinidos AWS Service Catalog e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio facilita la configuración AWS Service Catalog , ya que no es necesario añadir manualmente los permisos necesarios. AWS Service Catalog define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS Service Catalog puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. Esto protege sus AWS Service Catalog recursos porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

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 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 de **AWSServiceRoleForServiceCatalogSync**

AWS Service Catalog puede usar el rol vinculado al servicio denominado **AWSServiceRoleForServiceCatalogSync**: este rol vinculado al servicio es necesario para AWS Service Catalog poder usar CodeConnections y crear, actualizar y describir los artefactos de aprovisionamiento para un producto. AWS Service Catalog

El rol vinculado al servicio `AWSServiceRoleForServiceCatalogSync` depende de los siguientes servicios para asumir el rol:

- `sync.servicecatalog.amazonaws.com`

La política de permisos de roles denominada `AWSServiceCatalogSyncServiceRolePolicy` permite AWS Service Catalog realizar las siguientes acciones en los recursos especificados:

- Acción: `Connection` en `CodeConnections`
- Acción: `Create, Update, and Describe` activada `ProvisioningArtifact` para un AWS Service Catalog producto

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte [Permisos de roles vinculados a servicios](#) en la Guía del usuario de IAM.

Creación del rol **`AWSServiceRoleForServiceCatalogSync`** vinculado al servicio

No es necesario crear manualmente el rol `AWSServiceRoleForServiceCatalogSync` vinculado al servicio. AWS Service Catalog crea automáticamente el rol vinculado al servicio cuando lo estableces `CodeConnections` en la AWS Management Console, la o la API AWS CLI. AWS

#### Important

Este rol vinculado a servicios puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol. Además, si utilizabas el AWS Service Catalog servicio antes del 18 de noviembre de 2022, cuando comenzó a admitir funciones vinculadas al servicio, entonces AWS Service Catalog creaste la `AWSServiceRoleForServiceCatalogSync` función en tu cuenta. Para obtener más información, consulte [Un nuevo rol ha aparecido en mi cuenta de IAM](#).

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando lo estableces `CodeConnections`, vuelve a AWS Service Catalog crear el rol vinculado al servicio para ti.

También puedes usar la consola de IAM para crear un rol vinculado a un servicio con el caso de uso de los productos sincronizados. AWS Service Catalog En la API AWS CLI

o en la AWS API, cree una función vinculada a un servicio con el nombre del servicio. `sync.servicecatalog.amazonaws.com` Para obtener más información, consulte [Crear un rol vinculado a un servicio](#) en la Guía del usuario de IAM. Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

## Permisos de roles vinculados a servicios de **AWSServiceRoleForServiceCatalogOrgsDataSync**

AWS Service Catalog puede usar el rol vinculado al servicio denominado **AWSServiceRoleForServiceCatalogOrgsDataSync**: este rol vinculado al servicio es necesario para que AWS Service Catalog las organizaciones estén sincronizadas con él. AWS Organizations

El rol vinculado al servicio `AWSServiceRoleForServiceCatalogOrgsDataSync` depende de los siguientes servicios para asumir el rol:

- `orgsdatasync.servicecatalog.amazonaws.com`

El rol `AWSServiceRoleForServiceCatalogOrgsDataSync` vinculado al servicio requiere que utilice la siguiente política de confianza además de la [política administrada](#) `AWSServiceCatalogOrgsDataSyncServiceRolePolicy`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "orgsdatasync.servicecatalog.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

La política de permisos de roles denominada `AWSServiceCatalogOrgsDataSyncServiceRolePolicy` permite AWS Service Catalog realizar las siguientes acciones en los recursos especificados:

- Acción: DescribeAccount, DescribeOrganization y ListAWSServiceAccessForOrganization en Organizations accounts
- Acción: ListAccounts, ListChildren y ListParent en Organizations accounts

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte [Permisos de roles vinculados a servicios](#) en la Guía del usuario de IAM.

Creación del rol **AWSServiceRoleForServiceCatalogOrgsDataSync** vinculado al servicio

No es necesario crear manualmente el rol AWSServiceRoleForServiceCatalogOrgsDataSync vinculado al servicio. AWS Service Catalog considera su acción de habilitar [Compartiendo con AWS Organizations](#) o [Uso compartido de carteras](#) dar permiso AWS Service Catalog para crear una SLR en segundo plano en su nombre.

AWS Service Catalog te crea automáticamente el rol vinculado al servicio cuando lo solicitas EnableAWSOrganizationsAccess o CreatePortfolioShare en la AWS Management Console, la o la AWS CLI API. AWS

#### Important

Este rol vinculado a servicios puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol. Para obtener más información, consulte [Un nuevo rol ha aparecido en mi cuenta de IAM](#).

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al pedir EnableAWSOrganizationsAccess o CreatePortfolioShare, AWS Service Catalog se encarga de volver crear automáticamente la función vinculada al servicio.

## Modificación de un rol vinculado a servicios de AWS Service Catalog

AWS Service Catalog no le permite editar los roles AWSServiceRoleForServiceCatalogSync o los roles vinculados al AWSServiceRoleForServiceCatalogOrgsDataSync servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con 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 de AWS Service Catalog

Puede utilizar la consola de IAM, la AWS CLI o la AWS API para eliminar manualmente la `AWSServiceRoleForServiceCatalogSync` `AWSServiceRoleForServiceCatalogOrgsDataSync` SLR. Para ello, primero debe eliminar manualmente todos los recursos que utilizan la función vinculada al servicio (por ejemplo, cualquier AWS Service Catalog producto que esté sincronizado con un repositorio externo) y, a continuación, la función vinculada al servicio se puede eliminar manualmente.

## Regiones admitidas para los roles vinculados a un servicio de AWS Service Catalog

AWS Service Catalog admite el uso de funciones vinculadas al servicio en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte [Puntos de enlace y regiones de AWS](#).

Nombres de las regiones	Identidad de la región	Support en AWS Service Catalog
Este de EE. UU. (Norte de Virginia)	us-east-1	Sí
Este de EE. UU. (Ohio)	us-east-2	Sí
Oeste de EE. UU. (Norte de California)	us-west-1	Sí
Oeste de EE. UU. (Oregón)	us-west-2	Sí
África (Ciudad del Cabo)	af-south-1	Sí
Asia-Pacífico (Hong Kong)	ap-east-1	Sí
Asia-Pacífico (Yakarta)	ap-southeast-3	Sí
Asia Pacífico (Mumbai)	ap-south-1	Sí
Asia Pacífico (Osaka)	ap-northeast-3	Sí
Asia Pacífico (Seúl)	ap-northeast-2	Sí
Asia-Pacífico (Singapur)	ap-southeast-1	Sí
Asia Pacífico (Sídney)	ap-southeast-2	Sí

Nombres de las regiones	Identidad de la región	Support en AWS Service Catalog
Asia-Pacífico (Tokio)	ap-northeast-1	Sí
Canadá (centro)	ca-central-1	Sí
Europa (Fráncfort)	eu-central-1	Sí
Europa (Irlanda)	eu-west-1	Sí
Europa (Londres)	eu-west-2	Sí
Europa (Milán)	eu-south-1	Sí
Europa (París)	eu-west-3	Sí
Europa (Estocolmo)	eu-north-1	Sí
Medio Oriente (Baréin)	me-south-1	Sí
América del Sur (São Paulo)	sa-east-1	Sí
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	No
AWS GovCloud (Estados Unidos-Oeste)	us-gov-west-1	No

## Solución de problemas AWS Service Catalog de identidad y acceso

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas más comunes que pueden surgir al trabajar con AWS Service Catalog un IAM.

### Temas

- [No estoy autorizado a realizar ninguna acción en AWS Service Catalog](#)
- [No tengo autorización para realizar iam:PassRole](#)
- [Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis recursos AWS Service Catalog](#)

## No estoy autorizado a realizar ninguna acción en AWS Service Catalog

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. El siguiente ejemplo de error se produce cuando el usuario mateojackson intenta usar la consola para ver detalles sobre un my-example-widget recurso ficticio pero no tiene los permisos ficticiosaws:GetWidget.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
aws:GetWidget on resource: my-example-widget
```

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso my-example-widget mediante la acción aws:GetWidget.

## No tengo autorización para realizar **iam:PassRole**

Si recibe un error que indica que no está autorizado para llevar a cabo la acción iam:PassRole, debe ponerse en contacto con su administrador para recibir ayuda. Su administrador es la persona que le facilitó su nombre de usuario y contraseña. Pida a la persona que actualice sus políticas de forma que pueda transferir un rol a AWS Service Catalog.

Algunos AWS servicios 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 un usuario denominado marymajor intenta utilizar la consola para realizar una acción en AWS Service Catalog. Sin embargo, la acción requiere que el servicio cuente con permisos otorgados por 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, Mary pide a su administrador que actualice sus políticas para poder realizar la acción iam:PassRole

## Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis recursos AWS Service Catalog

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 AWS Service Catalog es compatible con estas funciones, consulte AWS Identity and Access ManagementAWS Service Catalog la Guía AWS Service Catalog del administrador.](#)
- Para obtener información sobre cómo proporcionar acceso a sus recursos en todas AWS las cuentas de su propiedad, consulte [Proporcionar acceso a un usuario de IAM en otra AWS cuenta de su](#) propiedad en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a AWS cuentas de terceros, consulta Cómo [proporcionar acceso a AWS cuentas 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 sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte [Cómo los roles de IAM difieren de las políticas basadas en recursos](#) en la Guía del usuario de IAM.

## Control de acceso

una AWS Service Catalog cartera proporciona a sus administradores un nivel de control de acceso para sus grupos de usuarios finales. Cuando añada usuarios a una cartera de productos, ellos mismos podrán explorar y lanzar cualquiera de los productos de la cartera. Para obtener más información, consulte [the section called “Administración de carteras”](#).

## Restricciones

Las restricciones controlan qué reglas se aplican a los usuarios finales al lanzar un producto de una cartera específica. Úselas para aplicar límites a los productos para el control de costos o de

dirección. Para obtener más información acerca de las restricciones, consulte [the section called “Uso de las restricciones”](#).

AWS Service Catalog las restricciones de lanzamiento le proporcionan un mayor control sobre los permisos que necesita el usuario final. Cuando su administrador crea una restricción de lanzamiento para un producto de una cartera, la restricción de lanzamiento asocia un ARN de rol que se utiliza cuando sus usuarios finales lanzan el producto desde esa cartera. Con este patrón, puede controlar el acceso a la creación AWS de recursos. Para obtener más información, consulte [the section called “Restricciones de lanzamiento”](#).

## Inicio de sesión y supervisión AWS Service Catalog

AWS Service Catalog se integra con AWS CloudTrail un servicio que captura todas las llamadas a la AWS Service Catalog API y entrega los archivos de registro a un bucket de Amazon S3 que usted especifique. Para obtener más información, consulte [Registrar llamadas a la AWS Service Catalog API con CloudTrail](#).

También puede utilizar restricciones de notificación para configurar notificaciones de Amazon SNS sobre eventos de pila. Para obtener más información, consulte [the section called “Restricciones de notificación”](#).

## Validación de conformidad para AWS Service Catalog

Los auditores externos evalúan la seguridad y el cumplimiento AWS Service Catalog como parte de varios programas de AWS cumplimiento, incluidos los siguientes:

- Controles del Sistema y Organizaciones (System and Organization Controls, SOC)
- La norma de seguridad de datos del sector de pagos con tarjeta (PCI DSS)
- Programa Federal de Administración de Riesgos y Autorizaciones (Federal Risk and Authorization Management Program, FedRAMP)
- Ley de Portabilidad y Responsabilidad de Seguros Médicos de EE. UU (Health Insurance Portability and Accountability Act, HIPAA).

Para obtener una lista de AWS los servicios incluidos en el ámbito de los programas de conformidad específicos, consulte [Servicios de AWS incluidos en el ámbito de aplicación por programa de conformidad](#). Para obtener información general, consulte Programas de [AWS conformidad](#), [Programas AWS](#) y .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#).

Su responsabilidad de conformidad al AWS Service Catalog utilizarlos depende de la confidencialidad de sus datos, de los objetivos de cumplimiento de su empresa y de 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 la seguridad y el cumplimiento. AWS
- Documento técnico sobre [cómo diseñar una arquitectura para la seguridad y el cumplimiento de la HIPAA: este documento técnico describe cómo las](#) empresas pueden utilizar para crear aplicaciones que cumplan con la HIPAA. AWS
- [AWS Recursos de conformidad](#): este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- [AWS Config](#)— Este AWS servicio evalúa en qué medida las configuraciones de sus recursos cumplen con las prácticas internas, las directrices del sector y las normativas.
- [AWS Security Hub](#)— Este AWS servicio proporciona una visión integral del estado de su seguridad AWS que le ayuda a comprobar el cumplimiento de los estándares y las mejores prácticas del sector de la seguridad.

## Resiliencia en AWS Service Catalog

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. 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.

[Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura global.AWS](#)

Además de la infraestructura AWS global, AWS Service Catalog ofrece acciones de AWS Service Catalog autoservicio. Con las acciones de autoservicio, los clientes pueden reducir el mantenimiento administrativo y la formación técnica de los usuarios finales a la vez que se cumplen las medidas

de conformidad y seguridad. Con las acciones de autoservicio, como administrador, puede permitir a los usuarios finales que realicen tareas operativas (como copia de seguridad y restauración), solucionen problemas, ejecuten comandos aprobados y soliciten permisos en AWS Service Catalog. Para obtener más información, consulte [the section called “Uso de acciones de servicio”](#).

## Seguridad de la infraestructura en AWS Service Catalog

Como servicio gestionado, AWS Service Catalog 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.

Utiliza las llamadas a la API AWS publicadas para acceder a AWS Service Catalog través de la red. Los clientes deben admitir lo siguiente:

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

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

Con AWS Service Catalog, puede controlar las regiones en las que se almacenan los datos. Las carteras y los productos solo están disponibles en las regiones en las que haya decidido incluirlos. Puede utilizar la API CopyProduct para copiar un producto a otra región.

## Mejores prácticas de seguridad para AWS Service Catalog

AWS Service Catalog proporciona una serie de características de seguridad que debe tener en cuenta a la hora de desarrollar e implementar sus propias políticas de seguridad. Las siguientes prácticas recomendadas son directrices generales y no constituyen 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.

Puede definir reglas para limitar los valores de los parámetros que un usuario especifica cuando lanza un producto. Estas reglas se llaman restricciones de plantilla porque restringen el modo en que se implementa la plantilla de AWS CloudFormation del producto. Utilice un editor simple para crear estas restricciones, que puede aplicar a cada uno de los productos.

AWS Service Catalog aplica restricciones al aprovisionar un producto nuevo o al actualizar un producto que ya está en uso. De todas las restricciones aplicadas en el producto y la cartera de productos se aplica siempre la más restrictiva. Por ejemplo, pensemos en una situación en la que el producto permita que se lancen todas las instancias Amazon EC2 y la cartera de productos tenga dos restricciones: una que permita que se lancen todas las instancias EC2 que no sean de tipo GPU y otra que permita que se lancen solo las instancias EC2 t1.micro y m1.small. Para este ejemplo, AWS Service Catalog aplica la segunda restricción, más restrictiva (t1.micro y m1.small).

Puede limitar el acceso de los usuarios finales a los AWS recursos al adjuntar una política de IAM a una función de lanzamiento. A continuación, se crea una restricción de lanzamiento para utilizar el rol al lanzar el producto. AWS Service Catalog

Para obtener más información sobre las políticas gestionadas para AWS Service Catalog, consulte [Políticas AWS gestionadas para AWS Service Catalog](#).

# Administración de catálogos

AWS Service Catalog proporciona una interfaz para administrar carteras, productos y restricciones desde la consola del administrador.

## Note

Para realizar cualquiera de las tareas de esta sección, debe tener permisos de administrador para AWS Service Catalog. Para obtener más información, consulte [Administración de identidad y acceso en AWS Service Catalog](#).

## Tareas

- [Administración de carteras](#)
- [Administración de productos](#)
- [Uso de las restricciones AWS Service Catalog](#)
- [Acciones de servicio de AWS Service Catalog](#)
- [Adición de productos de AWS Marketplace a la cartera](#)
- [Uso AWS CloudFormation StackSets](#)
- [Administración de presupuestos](#)

# Administración de carteras

Puede crear, ver y actualizar carteras en la página Carteras de la consola del administrador de AWS Service Catalog.

## Tareas

- [Creación, visualización y eliminación de carteras](#)
- [Ver los detalles de la cartera](#)
- [Crear y eliminar carteras](#)
- [Adición de productos](#)
- [Adición de restricciones](#)
- [Conceder acceso a los usuarios](#)

- [Uso compartido de carteras](#)
- [Compartir e importar carteras](#)

## Creación, visualización y eliminación de carteras

La página Carteras muestra una lista de carteras que se han creado en la región actual. Esta página se utiliza para crear nuevas carteras, ver los detalles de una de ellas o eliminarlas de la cuenta.

Para ver la página Carteras

1. Abra la consola de Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. Seleccione otra región según sea necesario.
3. Si es la primera vez que utiliza AWS Service Catalog, aparecerá una página de inicio de AWS Service Catalog. Elija Get started para crear una cartera. Siga las instrucciones para crear la primer cartera y, a continuación, continúe a la página Carteras.

Cuando utilice AWS Service Catalog, puede volver a la página Carteras en cualquier momento; elija Catálogo de servicios en la barra de navegación y, a continuación, elija Carteras.

## Ver los detalles de la cartera

En la consola del administrador de AWS Service Catalog, la página Portfolio details (Detalles de la cartera) muestra la configuración de una cartera. Utilice esta página para gestionar los productos de la cartera, conceder a los usuarios acceso a los productos TagOptions y aplicar restricciones.

Para ver la página Portfolio details

1. Abra la consola de Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. Elija la cartera que desea administrar.

## Crear y eliminar carteras

Utilice la página Carteras para crear y eliminar carteras.

Para crear una nueva cartera

1. En el menú de navegación izquierdo, seleccione Carteras.

2. Seleccione Crear cartera.
3. En la página Crear cartera, introduzca la información solicitada.
4. Seleccione Crear. AWS Service Catalog crea la cartera y muestra sus detalles.

Para eliminar una cartera

 Note

Solo puede eliminar carteras locales. Puede eliminar carteras importadas (compartidas), pero no puede eliminar carteras importadas.

Antes de poder eliminar una cartera, debe eliminar todos sus productos, restricciones, grupos, funciones, usuarios, recursos compartidos y TagOptions. Para ello, abra una cartera para ver los Detalles de la cartera. A continuación, seleccione una pestaña para eliminarlas.

 Note

Para evitar errores, elimine las restricciones de la cartera antes de eliminar cualquier producto.

1. En el menú de navegación izquierdo, seleccione Carteras.
2. Seleccione la cartera que desea eliminar.
3. Elija Eliminar. Solo puede eliminar carteras locales. Si está intentando eliminar una cartera importada (compartida), el menú Acciones no está disponible.
4. En la ventana de confirmación, elija Delete.

## Adición de productos

Puede añadir productos a una cartera cargando un producto nuevo directamente a una cartera existente o asociando un producto existente de su catálogo a la cartera.

 Note

Al crear un producto AWS Service Catalog, puede cargar una plantilla AWS CloudFormation o un archivo de configuración de Terraform. La plantilla de AWS CloudFormation se

almacena en un bucket de Amazon Simple Storage Service (Amazon S3) y el nombre del bucket comienza por “cf-templates-.” También debe tener permiso para recuperar objetos de buckets adicionales al aprovisionar un producto. Para obtener más información acerca de la creación de un producto, consulte [Crear productos](#).

## Adición de un nuevo producto

Los productos nuevos se agregan directamente desde la página de detalles de la cartera. Al crear un producto desde esta página, AWS Service Catalog lo agrega a la cartera que está seleccionada en ese momento.

### Para agregar un nuevo producto

1. Vaya a la página Carteras y, a continuación, elija el nombre de la cartera a la que desea agregar el producto.
2. En la página de detalles de la cartera , amplíe la sección Productos y, a continuación, elija Subir nuevo producto.
3. En Enter product details, escriba lo siguiente:
  - Product name: el nombre del producto.
  - Descripción del producto (opcional) – Descripción del producto. Esta descripción se muestra en el listado de productos para ayudarle a elegir el producto correcto.
  - Descripción - la descripción completa. Esta descripción se muestra en el listado de productos para ayudarle a elegir el producto correcto.
  - Propietario o distribuidor – El nombre o la dirección de correo electrónico del propietario. La información de contacto del distribuidor es opcional.
  - Proveedor (opcional) - el nombre del proveedor de la aplicación. Este campo le permite ordenar la lista de productos para que les resulte más fácil buscar los que necesitan.
4. En la página Version details, escriba lo siguiente:
  - Elegir plantilla – Para los productos de AWS CloudFormation, seleccione su propio archivo de plantilla, una plantilla de AWS CloudFormation de una unidad local o una URL que apunte a una plantilla almacenada en Amazon S3, a una plantilla ARN de AWS CloudFormation de pila existente, o a un archivo de plantilla almacenado en un repositorio externo.

Para los productos Terraform, seleccione su propio archivo de plantilla, un archivo de configuración tar.gz de una unidad local o una URL que apunte a una plantilla almacenada en Amazon S3, o un archivo de configuración tar.gz almacenado en un repositorio externo.

- Nombre de la versión: el nombre de la versión del producto (por ejemplo, "v1", "v2beta"). No se permiten espacios.
- Description (opcional): una descripción de la versión del producto, incluidas sus diferencias respecto a la anterior.

5. En Enter support details, escriba lo siguiente:

- Email contact (opcional): la dirección de correo electrónico para comunicar problemas del producto.
- Enlace de soporte (opcional): dirección URL del sitio donde los usuarios pueden encontrar información de soporte o presentar tickets de servicio. La dirección URL debe comenzar por http:// o https://. Los administradores son responsables de mantener la precisión y el acceso a la información de soporte.
- Descripción del soporte (opcional): una descripción de cómo debe utilizar los datos de Contactos de correo electrónico y Enlace de soporte.

6. Seleccione Crear producto.

## Adición de un producto existente

Puede agregar productos existentes a una cartera desde tres ubicaciones: la lista de cartera, la página de Detalles de cartera y la lista de productos.

Para agregar un producto existente a una cartera

1. Vaya a la página Carteras.
2. Seleccione una cartera. A continuación, seleccione Acciones - Añadir producto a la cartera.
3. Elija un producto y, a continuación, haga clic en Añadir producto a la cartera.

## Eliminación de un producto de una cartera

Si ya no desea utilizar un producto, elimínelo de la cartera. El producto seguirá estando disponible en el catálogo desde la página Productos y podrá agregarlo a otras carteras. Puede eliminar varios productos de una cartera al mismo tiempo.

## Para eliminar un producto de una cartera

1. Vaya a la página Carteras y, a continuación, elija la cartera que contiene el producto. Se abrirá la página de detalles de la cartera.
2. Amplíe la sección de Productos.
3. Seleccione uno o más productos y, a continuación, elija Eliminar.
4. Confirme su elección.

## Adición de restricciones

Debería añadir restricciones para controlar la forma en que los usuarios interactúan con los productos. Para obtener más información acerca de los tipos de restricciones que se admiten en AWS Service Catalog, consulte [Uso de las restricciones AWS Service Catalog](#).

Las restricciones se agregan a los productos después de haberlos colocado en una cartera.

### Para agregar una restricción a un producto

1. Abra la consola de Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. Elija Carteras y seleccione una cartera.
3. En la página de detalles de la cartera, amplíe la sección Crear restricción y elija Añadir restricción.
4. En Producto, seleccione el producto al que se aplicará la restricción.
5. En Tipo de restricción, elija una de las siguientes opciones:

Lanzamiento – Le permite asignar un rol de IAM al producto que se utiliza para aprovisionar los recursos de AWS. Para obtener más información, consulte [Restricciones de lanzamiento AWS Service Catalog](#).

Notificación – Le permite transmitir notificaciones de productos a un tema de Amazon SNS. Para obtener más información, consulte [Restricciones de notificación de AWS Service Catalog](#).

Plantilla – Para limitar las opciones que los usuarios finales tienen a su disposición cuando lanzan un producto, se aplican restricciones de plantilla. Un template (Plantilla) es un archivo de texto con formato JSON que contiene una o varias reglas. Las reglas se agregan a la plantilla de AWS CloudFormation que el producto utiliza. Para obtener más información, consulte [Reglas de restricciones de plantilla](#).

Stack Set: le permite configurar la implementación del producto en todas las cuentas y regiones mediante AWS CloudFormation StackSets. Para obtener más información, consulte [Restricciones de conjunto de pilas de AWS Service Catalog](#).

Actualizar etiquetas – Le permite actualizar las etiquetas una vez que se haya aprovisionado el producto. Para obtener más información, consulte [AWS Service Catalog Restricciones de actualización de etiqueta](#).

6. Elija Continuar e introduzca la información que se le pida.

### Para editar una restricción

1. Para comenzar, inicie sesión en AWS Management Console y abra la consola de AWS Service Catalog administrador en <https://console.aws.amazon.com/catalog/>.
2. Elija Carteras y seleccione una cartera.
3. En la página de detalles de la cartera, amplíe la sección Crear restricción y seleccione la restricción que desee editar.
4. Seleccione Editar restricciones.
5. Edite la restricción según sea necesario y elija Guardar.

## Conceder acceso a los usuarios

Ofrezca a los usuarios acceso a las carteras a través de grupos o roles. La mejor manera de proporcionar acceso a las carteras a varios usuarios es incluirlos en un grupo de IAM y conceder acceso a dicho grupo. De esta forma, basta con agregar o eliminar usuarios del grupo para administrar el acceso a la cartera. Para obtener más información, consulte el tema relacionado con los [usuarios y grupos de IAM](#) en la Guía del usuario de IAM.

Además del acceso a una cartera, los usuarios de deben tener acceso a la consola del usuario final de AWS Service Catalog . Para conceder acceso a la consola, puede aplicar los permisos de IAM. Para obtener más información, consulte [Administración de identidad y acceso en AWS Service Catalog](#).

Si desea compartir una cartera y sus entidades principales con otras cuentas, puede asociar los nombres de entidad principal (grupos, roles o usuarios) a la cartera. Los nombres de entidad principal se comparten con la cartera y se utilizan en las cuentas de los destinatarios para conceder el acceso a los usuarios finales.

## Para conceder a usuarios o grupos acceso a una cartera

1. Abra la consola de Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. En el panel de navegación, seleccione Administración y, a continuación, seleccione Carteras.
3. Seleccione una cartera a la que quiera conceder acceso a grupos, roles o usuarios. AWS Service Catalog dirige a la página de Detalles de la cartera.
4. En la página de detalles de cartera, elija Acceso.
5. En Acceso a la cartera, seleccione Conceder acceso.
6. En Tipo, seleccione Nombre de entidad principal y, a continuación, seleccione el tipo de grupo/, rol/ o usuario/. Puede agregar hasta 9 nombres de entidad principal.
7. Seleccione Conceder acceso para asociar la entidad principal a la cartera actual.

## Para eliminar el acceso a una cartera

1. En la página de detalles de la cartera, elija la pestaña Elegir grupos, roles y usuarios.
2. Elija Eliminar acceso.

## Uso compartido de carteras

Para permitir que un AWS Service Catalog administrador de otra AWS cuenta distribuya sus productos a los usuarios finales, comparta su AWS Service Catalog cartera con ellos mediante el uso account-to-account compartido o AWS Organizations.

Cuando compartes una cartera mediante account-to-account sharing u Organizations, compartes una referencia de esa cartera. Los productos y las restricciones de la cartera importada se mantienen sincronizados con los cambios realizados en la cartera compartida, es decir, la cartera original que se ha compartido.

El destinatario no puede cambiar los productos o las restricciones, pero puede agregar acceso de AWS Identity and Access Management a los usuarios finales.

### Note

No puede compartir un recurso compartido. Esto incluye carteras que contienen un producto compartido.

## Un ccount-to-account intercambio

Para llevar a cabo estos pasos, debe obtener el ID de la cuenta de AWS de destino. Puede encontrar el ID en la página My Account (Mi página) de la AWS Management Console de la cuenta de destino.

Para compartir una cartera con una cuenta de AWS

1. Abra la consola de Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. En el menú de navegación de la izquierda, seleccione Carteras y, a continuación, seleccione la cartera que desea compartir. En el menú Acciones, seleccione Compartir.
3. En Introducir ID de cuenta, introduzca el ID de cuenta de la cuenta de AWS con la que está compartiendo. (Opcional) Seleccione [TagOption Compartir](#). A continuación, elija Compartir.
4. Envíe la URL al administrador de AWS Service Catalog de la cuenta de destino. La dirección URL abre la página Importar cartera y proporciona automáticamente el ARN de la cartera compartida.

### Importación de una cartera

Si un administrador de AWS Service Catalog de otra cuenta de AWS comparte una cartera con usted, debe importarla a su propia cuenta para poder distribuir los productos que contiene a sus usuarios finales.

No es necesario importar una cartera si la cartera se compartió mediante AWS Organizations.

Para importar la cartera, el administrador debe facilitarle una ID de cartera.

Para ver todas las carteras importadas, abra la consola AWS Service Catalog en <https://console.aws.amazon.com/servicecatalog/>. En la página Cartera, seleccione la pestaña Importadas. Revise la tabla de Carteras importadas.

### Compartiendo con AWS Organizations

Puede compartir carteras de AWS Service Catalog usando AWS Organizations.

En primer lugar, debe decidir si está compartiendo desde la cuenta de o desde una cuenta de administrador delegado. Si no desea compartir desde su cuenta de gestión, registre una cuenta de administrador delegada y úsela para compartirla. Para obtener más información, consulte [Registrar un administrador delegado](#) en la Guía del usuario de AWS CloudFormation.

A continuación, debe decidir con quién compartir. Puede compartir con las siguientes entidades:

- Una cuenta de organización.
- Una unidad organizativa (OU).
- La propia organización. (Esto comparte con todas las cuentas de la organización.)

### Compartir desde una cuenta de administración

Puede compartir una cartera con una organización cuando use su estructura organizativa o ingrese el ID de un nodo organizacional.

### Para compartir una cartera con una organización mediante la estructura organizativa

1. Abra la consola de AWS Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. En la página Carteras , seleccione la cartera que desea compartir. En el menú Acciones, seleccione Compartir.
3. Seleccione AWS Organizations y filtre según su estructura organizativa.

Puede seleccionar el nodo raíz para compartir la cartera con toda su organización, una unidad organizativa (OU) principal, una OU secundaria o una cuenta de AWS de su organización.

Al compartir con una unidad organizativa principal, se comparte la cartera con todas las cuentas y unidades organizativas secundarias de esa unidad organizativa principal.

Puede seleccionar Ver solo cuentas de AWS para ver una lista de todas las cuentas de AWS de su organización.

### Para compartir una cartera con una organización, introduzca el ID del nodo organizativo

1. Abra la consola de AWS Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. En la página Carteras , seleccione la cartera que desea compartir. En el menú Acciones, seleccione Compartir.
3. Seleccione el Nodo de la organización.

Seleccione si desea compartir con toda la organización, una cuenta de AWS de su organización o una unidad organizativa.

Introduzca el ID del nodo organizativo que ha seleccionado, que encontrará en la consola AWS Organizations en <https://console.aws.amazon.com/organizations/>.

## Compartir desde una cuenta de administrador delegado

La cuenta de gestión de una organización puede registrar y anular el registro de otras cuentas como administradores delegados para la organización.

Un administrador delegado puede compartir recursos de AWS Service Catalog en su organización de la misma manera que una cuenta de gestión. Están autorizados a crear, eliminar y compartir carteras.

Para registrar o anular el registro de un administrador delegado, debe usar la API o la CLI desde la cuenta de gestión. Para obtener más información consulte [RegisterDelegatedAdministrator](#) y [DeregisterDelegatedAdministrator](#) en la Referencia de la API de AWS Organizations.

### Note

Antes de poder designar a un delegado, el administrador debe llamar a [EnableAWSOrganizationsAccess](#).

El procedimiento para compartir una cartera desde una cuenta de administrador delegada es el mismo que compartir desde una cuenta maestra, como se ve anteriormente en [the section called “Compartir desde una cuenta de administración”](#).

Si se anula el registro de un miembro como administrador delegado, ocurre lo siguiente:

- Se eliminan las acciones de cartera creadas a partir de esa cuenta.
- Ya no pueden crear nuevas acciones de cartera.

### Note

Si la cartera y las acciones creadas por un administrador delegado no se eliminan después de anular el registro del administrador delegado, registre y anule el registro del administrador delegado de nuevo. Esto eliminará la cartera y las acciones creadas por esa cuenta.

## Mover cuentas dentro de su organización

Si mueve una cuenta dentro de su organización, las carteras AWS Service Catalog compartidas con la cuenta podrían cambiar.

Las cuentas solo tienen acceso a las carteras compartidas con la organización o unidad organizativa de destino.

## Compartir TagOptions al compartir carteras

Como administrador, puede crear un recurso compartido para TagOptions incluirlo. TagOptions son pares clave-valor que permiten a los administradores:

- Defina y aplique la taxonomía de las etiquetas.
- Defina las opciones de etiquetas y asócielas a productos y carteras.
- Comparta las opciones de etiquetas asociadas a carteras y productos con otras cuentas.

Al añadir o eliminar opciones de etiquetas en la cuenta principal, el cambio aparece automáticamente en las cuentas de los destinatarios. En las cuentas de los destinatarios, cuando un usuario final aprovisiona un producto TagOptions, debe elegir valores para las etiquetas que se convierten en etiquetas del producto aprovisionado.

En las cuentas de destinatarios, los administradores pueden asociar productos locales adicionales TagOptions a su cartera importada para hacer cumplir las reglas de etiquetado específicas de cada cuenta.

### Note

Para compartir una cartera, necesita el ID de la cuenta de AWS del consumidor. Busque el ID de la cuenta de AWS en Mi cuenta en la consola.

### Note

Si a TagOption tiene un valor único, lo aplica AWS automáticamente durante el proceso de aprovisionamiento.

## Para compartir TagOptions al compartir carteras

1. En el menú de navegación izquierdo, seleccione Carteras.
2. En Carteras locales, seleccione y abra una cartera.
3. Seleccione Compartir de la lista anterior y, a continuación, pulse el botón Compartir.

4. Seleccione compartir con otra cuenta u organización de AWS.
5. Introduzca el número de identificación de la cuenta de 12 dígitos, seleccione Habilitar y, a continuación, seleccione Compartir.

La cuenta que ha compartido aparece en la sección Cuentas compartidas con. Indica si están TagOptions habilitados.

También puede actualizar una acción de cartera para incluirla TagOptions. Todo lo TagOptions que pertenece a la cartera y al producto ahora se comparte en esta cuenta.

Para actualizar una cartera, comparta para incluir TagOptions

1. En el menú de navegación izquierdo, seleccione Carteras.
2. En Cartera local, seleccione y abra una cartera.
3. Seleccione Compartir de la lista anterior.
4. En Cuentas compartidas con, seleccione un ID de cuenta y, a continuación, seleccione Acciones.
5. Seleccione Actualizar dejar de compartir o Dejar de compartir.

Al seleccionar Actualizar dejar de compartir, selecciona Activar para iniciar el uso compartido TagOptions. La cuenta que ha compartido aparece en la sección Cuentas compartidas con.

Al seleccionar Dejar de compartir, confirma que ya no desea compartir la cuenta.

## Compartir los nombres de entidad principal al compartir carteras

Como administrador, puede crear una cartera compartida que incluya los nombres de entidad principales. Los nombres de entidad principales son nombres para grupos, funciones y usuarios que los administradores pueden especificar en una cartera y luego compartir con la cartera. Al compartir la cartera, AWS Service Catalog verifica si esos nombres de entidad principal ya existen. Si existen, AWS Service Catalog asocia automáticamente las entidades principales de IAM coincidentes a la cartera compartida para conceder el acceso a los usuarios finales.

### Note

Al asociar una entidad principal a una cartera, puede producirse una posible escalada de privilegios cuando esa cartera se comparte con otras cuentas. Para un usuario de una

cuenta de destinatario que no sea administrador de AWS Service Catalog, pero que aún pueda crear entidades principales (usuarios/roles), ese usuario podría crear un rol IAM que coincida con la asociación de nombres de entidades principales de la cartera. Si bien es posible que este usuario no sepa qué nombres de entidades principales están asociados a través de AWS Service Catalog, es posible que pueda adivinar el usuario. Si esta posible ruta de escalamiento es motivo de preocupación, AWS Service Catalog recomienda utilizar `PrincipalType` como IAM. Con esta configuración, el `PrincipalARN` ya debe existir en la cuenta del destinatario antes de poder asociarla.

Al añadir o eliminar los nombres de entidad principal de la cuenta principal, AWS Service Catalog aplica automáticamente esos cambios a la cuenta del destinatario. Los usuarios de la cuenta destinataria pueden entonces realizar tareas en función de su rol:

- Los Usuarios finales pueden aprovisionar, actualizar y cancelar el producto de la cartera.
- Los administradores pueden asociar más entidades principales de IAM a su cartera importada para permitir el acceso a los usuarios finales específicos de esa cuenta.

 Note

El uso compartido de nombres de entidad principal solo está disponible para AWS Organizations.

Para compartir los nombres de entidad principal al compartir carteras

1. En el menú de navegación izquierdo, seleccione Carteras.
2. En Carteras locales, seleccione la cartera que desea compartir.
3. En el menú Acciones, elija Compartir.
4. Seleccione una organización en AWS Organizations.
5. Seleccione toda la Raíz de la organización, una unidad organizativa (OU) o un miembro de la organización.
6. En la configuración de compartir, habilite la opción de compartir entidad principal.

También puede actualizar una cartera compartida para incluir el nombre de entidad principal. Esto comparte todos los nombres de entidad principal que pertenecen a esa cartera con la cuenta del destinatario.

Para actualizar una cartera compartida para habilitar o deshabilitar los nombres de entidad principal

1. En el menú de navegación izquierdo, seleccione Carteras.
2. En Cartera local, seleccione la cartera que desea actualizar.
3. Elija la pestaña Compartir.
4. Seleccione el recurso compartido que desea actualizar y, a continuación, seleccione Compartir.
5. Seleccione Actualizar el recurso compartido y, a continuación, seleccione Habilitar para iniciar el uso compartido de entidad principal. A continuación, AWS Service Catalog comparte los nombres de entidad principal en las cuentas de los destinatarios.

Deshabilitar el uso compartido de la entidad principal si desea dejar de compartir los nombres de entidad principal con las cuentas de los destinatarios.

Uso de caracteres comodín al compartir nombres de entidad principal

AWS Service Catalog permite conceder acceso a la cartera a los nombres de entidad principal (usuario, grupo o rol) de IAM con caracteres comodín, como '\*' o '?'. El uso de patrones comodín permite cubrir varios nombres de entidad principal de IAM a la vez. La ruta del ARN y el nombre de la entidad principal permiten caracteres comodín ilimitados.

Ejemplos de un comodín de ARN aceptable:

- **arn:aws:iam::role/ResourceName\_\***
- **arn:aws:iam::role/\*/ResourceName\_?**

Ejemplos de un comodín de ARN inaceptable:

- **arn:aws:iam::\*/ResourceName**

En el formato ARN de entidad principal de IAM (**arn:partition:iam::resource-type/resource-path/resource-name**), los valores válidos incluyen usuario/, grupo/, o rol/. Los caracteres "?" y "\*" solo se permiten después del tipo de recurso en el segmento de identificador del recurso. Puede usar caracteres especiales en cualquier parte del identificador del recurso.

El carácter “\*” también coincide con el carácter “/”, lo que permite que se formen rutas dentro del identificador del recurso. Por ejemplo:

**arn:aws:iam:::role/\*/ResourceName\_?** coincide tanto con **arn:aws:iam:::role/pathA/pathB/ResourceName\_1** como con **arn:aws:iam:::role/pathA/ResourceName\_1**.

## Compartir e importar carteras

Para que sus productos del AWS Service Catalog estén a disposición de usuarios que no pertenecen a su cuenta de Cuentas de AWS, tales como los usuarios que pertenecen a otras organizaciones o a otras cuentas de Cuentas de AWS de su organización, comparte las carteras con ellos. Puede compartir de varias formas, como account-to-account compartir, compartir de forma organizativa e implementar catálogos mediante conjuntos de pilas.

Antes de compartir sus productos y carteras con otras cuentas, debe decidir si desea compartir una referencia del catálogo o implementar una copia del catálogo en cada cuenta de destinatario. Tenga en cuenta que si implementa una copia, debe volver a implementar si hay actualizaciones que desea propagar a las cuentas de destinatario.

Puede utilizar conjuntos de pilas para implementar el catálogo en muchas cuentas al mismo tiempo. Si quieres compartir una referencia (una versión importada de tu portafolio que permanece sincronizada con la original), puedes usar la opción account-to-account compartir o puedes compartir usando AWS Organizations.

Para utilizar conjuntos de pilas para implementar una copia del catálogo, consulte [Cómo configurar un catálogo para varias regiones y varias cuentas de productos de AWS Service Catalog estándar de la empresa](#).

Al compartir una cartera o AWS Organizations al account-to-account permitir que un AWS Service Catalog administrador de otra AWS cuenta importe la cartera a su cuenta y distribuya los productos entre los usuarios finales de esa cuenta.

Esta cartera importada no es una copia independiente. Los productos y las restricciones de la cartera importada se mantienen sincronizados con los cambios realizados en la cartera compartida, es decir, la cartera original que se ha compartido. El administrador destinatario, aquel con quien se comparte la cartera, no puede modificar los productos ni las restricciones, pero sí puede agregar accesos de AWS Identity and Access Management IAM para los usuarios finales. Para obtener más información, consulte [Conceder acceso a los usuarios](#).

El administrador destinatario puede distribuir los productos a los usuarios finales que pertenecen a su AWS cuenta de AWS de las siguientes maneras:

- Agregando usuarios, grupos y funciones a la cartera importada.
- Agregando productos de la cartera importada a una cartera local, es decir, una cartera creada por el administrador destinatario que pertenece a su cuenta de AWS. A continuación, el administrador destinatario agrega los usuarios, grupos y roles a la cartera local. Cualquier restricción que usted haya aplicado a los productos de la cartera compartida también están presentes en la cartera local. El administrador del destinatario de la cartera local puede añadir restricciones adicionales, pero no puede eliminar las restricciones que se importaron originalmente de la cartera compartida.

Cuando se agregan productos o restricciones a la cartera compartida o se eliminan productos o restricciones de ella, el cambio se propaga a todas las instancias importadas de la cartera. Por ejemplo, si elimina un producto de la cartera compartida, dicho producto también se eliminará de la cartera importada. También se eliminará de todas las carteras locales a la que se haya agregado el producto importado. Si un usuario final ha lanzado un producto antes de eliminarlo, el producto provisionado por el usuario final continuará ejecutándose, pero ya no estará disponible para lanzamientos futuros.

Si se aplica una restricción de lanzamiento a un producto de una cartera compartida, esta se propaga a todas las instancias importadas del producto. Para anular la restricción de lanzamiento, el administrador destinatario puede agregar el producto a una cartera local y, a continuación, aplicarle una restricción de lanzamiento diferente. La restricción de lanzamiento que se encuentre en vigor establece un rol de lanzamiento para el producto.

Una función de lanzamiento es una función de IAM que AWS Service Catalog utiliza para provisionar recursos de AWS (tales como instancias Amazon EC2 o bases de datos de Amazon RDS) cuando un usuario final lanza el producto. Como administrador, puede elegir designar un ARN de rol de lanzamiento específico o un nombre de rol local. Si utiliza el ARN del rol, el rol se utilizará incluso si el usuario final pertenece a una cuenta de AWS diferente de la que posee el rol de lanzamiento. Si utiliza un nombre de rol local, se utilizará el rol de IAM con ese nombre en la cuenta del usuario final.

Para obtener más información sobre las restricciones de lanzamiento y los roles de lanzamiento, consulte [Restricciones de lanzamiento AWS Service Catalog](#). La cuenta de AWS que posee la función de lanzamiento provisiona los recursos de AWS y es la cuenta que incurre en los cargos por el uso de esos recursos. Para más información, consulte [Precios de AWS Service Catalog](#).

Este vídeo muestra cómo compartir carteras entre cuentas en AWS Service Catalog.

[Comparta \(https://www.youtube.com/embed/BVSohYOppjk%22%3EShare\)](https://www.youtube.com/embed/BVSohYOppjk%22%3EShare) carteras entre cuentas en [AWS Service Catalog](#).

**Note**

No se pueden volver a compartir los productos de una cartera que se ha importado o compartido.

**Note**

Las importaciones de carteras deben realizarse en la misma región entre la cuenta de administración y la dependiente.

## Relación entre las carteras compartidas e importadas

Esta tabla se indica la relación entre una cartera importada y una cartera compartida, así como las acciones que un administrador que importe una cartera de productos puede y no puede realizar con ese cartera y con los productos que contiene.

Elemento de la cartera compartida	Relación con la cartera importada	El administrador destinatario puede	El administrador destinatario no puede
Productos y versiones de productos	Se heredan. Si el creador de la cartera agrega o elimina productos de la cartera compartida, el cambio se propaga a la cartera importada.	Agregar productos importados a las carteras locales. Los productos se mantienen sincronizados con la cartera compartida.	Cargar o agregar productos a cartera importada ni quitar productos de ella.
Restricciones de lanzamiento	Se heredan. Si el creador de la cartera agrega	En una cartera local, el administrador puede aplicar restricciones de lanzamiento	Agregar restricciones de lanzamiento a la cartera importada o quitarlas de ella.

Elemento de la cartera compartida	Relación con la cartera importada	El administrador destinatario puede	El administrador destinatario no puede
	<p>restricciones de lanzamiento a un producto compartido o las elimina de él, el cambio se propaga a todas las instancias importadas del producto.</p> <p>Si el administrador destinatario agrega un producto importado a una cartera local, la restricción de lanzamiento importada que se aplica a ese producto está presente en la cartera local.</p>	to que afecten al lanzamiento local del producto.	

Elemento de la cartera compartida	Relación con la cartera importada	El administrador destinatario puede	El administrador destinatario no puede
Restricciones de plantilla	<p>Se heredan.</p> <p>Si el creador de la cartera agrega una restricción de plantilla a un producto compartido o la elimina de él, el cambio se propaga a todas las instancias importadas del producto.</p> <p>Si el administrador destinatario agrega un producto importado a una cartera local, las restricciones de plantilla importadas no se trasladan a la cartera local.</p>	En una cartera local, el administrador puede agregar restricciones de plantilla que se aplicarán al producto local.	Eliminar las restricciones de plantilla importadas.
Usuarios, grupos y roles	No se heredan.	Agregar usuarios, grupos y funciones de AWS que están presentes en la cuenta de del administrador.	No se usa.

## Administración de productos

Puede crear productos empaquetando una plantilla con metadatos, actualizar productos creando una nueva versión basada en una plantilla actualizada y agrupar los productos en carteras para distribuirlos a los usuarios.

Las nuevas versiones de los productos se propagan a todos los usuarios que tienen acceso al producto a través de una cartera. Cuando se distribuye una actualización, los usuarios finales pueden actualizar los productos aprovisionados existentes con tan solo unos clics.

## Tareas

- [Ver la página de productos](#)
- [Creación de productos](#)
- [Adición de productos a las carteras](#)
- [Actualización de productos](#)
- [Sincronizar productos con archivos de plantilla desde GitHub GitHub Enterprise o Bitbucket](#)
- [Eliminación de productos](#)
- [Administración de versiones](#)

## Ver la página de productos

Los productos se administran en la página Lista de productos de la AWS Service Catalog consola del administrador.

Para ver la página Lista de productos

1. Abra la consola de Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. Seleccione Lista de productos.

## Creación de productos

Los productos se crean en la página Products (Productos) de la consola del administrador de AWS Service Catalog.

### Note

La creación de productos de Terraform requiere una configuración adicional, incluyendo un motor de aprovisionamiento de Terraform y un rol de lanzamiento. Para obtener más información, consulte [Introducción a un producto Terraform](#).

## Para crear un nuevo producto de AWS Service Catalog

1. Vaya a la página Lista de productos.
2. Seleccione Crear producto y, a continuación, seleccione Crear producto.
3. Detalles del producto: le permite elegir el tipo de producto que desea crear. AWS Service Catalog admite AWS CloudFormation, Terraform Cloud y los tipos de productos externos (que admiten los productos de Terraform Community Edition). Los detalles del producto también contienen los metadatos que aparecen al buscar y ver productos en una lista o página de detalles. Introduzca lo siguiente:
  - Product name: el nombre del producto.
  - Descripción del producto – La descripción se muestra en la lista de productos para ayudarlo a elegir el producto correcto.
  - Propietario – La persona u organización que publica este producto. El propietario puede ser el nombre de su organización de TI o del administrador.
  - Distribuidor (opcional): el nombre del publicador de la aplicación. Este campo le permite ordenar la lista de productos para que les resulte más fácil buscarlos.
4. Los Detalles de la versión le permiten añadir el archivo de plantilla y crear el producto. Introduzca lo siguiente:
  - Elegir un método – Hay cuatro formas de añadir un archivo de plantilla.
    - Utilizar un archivo de plantilla local - Cargue una plantilla de AWS CloudFormation o un archivo de configuración tar.gz de Terraform desde una unidad local.
    - Utilizar una URL de Amazon S3 - Especifique una URL que apunte a una plantilla de AWS CloudFormation o a un archivo de configuración tar.gz de Terraform almacenado en Amazon S3. Si especifica una dirección URL de Amazon S3, debe comenzar con `https://`.
    - Usa un repositorio externo: especifica tu repositorio de código GitHub, GitHub Enterprise o Bitbucket. AWS Service Catalogte permite sincronizar los productos con los archivos de plantilla. En el caso de los productos Terraform, el formato del archivo de plantilla debe ser un único archivo archivado en Tar y comprimido en Gzip.
    - Utilizar una CloudFormation pila existente: introduce el ARN de una pila existente CloudFormation . Este método no es compatible con los productos de Terraform Cloud o externos.

- Título de la versión (opcional) - el nombre de la versión del producto (por ejemplo, "v1", "v2beta"). No se permiten espacios.
  - Description (opcional): una descripción de la versión del producto, incluidas sus diferencias respecto a otras versiones.
  - Guía – Se gestiona en la pestaña de versiones de la página de Detalles del producto. Cuando se crea una versión del producto (durante el flujo de trabajo de creación del producto), la guía para esa versión se establece de forma predeterminada. Para obtener más información sobre la guía, consulte [Administración de versiones](#).
5. Los Detalles de soporte identifican la organización de su empresa y proporcionan un punto de contacto para el soporte. Introduzca lo siguiente:
- Email contact (opcional): la dirección de correo electrónico para comunicar problemas del producto.
  - Enlace de soporte (opcional): dirección URL del sitio donde los usuarios pueden encontrar información de soporte o presentar tickets de servicio. La dirección URL debe comenzar por `http://` o `https://`. Los administradores son responsables de mantener la precisión y el acceso a la información de soporte.
  - Descripción del soporte (opcional): una descripción de cómo debe utilizar los datos de Email contact y Enlace de soporte.
6. Administrar etiquetas (opcional) – Además de usar etiquetas para categorizar sus recursos, también puede usarlas para autenticar sus permisos para crear este recurso.
7. Crear producto – Cuando haya completado el formulario, seleccione Crear producto. Transcurridos unos segundos, el producto aparecerá en la página Lista de productos. Puede que necesite actualizar el navegador para ver el producto.

También puedes usarlo CodePipeline para crear y configurar una canalización para implementar la plantilla de producto AWS Service Catalog y entregar los cambios que hayas realizado en tu repositorio de origen. Para obtener más información, consulte [Tutorial: Crear una canalización que se implementa para AWS Service Catalog](#).

Puede definir las propiedades de los parámetros en su plantilla de AWS CloudFormation o en la de Terraform y aplicar esas reglas durante el aprovisionamiento. Estas propiedades pueden definir la longitud mínima y máxima, los valores mínimos y máximos, los valores permitidos y una expresión regular para el valor. AWS Service Catalog emite una advertencia durante el aprovisionamiento si el valor proporcionado no se ajusta a la propiedad del parámetro. Para obtener más información

sobre las propiedades de los parámetros, consulte [Parámetros](#) en la Guía del usuario de AWS CloudFormation.

## Solución de problemas

Debe tener permiso para recuperar objetos de los buckets de Amazon S3. De lo contrario, podría encontrarse con el siguiente error al lanzar o actualizar un producto.

***Error: failed to process product version s3 access denied exception***

Si aparece este mensaje, asegúrese de tener permiso para recuperar objetos de los siguientes buckets:

- El bucket en el que se almacena la plantilla de artefacto de aprovisionamiento.
- El bucket que empieza por "cf-templates-\*" y donde AWS Service Catalog almacena la plantilla de artefacto de aprovisionamiento.
- El bucket interno que empieza por "sc-\*" y donde AWS Service Catalog almacena los metadatos. No podrá ver este bucket desde su cuenta.

El siguiente ejemplo de política muestra los permisos mínimos necesarios para recuperar objetos de los buckets mencionados anteriormente.

```
{
  "Sid": "VisualEditor1",
  "Effect": "Allow",
  "Action": "s3:GetObject*",
  "Resource": [
    "arn:aws:s3:::YOUR_TEMPLATE_BUCKET",
    "arn:aws:s3:::YOUR_TEMPLATE_BUCKET/*",
    "arn:aws:s3:::cf-templates-*",
    "arn:aws:s3:::cf-templates-*/*",
    "arn:aws:s3:::sc-*",
    "arn:aws:s3:::sc-*/*"
  ]
}
```

## Adición de productos a las carteras

Puede agregar productos a cualquier cantidad de carteras. Cuando un producto se actualiza, todas las carteras que lo contienen reciben automáticamente la nueva versión, incluidas las carteras compartidas.

Para agregar un producto del catálogo a una cartera

1. Vaya a la página Lista de productos.
2. Seleccione un producto y, a continuación, seleccione Acciones. En el menú desplegable, seleccione Añadir producto a la cartera. Se te redirigirá a la página Añadir *name-of-product* portafolio.
3. Elija una cartera y, a continuación, haga clic en Añadir producto a cartera.

Al agregar un producto de Terraform a una cartera, el producto requiere una restricción de lanzamiento. Debe seleccionar un rol de IAM de su cuenta, introducir un ARN de rol de IAM o introducir un nombre de rol. Si especifica un nombre del rol, cuando una cuenta utilice la restricción de lanzamiento, se utilizará el rol de IAM con ese nombre en la cuenta. Esto permite que las restricciones del rol de lanzamiento sean independientes de la cuenta, de modo que pueda crear menos recursos por cuenta compartida. Para obtener información e instrucciones, consulte [Paso 6: Añadir una restricción de lanzamiento a su producto de Terraform](#)

Una cartera puede contener una gran cantidad de productos que son una combinación de AWS CloudFormation y tipos de productos de Terraform.

## Actualización de productos

Cuando actualice la plantilla de un producto, cree una nueva versión del producto. Una nueva versión de un producto se pone automáticamente a disposición de todos los usuarios que tienen acceso a la cartera que lo contiene.

### Note

Al actualizar un producto existente, no puede cambiar el tipo de producto (AWS CloudFormation o Terraform). Por ejemplo, si actualiza un producto AWS CloudFormation, no puede reemplazar la plantilla AWS CloudFormation existente por un archivo de configuración

tar.gz de Terraform. Debe actualizar el archivo de plantilla de AWS CloudFormation existente con un archivo de plantilla de AWS CloudFormation nuevo.

Los usuarios que actualmente están ejecutando un producto aprovisionado de la versión anterior del producto pueden actualizar el producto aprovisionado en la vista de la consola del usuario final. Cuando está disponible una nueva versión de un producto, los usuarios pueden utilizar el comando Actualizar productos o aprovisionado de la página Lista de producto aprovisionado o Detalles de producto aprovisionado.

Antes de crear una nueva versión de un producto, AWS Service Catalog recomienda probar las actualizaciones en AWS CloudFormation o en el motor de Terraform para asegurarse de que funcionan de manera adecuada.

Para crear una nueva versión de un producto

1. Vaya a la página Lista de productos.
2. Seleccione el producto que desea actualizar. Se le redirigirá a la página de Detalles del producto.
3. En la página de detalles del producto , amplíe la sección Versiones ; y, a continuación, elija Crear nueva versión.
4. En Detalles de la versión, realice lo siguiente:
  - Elegir plantilla – Hay cuatro formas de añadir un archivo de plantilla.

Usar un archivo de plantilla local - Cargue una plantilla de AWS CloudFormation o un archivo de configuración tar.gz de Terraform desde una unidad local.

Utilizar una URL de Amazon S3 - Especifique una URL que apunte a una plantilla de AWS CloudFormation o a un archivo de configuración tar.gz de Terraform almacenado en Amazon S3. Si especifica una dirección URL de Amazon S3, debe comenzar por https://.

Usa un repositorio externo: especifica tu repositorio de código GitHub, GitHub Enterprise o Bitbucket. AWS Service Catalog permite sincronizar los productos con los archivos de plantilla. En el caso de los productos Terraform, el formato del archivo de plantilla debe ser un único archivo archivado en Tar y comprimido en Gzip.

Utilizar una CloudFormation pila existente: introduce el ARN de una pila existente CloudFormation . Este método no es compatible con los productos de Terraform Cloud o externos.

- Título de la versión - el nombre de la versión del producto (por ejemplo, "v1", "v2beta"). No se permiten espacios.
- Descripción (opcional): una descripción de la versión del producto, incluidas sus diferencias respecto a la anterior.

5. Seleccione Crear versión del producto.

También se puede utilizar CodePipeline para crear y configurar una canalización en la que implementar la plantilla de producto y entregar los cambios en el repositorio de origen. AWS Service Catalog Para obtener más información, consulte [Tutorial: Crear una canalización que se implementa para AWS Service Catalog](#).

## Sincronizar productos con archivos de plantilla desde GitHub GitHub Enterprise o Bitbucket

AWS Service Catalog te permite sincronizar los productos con los archivos de plantilla que se gestionan a través de un proveedor de repositorios externo. AWS Service Catalog se refiere a los productos con este tipo de conexión de plantilla como productos sincronizados con Git. Las opciones de repositorio incluyen GitHub GitHub Enterprise o Bitbucket. Tras autorizarte Cuenta de AWS con una cuenta de repositorio externa, puedes crear nuevos AWS Service Catalog productos o actualizar los existentes para sincronizarlos con un archivo de plantilla del repositorio. Cuando se realizan cambios en el archivo de plantilla y se guardan en el repositorio (por ejemplo, mediante git-push), los detecta AWS Service Catalog automáticamente y crea una nueva versión del producto (artefacto).

### Temas

- [Permisos necesarios para sincronizar productos con archivos de plantilla externos](#)
- [Crear una conexión de cuenta](#)
- [Visualizar las conexiones de productos sincronizados con Git](#)
- [Actualizar las conexiones de productos sincronizados con Git](#)
- [Eliminar conexiones de productos sincronizados con Git](#)
- [Sincronizar los productos de Terraform con archivos de plantilla de GitHub GitHub Enterprise o Bitbucket](#)

- [Región de AWS soporte para productos sincronizados con Git](#)

## Permisos necesarios para sincronizar productos con archivos de plantilla externos

Puedes usar la siguiente política AWS Identity and Access Management (IAM) como plantilla para que AWS Service Catalog los administradores puedan sincronizar los productos con los archivos de plantillas de un repositorio externo. Esta política incluye los permisos necesarios tanto de como CodeConnections de AWS Service Catalog. AWS Service Catalog recomienda copiar la política de plantillas que aparece a continuación y utilizar también la [política AWS Service CatalogAWSServiceCatalogAdminFullAccess gestionada](#) al habilitar los productos sincronizados en el repositorio.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CodeStarAccess",
      "Effect": "Allow",
      "Action": [
        "codestar-connections:UseConnection",
        "codestar-connections:PassConnection",
        "codestar-connections:CreateConnection",
        "codestar-connections>DeleteConnection",
        "codestar-connections:GetConnection",
        "codestar-connections:ListConnections",
        "codestar-connections:ListInstallationTargets",
        "codestar-connections:GetInstallationUrl",
        "codestar-connections:StartOAuthHandshake",
        "codestar-connections:UpdateConnectionInstallation",
        "codestar-connections:GetIndividualAccessToken"
      ],
      "Resource": "arn:aws:codestar-connections:*:*:connection/*"
    },
    {
      "Sid": "CreateSLR",
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam:*:*:role/aws-service-role/
sync.servicecatalog.amazonaws.com/AWSServiceRoleForServiceCatalogArtifactSync",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": "sync.servicecatalog.amazonaws.com"
        }
      }
    }
  ]
}
```

```
}  
  }  
} ]  
}
```

## Crear una conexión de cuenta

Antes de sincronizar un archivo de plantilla con un AWS Service Catalog producto, debes crear y autorizar una conexión única. account-to-account Esta conexión se utiliza para especificar los detalles del repositorio que contiene el archivo de plantilla deseado. Puede crear una conexión mediante la AWS Service Catalog consola, la CodeConnections consola AWS Command Line Interface (CLI) o CodeConnections las API.

Tras establecer una conexión, puede utilizar la AWS Service Catalog consola, la AWS Service Catalog API o la CLI para crear un AWS Service Catalog producto sincronizado. AWS Service Catalog los administradores pueden crear AWS Service Catalog productos nuevos o actualizar los existentes a partir de un archivo de plantilla en un repositorio o una sucursal. Si se realiza un cambio en el repositorio, lo detecta AWS Service Catalog automáticamente y crea una nueva versión del producto. Las versiones anteriores del producto se mantienen hasta el límite de versiones prescrito y se les asigna un estado obsoleto.

Además, crea AWS Service Catalog automáticamente un rol vinculado a un servicio (SLR) una vez creada la conexión. Esta SLR permite a AWS Service Catalog detectar cualquier cambio en el archivo de plantilla que se haya registrado en el repositorio. La SLR también permite crear automáticamente nuevas versiones de productos AWS Service Catalog para los productos sincronizados. Para obtener más información sobre los permisos y la funcionalidad de SLR, consulte [Funciones vinculadas al servicio para AWS Service Catalog](#).

Para crear un nuevo producto sincronizado con Git

1. En el panel de navegación izquierdo, elija Lista de productos y, a continuación, elija Crear un proveedor.
2. Introducir los Detalles del producto.
3. En Detalles de la versión, selecciona Especificar tu repositorio de código mediante un AWS CodeStar proveedor y, a continuación, selecciona el enlace Crear una nueva AWS CodeStar conexión.

4. Después de crear la conexión, actualice la lista de conexiones y, a continuación, seleccione la nueva conexión. Especifique los detalles del repositorio, incluyendo el repositorio, la rama y la ruta del archivo de plantilla.

Para obtener más información sobre cómo usar archivos de configuración Terraform, consulte [Sincronizar los productos de Terraform con archivos de plantilla de GitHub GitHub Enterprise o Bitbucket](#).

- a. (Opcional al crear un recurso de AWS Service Catalog producto nuevo) En la sección Support Details, añada metadatos para el producto.
  - b. (Opcional al crear un nuevo recurso de AWS Service Catalog producto) En la sección Etiquetas, elija Añadir nueva etiqueta e introduzca los pares clave y valor.
5. Elija Crear nuevo producto.

Para crear varios productos sincronizados con Git

1. En el panel de navegación izquierdo de la AWS Service Catalog consola, selecciona Lista de productos y, a continuación, selecciona Crear varios productos gestionados por git.
2. Introducir los Detalles comunes del producto.
3. En detalles del repositorio externo, seleccione una AWS CodeStar conexión y, a continuación, especifique el repositorio y la rama.
4. En el panel Añadir productos, introduzca la Ruta del archivo de plantilla y el Nombre del producto. Seleccione Añadir un nuevo elemento y siga añadiendo los productos que desee.
5. Tras añadir todos los productos deseados, seleccione Crear productos de forma masiva.

Para conectar un AWS Service Catalog producto existente a un repositorio externo

1. En el panel de navegación izquierdo de la AWS Service Catalog consola, selecciona Lista de productos y, a continuación, selecciona Conectar productos a un repositorio externo.
2. En la página Seleccionar productos, seleccione los productos que desea conectar a un repositorio externo y, a continuación, seleccione Siguiente.
3. En la página Especificar los detalles de la fuente, seleccione una AWS CodeStar conexión existente y, a continuación, especifique el repositorio, la sucursal y la ruta del archivo de plantilla.
4. Elija Siguiente.

5. En la página Revisar y enviar, verifique los detalles de la conexión y, a continuación, seleccione Conectar los productos a un repositorio externo.

## Visualizar las conexiones de productos sincronizados con Git

Puede usar la AWS Service Catalog consola, la API o ver AWS CLI los detalles de la conexión al repositorio. En el caso de los AWS Service Catalog productos que están vinculados a un archivo de plantilla, puedes recuperar información sobre la conexión al repositorio y la última vez que la plantilla se sincronizó con el producto desde el estado de última sincronización.

### Note

Puede ver la información del repositorio y el Estado de la última sincronización a nivel de producto. Los usuarios deben tener permisos de IAM en las CodeConnections API para ver los detalles del repositorio. Consulta [los permisos necesarios para sincronizar AWS Service Catalog productos con archivos de plantilla para](#) obtener más información sobre la política requerida para estos permisos de IAM.

Para ver los detalles de la conexión y el repositorio mediante AWS Management Console

1. En el menú de navegación izquierdo, elija Lista de productos.
2. Seleccione el producto de la lista.
3. En la página del Producto, vaya a la sección de Detalles de la fuente del producto.
4. Para ver el ID de revisión de origen de una versión del producto, seleccione el enlace Última versión creada. La sección de Detalles de la versión muestra el ID de revisión de origen.

Para ver los detalles de la conexión y el repositorio mediante AWS CLI

Desde AWS CLI, ejecute los siguientes comandos:

```
$ aws servicecatalog describe-product-as-admin
```

```
$ aws servicecatalog describe-provisioning-artifact
```

```
$ aws servicecatalog search-product-as-admin
```

```
$ aws servicecatalog list-provisioning-artifacts
```

## Actualizar las conexiones de productos sincronizados con Git

Puedes actualizar las conexiones de cuentas existentes y los productos sincronizados con Git mediante la AWS Service Catalog consola, la AWS Service Catalog API o. AWS CLI

Para obtener información sobre cómo conectar un AWS Service Catalog producto existente a un archivo de plantilla, consulta Cómo [crear nuevas conexiones de productos sincronizados](#) con Git.

Para actualizar los productos existentes a productos sincronizados con Git

1. En el panel de navegación de la izquierda, seleccione Lista de productos y, a continuación, seleccione una de las siguientes opciones:
  - Para actualizar un solo producto, seleccione el producto, vaya a la sección de Detalles de la fuente del producto y, a continuación, seleccione Editar detalles.
  - Para actualizar varios productos, seleccione Conectar productos a un repositorio externo, seleccione hasta diez productos y, a continuación, seleccione Siguiente.
2. En la sección Detalles de la fuente del producto, realice las siguientes actualizaciones:
  - Especifique la conexión.
  - Especifique el repositorio
  - Especifique la ramificación.
  - Asigne un nombre al archivo de plantilla.
3. Elija Guardar cambios.

### Note

Para los productos que aún no están conectados a un repositorio externo, puedes usar la opción Conectar a un repositorio externo que aparece en la alerta en la parte superior de la página de información del producto después de seleccionar el producto.

También puedes usar la AWS Service Catalog consola o para AWS CLI

- Conectar un AWS Service Catalog producto existente a un archivo de plantilla en un repositorio externo

- Actualice los metadatos del producto, incluyendo el nombre, la descripción y las etiquetas del producto.
- Reconfigure (actualice la sincronización para usar una fuente de repositorio diferente) una conexión para un producto AWS Service Catalog previamente conectado.

Para actualizar los detalles de la conexión y del repositorio mediante AWS Service Catalog la consola

1. En el panel de navegación izquierdo de la AWS Service Catalog consola, elija Lista de productos y, a continuación, seleccione un producto que esté conectado actualmente a un repositorio externo.
2. En la sección Detalles de la fuente del producto, seleccione Editar fuente del producto.
3. En la sección Detalles de la fuente del producto, especifique el nuevo repositorio deseado.
4. Elija Guardar cambios.

Para actualizar los detalles de la conexión y del repositorio mediante AWS CLI

A partir de la AWS CLI ejecución de los `$ aws servicecatalog update-provisioning-artifact` comandos `$ aws servicecatalog update-product` y.

## Eliminar conexiones de productos sincronizados con Git

Puedes eliminar una conexión entre un AWS Service Catalog producto y un archivo de plantilla mediante la AWS Service Catalog consola, la CodeConnections API o AWS CLI. Al desconectar un producto de un archivo de plantilla, el AWS Service Catalog producto sincronizado pasa a ser un producto gestionado de forma habitual. Tras desconectar el producto, si el archivo de plantilla se modifica y se archiva en el repositorio anteriormente conectado, los cambios no se reflejan. Para volver a conectar un AWS Service Catalog producto a un archivo de plantilla de un repositorio externo, consulte [Actualización de conexiones y productos sincronizados AWS Service Catalog](#).

Para desconectar un producto sincronizado con Git mediante la consola AWS Service Catalog

1. En el AWS Management Console, selecciona Lista de productos en el panel de navegación izquierdo.
2. Seleccione un producto de la lista.
3. En la página del Producto, vaya a la sección de Detalles de la fuente del producto.
4. Seleccione Desconectar.

## 5. Confirme la acción y, a continuación, seleccione Desconectar.

Para desconectar un producto sincronizado con Git mediante AWS CLI

Desde AWS CLI, ejecuta el comando. `$ aws servicecatalog update-product` En la entrada `ConnectionParameters`, elimine la conexión especificada.

Para eliminar una conexión mediante la CodeConnections API o AWS CLI

En la CodeConnections API o AWS CLI, ejecute el `$ aws codestar-connections delete-connection` comando.

## Sincronizar los productos de Terraform con archivos de plantilla de GitHub GitHub Enterprise o Bitbucket

Al crear un producto sincronizado con Git mediante un archivo de configuración de Terraform, la ruta del archivo solo acepta el formato `tar.gz`. No se aceptan los formatos de carpetas de Terraform en la ruta del archivo.

## Región de AWS soporte para productos sincronizados con Git

AWS Service Catalog es compatible con los productos sincronizados con Git tal y como se indica en la siguiente tabla.

Región de AWS nombre	Región de AWS identidad	Soporte para productos sincronizados con Git
Este de EE. UU. (Norte de Virginia)	us-east-1	Sí
Este de EE. UU. (Ohio)	us-east-2	Sí
Oeste de EE. UU. (Norte de California)	us-west-1	Sí
EE. UU. Oeste (Oregon)	us-west-2	Sí
África (Ciudad del Cabo)	af-south-1	No
Asia-Pacífico (Hong Kong)	ap-east-1	No
Asia-Pacífico (Yakarta)	ap-southeast-3	No

Región de AWS nombre	Región de AWS identidad	Soporte para productos sincronizados con Git
Asia-Pacífico (Bombay)	ap-south-1	Sí
Asia Pacífico (Osaka)	ap-northeast-3	No
Asia Pacífico (Seúl)	ap-northeast-2	Sí
Asia Pacífico (Singapur)	ap-southeast-1	Sí
Asia Pacífico (Sídney)	ap-southeast-2	Sí
Asia Pacífico (Tokio)	ap-northeast-1	Sí
Canadá (Central)	ca-central-1	Sí
Europa (Frankfurt)	eu-central-1	Sí
Europa (Irlanda)	eu-west-1	Sí
Europa (Londres)	eu-west-2	Sí
Europa (Milán)	eu-south-1	No
Europa (París)	eu-west-3	Sí
Europa (Estocolmo)	eu-north-1	Sí
Medio Oriente (Baréin)	me-south-1	No
América del Sur (São Paulo)	sa-east-1	Sí
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	No
AWS GovCloud (Estados Unidos-Oeste)	us-gov-west-1	No

## Eliminación de productos

Al eliminar un producto, AWS Service Catalog elimina todas las versiones de productos de todas las carteras que lo contengan.

AWS Service Catalog le permite eliminar un producto desde la consola AWS Service Catalog o AWS CLI. Para eliminar correctamente un producto, primero debe disociar todos los recursos asociados al producto. Algunos ejemplos de asociaciones de recursos de productos incluyen asociaciones de portafolios TagOptions, presupuestos y acciones de servicio.

 Important

No se puede recuperar un producto después de que se haya eliminado.

Para eliminar un producto con la consola de AWS Service Catalog

1. Vaya a la página Carteras y seleccione la cartera que contiene el producto que desea eliminar.
2. Seleccione el producto que desea eliminar y, a continuación, seleccione Eliminar en la esquina superior derecha del panel de productos.
3. En el caso de los productos sin recursos asociados, confirme el producto que desea eliminar introduciendo eliminar en el cuadro de texto y, a continuación, seleccione Eliminar.

Para los productos con recursos asociados, continúe con el paso 4.

4. En la ventana Eliminar producto, consulte la tabla de Asociaciones que muestra todos los recursos asociados al producto. AWS Service Catalog intenta disociar estos recursos al eliminar el producto.
5. Confirme que desea eliminar el producto y eliminar todos sus recursos asociados; para ello, escriba eliminar en el cuadro de texto.
6. Seleccione Disociar y eliminar.

Si AWS Service Catalog no puede disociar todos los recursos del producto, el producto no se eliminará. La ventana Eliminar producto muestra el número de disociaciones fallidas y una descripción de cada error. Para obtener más información sobre cómo resolver las disociaciones de recursos fallidas al eliminar un producto, consulte Resolver las disociaciones de recursos fallidas al eliminar un producto a continuación.

## Temas

- [Eliminar productos mediante la AWS CLI](#)
- [Resolver las disociaciones de recursos fallidas al eliminar un producto](#)

## Eliminar productos mediante la AWS CLI

AWS Service Catalog le permite usar [AWS Command Line Interface](#) (AWS CLI) para eliminar productos de su cartera. La AWS CLI es una herramienta de código abierto que le permite interactuar con los servicios de AWS mediante el uso de comandos en el shell de la línea de comandos. La función AWS Service Catalog de eliminación forzada requiere un [alias de AWS CLI](#), que es un acceso directo que se puede crear en la AWS CLI para acortar los comandos o los scripts que utiliza con frecuencia.

### Requisitos previos

- Instalar y configurar la AWS CLI. Para obtener más información, consulte [Instalación o actualización de la versión más reciente AWS CLI](#) y [Configuración básica](#). Utilice como mínimo una versión de 1.11.24 o 2.0.0 de AWS CLI.
- El alias CLI para eliminar el producto requiere un terminal compatible con bash y el procesador JSON de línea de comandos JQ. Para obtener más información sobre la instalación del procesador JSON de línea de comandos, consulte [Descargar jq](#).
- Cree un alias de AWS CLI para agrupar las llamadas a la API `Disassociation`, lo que le permitirá eliminar un producto con un solo comando.

Para eliminar correctamente un producto, primero debe disociar todos los recursos asociados al producto. Algunos ejemplos de asociaciones de recursos de productos incluyen las asociaciones de carteras, presupuestos, opciones de etiquetas y acciones de servicio. Cuando se utiliza la CLI para eliminar un producto, el alias `force-delete-product` de la CLI le permite llamar a la API `Disassociate` para disociar cualquier recurso que pudiera impedir la API `DeleteProduct`. Esto evita tener que llamar por separado a las disociaciones individuales.

#### Note

Las rutas de los archivos que se muestran en los procedimientos siguientes pueden variar en función del sistema operativo que utilice para realizar estas acciones.

### Crear un alias de AWS CLI para eliminar productos AWS Service Catalog

Cuando se utiliza la AWS CLI para eliminar un producto AWS Service Catalog, el alias `force-delete-product` de la CLI le permite llamar a la API `Disassociate` para disociar cualquier recurso que impida la llamada `DeleteProduct`.

Cree un **alias** archivo en su AWS CLI archivo de configuración.

1. En la consola AWS CLI, vaya a la carpeta de configuración. De forma predeterminada, la carpeta de configuración es `~/ .aws/` en Linux o macOS o `%USERPROFILE%\ .aws\` en Windows.
2. Cree una subcarpeta denominada `cli` mediante la navegación de archivos o introduciendo el siguiente comando en su terminal preferido:

```
$ mkdir -p ~/.aws/cli
```

La ruta predeterminada resultante de la carpeta `cli` es `~/ .aws/cli/` en Linux o macOS o `%USERPROFILE%\ .aws\cli` en Windows.

3. En la nueva carpeta `cli`, cree un archivo de texto con el nombre `alias` sin extensión. Puede crear el archivo `alias` mediante la navegación de archivos o introduciendo el siguiente comando en la terminal que prefiera:

```
$ touch ~/.aws/cli/alias
```

4. Introduzca `[toplevel]` en la primera línea.
5. Guarde el archivo.

A continuación, puede añadir el `force-delete-product` alias al `alias` archivo pegando manualmente el script del alias en el archivo o utilizando un comando en la ventana del terminal.

Añada manualmente el `force-delete-product` alias al archivo **alias**

1. En la consola AWS CLI, vaya a su carpeta de configuración AWS CLI y abra el archivo `alias`.
2. Introduzca el siguiente alias de código en el archivo, debajo de la línea `[toplevel]`:

```
[command servicecatalog]
force-delete-product =
  !f() {
    if [ "$#" -ne 1 ]; then
```

```

        echo "Illegal number of parameters"
        exit 1
    fi

    if [[ "$1" != prod-* ]]; then
        echo "Please provide a valid product id."
        exit 1
    fi

    productId=$1
    describeProductAsAdminResponse=$(aws servicecatalog describe-
product-as-admin --id $productId)
    listPortfoliosForProductResponse=$(aws servicecatalog list-
portfolios-for-product --product-id $productId)

    tagOptions=$(echo "$describeProductAsAdminResponse" | jq -r
'.TagOptions[].Id')
    budgetName=$(echo "$describeProductAsAdminResponse" | jq -r
'.Budgets[].BudgetName')
    portfolios=$(echo "$listPortfoliosForProductResponse" | jq -r
'.PortfolioDetails[].Id')
    provisioningArtifacts=$(echo "$describeProductAsAdminResponse" | jq
-r '.ProvisioningArtifactSummaries[].Id')
    provisioningArtifactServiceActionAssociations=()

    for provisioningArtifactId in $provisioningArtifacts; do
        listServiceActionsForProvisioningArtifactResponse=$(aws
servicecatalog list-service-actions-for-provisioning-artifact --product-id
$productId --provisioning-artifact-id $provisioningArtifactId)
        serviceActions=$(echo
"$listServiceActionsForProvisioningArtifactResponse" | jq -r
' [.ServiceActionSummaries[].Id] | join(",") ')
        if [[ -n "$serviceActions" ]]; then
            provisioningArtifactServiceActionAssociations
+=("${provisioningArtifactId}:${serviceActions}")
        fi
    done

    echo "Before deleting a product, the following associated resources
must be disassociated. These resources will not be deleted. This action may take
some time, depending on the number of resources being disassociated."

    echo "Portfolios:"
    for portfolioId in $portfolios; do

```

```
        echo "\t${portfolioId}"
    done

    echo "Budgets:"
    if [[ -n "$budgetName" ]]; then
        echo "\t${budgetName}"
    fi

    echo "Tag Options:"
    for tagOptionId in $tagOptions; do
        echo "\t${tagOptionId}"
    done

    echo "Service Actions on Provisioning Artifact:"
    for association in
"${provisioningArtifactServiceActionAssociations[@]}"; do
        echo "\t${association}"
    done

    read -p "Are you sure you want to delete ${productId}? y,n "
    if [[ ! $REPLY =~ ^[Yy]$ ]]; then
        exit
    fi

    for portfolioId in $portfolios; do
        echo "Disassociating ${portfolioId}"
        aws servicecatalog disassociate-product-from-portfolio --product-
id $productId --portfolio-id $portfolioId
    done

    if [[ -n "$budgetName" ]]; then
        echo "Disassociating ${budgetName}"
        aws servicecatalog disassociate-budget-from-resource --budget-
name "$budgetName" --resource-id $productId
    fi

    for tagOptionId in $tagOptions; do
        echo "Disassociating ${tagOptionId}"
        aws servicecatalog disassociate-tag-option-from-resource --tag-
option-id $tagOptionId --resource-id $productId
    done

    for association in
"${provisioningArtifactServiceActionAssociations[@]}"; do
```

```

        associationPair=(${association//:/ })
        provisioningArtifactId=${associationPair[0]}
        serviceActionsList=${associationPair[1]}
        serviceActionIds=${serviceActionsList//,/ }
        for serviceActionId in $serviceActionIds; do
            echo "Disassociating ${serviceActionId} from
${provisioningArtifactId}"
            aws servicecatalog disassociate-service-action-from-
provisioning-artifact --product-id $productId --provisioning-artifact-id
$provisioningArtifactId --service-action-id $serviceActionId
        done
    done

    echo "Deleting product ${productId}"
    aws servicecatalog delete-product --id $productId

}; f

```

### 3. Guarde el archivo.

Usa la ventana del terminal para añadir el `force-delete-product` alias a tu **alias** archivo

#### 1. Abra una ventana del terminal y ejecute el siguiente comando:

```
$ cat >> ~/.aws/cli/alias
```

#### 2. Pegue el script del alias en la ventana del terminal y, a continuación, pulse CTRL+D para salir del comando `cat`.

Llama al `force-delete-product` alias

#### 1. Ejecute los siguientes comandos en una ventana de su terminal para borrar el alias del producto.

```
$ aws servicecatalog force-delete-product {product-id}
```

El siguiente ejemplo muestra el comando `alias force-delete-product` y su respuesta resultante.

```
$ aws servicecatalog force-delete-product prod-123
```

Before deleting a product, the following associated resources must be disassociated. These resources will not be deleted. This action may take some time, depending on the number of resources being disassociated.

Portfolios:

port-123

Budgets:

budgetName

Tag Options:

tag-123

Service Actions on Provisioning Artifact:

pa-123:act-123

Are you sure you want to delete prod-123? y,n

2. Introduzca y para confirmar que desea eliminar el producto.

Tras eliminar correctamente el producto, la ventana de terminal mostrará los siguientes resultados

```
Disassociating port-123
Disassociating budgetName
Disassociating tag-123
Disassociating act-123 from pa-123
Deleting product prod-123
```

## Recursos adicionales

Para obtener más información sobre AWS CLI, el uso de alias y la eliminación de productos AWS Service Catalog, consulte los siguientes recursos:

- [Creación y uso de alias de AWS CLI](#) en la guía del usuario de (CLI) AWS Command Line Interface.
- Repositorio git de [Repositorio de alias de AWS CLI](#).
- [Eliminación de AWS Service Catalog productos](#).
- [AWSRe:Invent 2016: The Effective AWS CLI User on](#). YouTube

## Resolver las disociaciones de recursos fallidas al eliminar un producto

Si su intento anterior de [eliminar un producto](#) falló debido a excepciones de disociación de recursos, consulte la lista de excepciones y sus soluciones a continuación.

### Note

Si ha cerrado la ventana Eliminar productos antes de recibir el mensaje de disociación fallida de un recurso, puede seguir los pasos del uno al tres de la sección correspondiente Eliminar un producto para volver a abrir la ventana.

Para resolver un error en la disociación de un recurso

En la ventana Eliminar producto, revise la columna Estado de la tabla de asociaciones. Identifique la excepción de disociación de recursos fallida y las soluciones sugeridas:

Tipo de excepción de estado	Causa	Resolución
Product prod-****	AWS Service Catalog no se ha podido eliminar el producto porque el producto todavía tiene presupuestos asociados TagOptions, al menos uno ProvisioningArtifact con acciones asociadas, el producto sigue asignado a una cartera, el producto tiene usuarios o tiene restricciones.	Intente eliminar el producto de nuevo.
Usuario: username no está autorizado para ejecutar:	El usuario que intenta eliminar el producto no tiene los permisos necesarios para disociar los recursos del producto.	AWS Service Catalog recomienda ponerse en contacto con el administrador de su cuenta para obtener más información

Tipo de excepción de estado	Causa	Resolución
		sobre la disociación de recursos de productos para los que actualmente no dispone de permisos para disociar.

## Administración de versiones

Las versiones de producto se asignan cuando se crea un producto y se pueden actualizar en cualquier momento.

Las versiones tienen una plantilla de AWS CloudFormation, un título, una descripción, un estado y una guía.

### Estado de la versión

Una versión puede tener uno de estos tres estados:

- **Active (Activo)** : aparece una versión activa en la lista de versiones y permite a los usuarios lanzarla.
- **Inactive (Inactivo)** : una versión inactiva está oculta en la lista de versiones. Los productos aprovisionados existentes lanzados desde esta versión no se verán afectados.
- **Eliminado**: si se elimina una versión, se elimina de la lista de versiones. No se puede deshacer la eliminación de una versión.

### Guía de versión

Puede establecer la guía de versión para proporcionar información a los usuarios finales sobre la versión del producto. La guía de versión solo afecta a las versiones de productos activas.

Hay dos opciones para la guía de versión:

- **Ninguno** - De forma predeterminada, las versiones de los productos no incluyen ninguna guía. Los usuarios finales pueden usar esa versión para actualizar y lanzar los productos aprovisionados.
- **Obsoleto** - Los usuarios no pueden lanzar nuevos productos aprovisionados con una versión de producto obsoleta. Si un producto aprovisionado lanzado anteriormente utiliza una versión ahora

obsoleta, los usuarios solo pueden actualizar ese producto a provisionado con la versión existente o con una versión nueva.

## Actualización de versiones

Las versiones de producto se asignan al crear un producto y también puede actualizar una versión en cualquier momento. Para obtener más información acerca de la creación de un producto, consulte [Creación de productos](#).

Para actualizar una versión de producto

1. En la consola de AWS Service Catalog, seleccione Products (Productos).
2. En la lista de productos, elija el producto del que desea actualizar la versión.
3. En la página Product details (Detalles del producto), seleccione la pestaña Versions (Versiones), a continuación elija la versión que desee actualizar.
4. En la página Version details (Detalles de la versión), edite la versión del producto, a continuación, elija Save changes (Guardar cambios).

## Uso de las restricciones AWS Service Catalog

Aplique restricciones para controlar las reglas que se aplican a un producto de una cartera concreta cuando los usuarios finales lo lanzan. Cuando los usuarios finales lancen el producto, verán las reglas que haya aplicado mediante restricciones. Puede aplicar restricciones a un producto una vez que se este se incluya en una cartera. Las restricciones se activan tan pronto como se crean y se aplican a todas las versiones de un producto que no se hayan lanzado.

### Restricciones

- [Restricciones de lanzamiento AWS Service Catalog](#)
- [Restricciones de notificación de AWS Service Catalog](#)
- [Restricciones de actualización de etiquetas de AWS Service Catalog](#)
- [Restricciones de conjunto de pilas de AWS Service Catalog](#)
- [Restricciones de plantilla de AWS Service Catalog](#)

## Restricciones de lanzamiento AWS Service Catalog

Una restricción de lanzamiento especifica una función de AWS Identity and Access Management (IAM) que AWS Service Catalog supone cuando un usuario final lanza, actualiza o termina un producto. Un rol de IAM es una colección de permisos que un usuario de o servicio de puede asumir temporalmente para usar los servicios de . Para obtener un ejemplo introductorio, consulte:

- AWS CloudFormation Tipo de producto: [Paso 6: Agregar una restricción de lanzamiento para asignar un rol de IAM.](#)
- Tipo de producto Terraform Open Source o Terraform Cloud: [Paso 5: Crear roles de lanzamiento](#)

Las restricciones de lanzamiento se aplican a los productos de la cartera (asociación producto-cartera). Las restricciones de lanzamiento no se aplican a nivel de cartera ni a un producto en todas las carteras. Para asociar una restricción de lanzamiento con todos los productos de una cartera, debe aplicar la restricción de lanzamiento individualmente a cada producto.

Sin una restricción de lanzamiento, los usuarios finales deben lanzar y administrar los productos con sus propias credenciales de IAM;. Para ello, deben tener permisos para AWS CloudFormation, los servicios de AWS que los productos utilizan y AWS Service Catalog. En cambio, el uso de un rol de lanzamiento permite limitar los permisos de los usuarios finales al mínimo necesario para el producto en cuestión. Para obtener más información acerca de los permisos de los usuarios finales, consulte [Administración de identidad y acceso en AWS Service Catalog](#).

Para crear y asignar roles de IAM;, debe contar con los siguientes permisos administrativos de IAM:

- iam:CreateRole
- iam:PutRolePolicy
- iam:PassRole
- iam:Get\*
- iam:List\*

### Configuración de un rol de lanzamiento

El rol de IAM que se asigna a un producto como restricción de lanzamiento debe tener permisos para utilizar lo siguiente:

Para los productos de Cloudformation

- La `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess` AWS CloudFormation política administrada
- Los servicios en la plantilla de AWS CloudFormation del producto;
- Acceso de solo lectura a la plantilla de AWS CloudFormation en un bucket de Amazon S3 propiedad del servicio.

#### Para productos Terraform

- los servicios utilizados en la plantilla de Amazon S3 del producto;
- Acceso de solo lectura a la plantilla de Amazon S3 en un bucket de Amazon S3 propiedad del servicio.
- `resource-groups:Tag` para etiquetar en una instancia de Amazon EC2 (asumido por el motor de aprovisionamiento Terraform al realizar operaciones de aprovisionamiento)
- `resource-groups:CreateGroup` para el etiquetado de grupos de recursos (asumido por AWS Service Catalog para crear grupos de recursos y asignar etiquetas)

La política de confianza del rol de IAM debe permitir a AWS Service Catalog asumir el rol. En el siguiente procedimiento, la política de confianza se establecerá automáticamente al seleccionar AWS Service Catalog como el tipo de rol. Si no utiliza la consola, consulte la sección Crear políticas de confianza para los servicios de AWS que asumen roles en [Cómo utilizar las políticas de confianza con los roles de IAM](#).

#### Note

Los permisos `servicecatalog:ProvisionProduct`, `servicecatalog:TerminateProvisionedProduct` y `servicecatalog:UpdateProvisionedProduct` no se pueden asignar en una función de lanzamiento. Debe usar los roles de IAM tal y como se muestra en los pasos de la política en línea en la sección [Conceder permisos a AWS Service Catalog los usuarios finales](#).

#### Note

Para ver los productos y recursos de Cloudformation aaaprovisionado en la consola AWS Service Catalog, los usuarios finales necesitan acceso de lectura al AWS CloudFormation.

Para ver los productos y recursos aaprovisionados en la consola no se utiliza el rol de lanzamiento.

Para crear un rol de lanzamiento

1. Abra la consola de IAM en <https://console.aws.amazon.com/iam/>.

Los productos de Terraform requieren configuraciones de roles de lanzamiento adicionales. Para obtener más información, consulte el [Paso 5: Crear roles de lanzamiento](#) en Cómo empezar con un producto de Terraform Open Source.

2. Elija Roles.
3. Elija Crear nuevo rol.
4. Escriba un nombre de función y elija Next Step.
5. En AWS Roles de Servicio elegir AWS Service Catalog Seleccionar.
6. En la página Attach Policy, elija Next Step.
7. Para crear una función, elija Create Role.

Para adjuntar una política al nuevo rol

1. Elija la función que ha creado para ver la página de detalles de dicha función.
2. Elija la pestaña Permissions y, a continuación, expanda la sección Inline Policies. A continuación, elija click here.
3. Elija Custom Policy y después Select.
4. Introduzca un nombre para la política y, a continuación, pegue lo siguiente en el editor Policy Document:

```
    "Statement":[
  {
    "Effect":"Allow",
    "Action":[
      "s3:GetObject"
    ],
    "Resource":"*",
    "Condition":{"
      "StringEquals":{
```

```

    "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
  }
}
]
}

```

#### Note

Al configurar un rol de lanzamiento para una restricción de lanzamiento, debe usar esta cadena: "s3:ExistingObjectTag/servicecatalog:provisioning": "true".

5. Agregue una línea a la política por cada servicio adicional que el producto utilice. Por ejemplo, si desea agregar permiso para Amazon Relational Database Service (Amazon RDS), escriba una coma al final de la última línea de la lista `Action` y, a continuación, agregue la siguiente línea:

```
"rds:*"
```

6. Seleccione `Apply Policy`.

## Aplicación de una restricción de lanzamiento

Tras configurar el rol de lanzamiento, asigne el rol al producto como una restricción de lanzamiento. Esta acción indica a AWS Service Catalog que debe asumir la función cuando un usuario final lance el producto.

Para asignar el rol a un producto

1. Abra la consola de Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. Elija la cartera que contiene el producto.
3. Elija la pestaña `Constraints (Restricciones)` y elija `Create constraint (Crear restricción)`.
4. Elija el producto en `Product (Producto)` y elija `Launch (Lanzar)` en `Constraint type (Tipo de restricción)`. Elija `Continuar`.
5. En la sección `Restricción de lanzamiento`, puede seleccionar un rol de IAM de su cuenta y especificar un ARN de rol de IAM o escribir el nombre del rol.

Si especifica el nombre del rol si una cuenta utilice la restricción de lanzamiento, se utilizará el rol de IAM con ese nombre en la cuenta. Este enfoque permite que las restricciones del rol de

lanzamiento sean independientes de la cuenta, de modo que pueda crear menos recursos por cuenta compartida.

 Note

El nombre del rol especificado debe existir en la cuenta creada para crear la restricción de lanzamiento y la cuenta del usuario que lanza un producto con esta restricción de lanzamiento.

6. Después de especificar el rol de IAM, elija Create (Crear).

## Añadir Confused Deputy a una restricción de lanzamiento

AWS Service Catalog admite la protección de [Confused Deputy](#) para las API que se ejecutan con una solicitud de Assume Role. Al añadir una restricción de lanzamiento, puede restringir el acceso a al rol de lanzamiento mediante las condiciones de la política de confianza del rol de lanzamiento `sourceAccount` y `sourceArn`. Garantiza que el rol de lanzamiento sea llamado por una fuente confiable.

En el siguiente ejemplo, la AWS Service Catalog usuario final pertenece a la cuenta 111111111111. Cuando el administrador AWS Service Catalog crea una `LaunchConstraint` para un producto, el usuario final puede especificar las siguientes condiciones en la política de confianza del rol de lanzamiento para restringir asumir el rol a la cuenta 111111111111.

```
"Condition":{
  "ArnLike":{
    "aws:SourceArn":"arn:aws:servicecatalog:us-east-1:111111111111:*"
  },
  "StringEquals":{
    "aws:SourceAccount":"111111111111"
  }
}
```

Un usuario que aprovisiona un producto con la `LaunchConstraint` debe tener el mismo `AccountId` (111111111111). En caso contrario, la operación falla con un error `AccessDenied`, lo que impide un uso indebido del rol de lanzamiento.

Las siguientes API AWS Service Catalog están protegidas para la protección de Confused Deputy:

- `LaunchConstraint`
- `ProvisionProduct`
- `UpdateProvisionedProduct`
- `TerminateProvisionedProduct`
- `ExecuteProvisionedProductServiceAction`
- `CreateProvisionedProductPlan`
- `ExecuteProvisionedProductPlan`

La protección `sourceArn` para AWS Service Catalog solo admite ARN con plantillas, como `"arn:<aws-partition>:servicecatalog:<region>:<accountId>:"`. No admite ARN de recursos específicos.

## Verificar la restricción de lanzamiento

Para comprobar que AWS Service Catalog utiliza la función para lanzar el producto y que el producto aprovisionado se ha creado correctamente, lance el producto desde la consola de AWS Service Catalog. Para probar una restricción antes de distribuirla a los usuarios, cree una cartera de prueba que contenga los mismos productos y pruebe las restricciones con ella.

Para lanzar el producto

1. En el menú de la consola de AWS Service Catalog, elija Catálogo de Servicios y Usuario final.
2. Elija el producto para abrir la página Detalles del producto. En la tabla Opciones de lanzamiento, compruebe que aparezca el nombre de recurso de Amazon (ARN) de la función.
3. Seleccione Lanzar producto.
4. Continúe con los demás pasos del lanzamiento y rellene la información que se le pida.
5. Compruebe que el producto se inicia correctamente.

## Restricciones de notificación de AWS Service Catalog

### Note

AWS Service Catalog no admite restricciones de notificación para los productos Terraform Open Source o Terraform Cloud.

Una restricción de notificación especifica un tema de Amazon SNS para recibir notificaciones sobre los eventos de la pila.

Utilice el siguiente procedimiento para crear un tema de SNS y suscríbase a él.

Para crear un tema de SNS y una suscripción

1. Abra la consola de Amazon SNS en <https://console.aws.amazon.com/sns/v3/home>.
2. Elija Crear nuevo tema.
3. Escriba el nombre del tema y, a continuación, elija Create topic.
4. Seleccione Crear suscripción.
5. En Protocol, seleccione Email. En Endpoint, escriba una dirección de correo electrónico que pueda utilizar para recibir notificaciones. Seleccione Create subscription.
6. Recibirá un email de confirmación con el asunto AWS Notification - Subscription Confirmation. Abra el mensaje y siga las instrucciones para completar la suscripción.

Utilice el siguiente procedimiento para aplicar una restricción de notificación mediante el tema de SNS que ha creado en el procedimiento anterior.

Para aplicar una restricción de notificación a un producto

1. Abra la consola de Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. Elija la cartera que contiene el producto.
3. Expanda Constraints (Restricciones) y elija Add constraints (Añadir restricciones).
4. Elija el producto de Producto and establezca Tipo de restricción a Notificación. Elija Continuar.
5. Elija Choose a topic from your account y seleccione el tema de SNS que ha creado en Topic Name.
6. Elija Enviar.

## Restricciones de actualización de etiquetas de AWS Service Catalog

### Note

AWS Service Catalog no admite las restricciones de actualización de etiquetas para los productos de Terraform Open Source.

Mediante las restricciones de actualización de etiquetas, AWS Service Catalog los administradores de pueden autorizar o no autorizar que los usuarios finales actualicen las etiquetas en los recursos asociados a un producto aaprovisionado. Si se autoriza la actualización de etiquetas, se aplicarán nuevas etiquetas asociadas a la cartera o al producto de a los recursos aaaprovisionado durante la actualización de un producto aaprovisionado.

Para habilitar las actualizaciones de etiquetas de un producto

1. Abra la consola de Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. Elija la cartera que contiene el producto que desea actualizar.
3. Elija la pestaña Restricciones y elija Crear restricción.
4. En Constraint type (Tipo de restricción), elija Tag Update (Actualización de etiquetas).
5. Elija el producto en Product (Producto) y, a continuación, seleccione Continue (Continuar).
6. En la página Tag Updates (Actualizaciones de etiquetas), seleccione Enable Tag Updates (Habilitar actualizaciones de etiquetas).
7. Elija Enviar.

## Restricciones de conjunto de pilas de AWS Service Catalog

### Note

- AWS Service Catalog no admite restricciones de conjuntos de pilas para los productos de Terraform Open Source.
- AutoTags actualmente no son compatibles con AWS CloudFormation StackSets.

Una restricción de conjunto de pilas permite configurar las opciones de despliegue de productos mediante AWS CloudFormation StackSets. Puede especificar varias cuentas y regiones para el lanzamiento del producto. Los usuarios finales pueden administrar esas cuentas y determinar dónde se implementan los productos y el orden de implementación.

Para aplicar una restricción de conjunto de pilas a un producto

1. Abra la consola de Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. Seleccione la cartera con el producto que desee.

3. Elija la pestaña Restricciones y luego elija Crear restricción.
4. En Producto, seleccione el producto. En Tipo de restricción, seleccione Conjunto de pilas.
5. Configure las cuentas, las regiones y los permisos para las restricciones de su conjunto de pilas.
  - En la Configuración de la cuenta, identifique las cuentas en las que desea crear los productos.
  - En la Configuración regional, seleccione las regiones geográficas en las que desea implementar los productos y el orden en el que desea que se implementen esos productos en esas regiones.
  - En Permisos, elija un rol de StackSet administrador de IAM para administrar sus cuentas de destino. Si no eliges un rol, StackSets usa el ARN predeterminado. [Obtenga más información sobre la configuración de permisos de conjunto de pilas.](#)
6. Seleccione Crear.

## Restricciones de plantilla de AWS Service Catalog

### Note

AWS Service Catalog no admite restricciones de plantilla para los productos Terraform Open Source o Terraform Cloud.

Para limitar las opciones que los usuarios finales tienen a su disposición cuando lanzan un producto, se aplican restricciones de plantilla. Aplique restricciones de plantilla para asegurarse de que los usuarios finales puedan usar los productos sin infringir los requisitos de conformidad de la organización. Puede aplicar las restricciones de plantilla a un producto de una cartera de AWS Service Catalog. Una cartera debe contener uno o varios productos para que sea posible definir restricciones de plantilla.

Una restricción de plantilla consta de una o varias reglas que filtran los valores admisibles de los parámetros que se definen en la plantilla de AWS CloudFormation subyacente del producto. Los parámetros de una plantilla de AWS CloudFormation definen el conjunto de valores que los usuarios pueden especificar al crear una pila. Por ejemplo, un parámetro puede definir los distintos tipos de instancias que los usuarios pueden elegir al lanzar una pila que incluya instancias EC2.

Si el conjunto de valores de parámetros de una plantilla es demasiado amplio para los destinatarios de la cartera, puede definir restricciones de plantilla con el fin de limitar los valores que los usuarios pueden elegir al lanzar un producto. Por ejemplo, si los parámetros de plantilla incluyen tipos

de instancias EC2 que son demasiado grandes para los usuarios (pues estos que deben utilizar únicamente tipos de instancia pequeña, como `t2.micro` o `t2.small`), entonces puede agregar una restricción de plantilla para limitar los tipos de instancias que los usuarios finales pueden elegir. Para obtener más información acerca de los parámetros de plantilla de AWS CloudFormation, consulte [Parámetros](#) en la Guía del usuario de AWS CloudFormation.

Las restricciones de plantilla están vinculadas a una cartera. Si se aplican restricciones de plantilla a un producto de una cartera y, a continuación, se incluye el producto en otra cartera, las restricciones no se aplicarán al producto en la segunda cartera.

Si se aplica una restricción de plantilla a un producto que ya se ha compartido con los usuarios, la restricción se activará de inmediato para todos los lanzamientos de productos posteriores y para todas las versiones del producto que contenga esa cartera.

Puede definir reglas de restricción de plantilla mediante un editor de reglas o escribiendo las reglas como texto JSON en la consola del administrador de AWS Service Catalog. Para obtener más información sobre las reglas, su sintaxis y ejemplos, consulte [Reglas de restricciones de plantilla](#).

Para probar una restricción antes de distribuirla a los usuarios, cree una cartera de prueba que contenga los mismos productos y pruebe las restricciones con ella.

Para aplicar restricciones de plantilla a un producto

1. Abra la consola de Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. En la página Portfolios, elija la cartera que contiene el producto al que desee aplicar una restricción de plantilla.
3. Expanda Restricciones y elija Añadir restricciones.
4. En la ventana Seleccionar el producto y el tipo, para Producto elija el producto para el que desea definir las restricciones de plantilla. A continuación, en Tipo de restricción, elija Plantilla. Elija Continuar.
5. En la página Template constraint builder edite las reglas de restricción mediante el editor de JSON o la interfaz del constructor de reglas.
  - Para editar el código JSON de la regla, elija la pestaña Constraint Text Editor. En esta pestaña se proporcionan varios ejemplos para ayudarlo a comenzar.

Para crear las reglas mediante una interfaz de constructor de reglas, elija la pestaña Rule Builder. En ella, puede elegir cualquier parámetro que se especifica en la plantilla del producto e indicar los valores admisibles para ese parámetro. En función del tipo de parámetro,

debe indicar los valores admisibles eligiendo los elementos en una lista de comprobación, especificando un número o especificando un conjunto de valores separados por comas en una lista.

Cuando haya terminado de crear la regla, elija **Añadir regla**. La regla aparecerá en la tabla en la pestaña **Creador de reglas**. Para revisar y editar el resultado JSON, elija la pestaña **Editor de texto de restricción**.

6. Cuando haya terminado de editar las reglas de la restricción, elija **Enviar**. Para ver la restricción, vaya a la página de detalles de la cartera y amplíe **Restricciones**.

## Reglas de restricciones de plantilla

Las reglas que definen las restricciones de plantilla de AWS Service Catalog describen cuándo los usuarios finales pueden utilizar la plantilla y qué valores pueden especificar para los parámetros que se declaran en la plantilla de AWS CloudFormation usada para crear el producto que desean utilizar. Las reglas son útiles para impedir que los usuarios finales especifiquen accidentalmente un valor incorrecto. Por ejemplo, puede agregar una regla que compruebe si los usuarios finales han especificado una subred válida en una VPC determinada o han usado tipos de instancia de `m1.small` para los entornos de pruebas. AWS CloudFormation utiliza reglas para validar los valores del parámetro antes de que cree los recursos del producto.

Cada regla consta de dos propiedades: una condición de regla (opcional) y declaraciones (obligatorias). La condición de regla determina cuándo surte efecto una regla. Las declaraciones describen qué valores pueden especificar los usuarios para un parámetro determinado. Si no se define la condición de regla, las declaraciones de la regla surten efecto en todos los casos. Para definir una condición de regla y las declaraciones, se utilizan funciones intrínsecas específicas de reglas, que son funciones que solo se pueden utilizar en la sección `Rules` de una plantilla. Puede anidar funciones, pero el resultado final de una condición de regla o una declaración debe ser verdadero o falso.

Por ejemplo, supongamos que ha declarado una VPC y un parámetro de subred en la sección `Parameters`. Puede crear una regla que valide que una subred determinada está en una VPC. Por lo tanto, cuando un usuario especifica una VPC, AWS CloudFormation evalúa la declaración para comprobar si el valor del parámetro de subred pertenece a esa VPC antes de crear o actualizar la pila. Si el valor del parámetro no es válido, AWS CloudFormation no creará ni actualizará la pila. Si los usuarios no especifican una VPC, AWS CloudFormation no comprobará el valor del parámetro de subred.

## Sintaxis

La sección `Rules` de una plantilla consta del nombre de clave `Rules`, seguido de un único signo de dos puntos. Todas las declaraciones de regla van entre llaves. Si se declaran varias reglas, deben delimitarse mediante comas. Para cada regla, se declara un nombre lógico entre comillas seguido de un signo de dos puntos y de las llaves que contienen la condición de regla y las declaraciones.

Una regla puede incluir una propiedad `RuleCondition` y necesariamente debe incluir una propiedad `Assertions`. Para cada regla, se puede definir una sola condición de regla. En la propiedad `Assertions` se pueden definir una o varias declaraciones. Puede definir una condición de regla y declaraciones mediante funciones intrínsecas específicas de reglas, como se muestra en la siguiente pseudoplantilla:

```
"Rules":{
  "Rule01":{
    "RuleCondition":{
      "Rule-specific intrinsic function"
    },
    "Assertions":[
      {
        "Assert":{
          "Rule-specific intrinsic function"
        },
        "AssertDescription":"Information about this assert"
      },
      {
        "Assert":{
          "Rule-specific intrinsic function"
        },
        "AssertDescription":"Information about this assert"
      }
    ]
  },
  "Rule02":{
    "Assertions":[
      {
        "Assert":{
          "Rule-specific intrinsic function"
        },
        "AssertDescription":"Information about this assert"
      }
    ]
  }
}
```

```

    }
  }
}

```

La pseudoplantilla muestra una sección de `Rules` que contiene dos reglas con el nombre `Rule01` y `Rule02`. `Rule01` incluye una condición de regla y dos declaraciones. Si la función de la condición de regla se evalúa en `true` (verdadero), se evalúan y aplican ambas funciones en cada declaración. Si la condición de regla es falsa, la regla no surte efecto. `Rule02` siempre surte efecto porque no tiene una condición de regla, lo que significa que la afirmación siempre se evalúa y aplica.

Para obtener información sobre las funciones intrínsecas específicas de las reglas para definir las condiciones y afirmaciones de las reglas, consulte [Funciones de regla de AWS](#) en la Guía del usuario de AWS CloudFormation.

Ejemplo: comprobación condicional del valor de un parámetro

Las dos reglas siguientes comprueban el valor del parámetro `InstanceType`. En función del valor del parámetro `Environment` (`test` o `prod`), el usuario debe especificar `m1.small` o `m1.large` para el parámetro `InstanceType`. Los parámetros `InstanceType` y `Environment` deben declararse en la sección `Parameters` de la misma plantilla.

```

"Rules" : {
  "testInstanceType" : {
    "RuleCondition" : {"Fn::Equals":[{"Ref":"Environment"}, "test"]},
    "Assertions" : [
      {
        "Assert" : { "Fn::Contains" : [ ["m1.small"], {"Ref" : "InstanceType"} ] },
        "AssertDescription" : "For the test environment, the instance type must be
m1.small"
      }
    ]
  },
  "prodInstanceType" : {
    "RuleCondition" : {"Fn::Equals":[{"Ref":"Environment"}, "prod"]},
    "Assertions" : [
      {
        "Assert" : { "Fn::Contains" : [ ["m1.large"], {"Ref" : "InstanceType"} ] },
        "AssertDescription" : "For the prod environment, the instance type must be
m1.large"
      }
    ]
  }
}

```

}

## Acciones de servicio de AWS Service Catalog

### Note

AWS Service Catalog no admite acciones de servicio para los productos Terraform Open Source o Terraform Cloud.

AWS Service Catalog le permite reducir el mantenimiento administrativo y la formación técnica de los usuarios finales a la vez que se cumplen las medidas de conformidad y seguridad. Con las acciones de servicio, como administrador, puede permitir a los usuarios finales que realicen tareas operativas, solucionen problemas, ejecuten comandos aprobados o soliciten permisos en AWS Service Catalog. Los [documentos de AWS Systems Manager](#) se utilizan para definir acciones. Los [documentos de AWS Systems Manager](#) proporcionan acceso a acciones predefinidas que implementan las AWS prácticas recomendadas, como detener y reiniciar Amazon EC2, y también puede definir acciones personalizadas.

En este tutorial proporcionará a los usuarios finales la capacidad de reiniciar una instancia Amazon EC2. Añadirá los permisos necesarios, definirá la acción de servicio, asociará la acción de servicio con un producto y probará la experiencia del usuario final utilizando la acción con un producto aprovisionado.

## Requisitos previos

En este tutorial se supone que tiene todos los permisos de administrador de AWS, que ya está familiarizado con AWS Service Catalog y que ya tiene un conjunto básico de productos, paquetes y usuarios. Si no está familiarizado con AWS Service Catalog, complete la tareas de [configuración](#) y [Introducción](#) antes de utilizar este tutorial.

### Temas

- [Paso 1: Configurar los permisos de usuario final](#)
- [Paso 2: Crear una acción de servicio](#)
- [Paso 3: Asociar la acción de servicio con una versión de producto](#)
- [Paso 4: Probar la experiencia del usuario final](#)

- [Paso 5: Administrar las acciones de servicio con AWS CloudFormation](#)
- [Paso 6: Solución de problemas](#)

## Paso 1: Configurar los permisos de usuario final

Los usuarios finales deben tener los permisos necesarios para ver y realizar acciones de servicio específicas. En este ejemplo, el usuario final necesita permiso para obtener acceso a la característica de AWS Service Catalog acciones de servicio de y para realizar un reinicio de Amazon EC2.

Para actualizar los permisos

1. Abra la AWS Identity and Access Management consola de IAM en <https://console.aws.amazon.com/iam/>.
2. En el menú, localice los grupos de usuarios.
3. Seleccione los grupos que los usuarios finales utilizarán para acceder a los recursos AWS Service Catalog. En este ejemplo, seleccionamos el grupo de usuarios finales. En su propia implementación, elija el grupo que utilizan los usuarios finales relevantes.
4. En la pestaña Permissions (Permisos) de la página de detalles de su grupo, puede crear una nueva política o editar una existente. En este ejemplo, añadimos permisos a la política existente seleccionando la política personalizada creada para los permisos Aprovisionar y Terminar de AWS Service Catalog del grupo.
5. En la página Policy (Política), seleccione Edit Policy (Editar política) para agregar los permisos necesarios. Puede utilizar el editor visual o el editor JSON para editar la política. En este ejemplo, utilizamos el editor JSON para añadir los permisos. Para este tutorial, añada los siguientes permisos a la política:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1536341175150",
      "Action": [
        "servicecatalog:ListServiceActionsForProvisioningArtifact",
        "servicecatalog:ExecuteProvisionedProductServiceAction",
        "ssm:DescribeDocument",
        "ssm:GetAutomationExecution",
```

```
"ssm:StartAutomationExecution",
"ssm:StopAutomationExecution",
"cloudformation:ListStackResources",
"ec2:DescribeInstanceStatus",
"ec2:StartInstances",
"ec2:StopInstances"
],
"Effect": "Allow",
"Resource": "*"
}
]
}
```

6. Después de editar la política, revise y apruebe el cambio en ella. Los usuarios del grupo de usuarios finales ahora tienen los permisos necesarios para realizar la acción de reinicio de Amazon EC2 en AWS Service Catalog.

## Paso 2: Crear una acción de servicio

A continuación, creará una acción de servicio para reiniciar las instancias Amazon EC2.

1. Abra la AWS Service Catalog consola en <https://console.aws.amazon.com/sc/>.
2. En el menú, elija Service actions (Acciones de servicio).
3. En la página acciones de servicio, elija Crear acción.
4. En la página Create action (Crear acción), elija un documento de AWS Systems Manager para definir la acción de servicio. La acción de reinicio de instancia Amazon EC2 está definida por un AWS Systems Manager documento, por lo que mantenemos la opción predeterminada en el menú desplegable Documentos de Amazon.
5. Busque y seleccione la acción AWS-RestartEC2Instance.
6. Proporcione un nombre y una descripción a la acción que tenga sentido para su entorno y su equipo. El usuario final verá esta descripción, así que elija algo que le ayude a entender lo que hace la acción.
7. En Configuración de parámetro y destino, elija el parámetro de documento de SSM que será el destino de la acción (por ejemplo, el ID de instancia) y elija el destino del parámetro. Seleccione Add parameter (Añadir parámetro) para añadir parámetros adicionales.
8. En Permissions (Permisos), elija un rol. Estamos usando permisos predeterminados para este ejemplo. Son posibles otras configuraciones de permisos y están definidas en esta página.

9. Después de revisar la configuración, elija **Create action** (Crear acción).
10. En la página siguiente, aparece una confirmación cuando se ha creado la acción y está lista para utilizarse.

## Paso 3: Asociar la acción de servicio con una versión de producto

Después de definir una acción, debe asociar un producto a dicha acción.

1. En la página acciones de servicio, elija **AWS-RestartEC2instance** y a continuación, **Asociar acción**.
2. En la página **Associate action** (Asociar acción), elija el producto en el que desea que sus usuarios finales realicen la acción de servicio. En este ejemplo, elegimos **Linux Desktop** (Escritorio Linux).
3. Seleccione una versión del producto. Tenga en cuenta que puede utilizar la casilla de verificación superior para seleccionar todas las versiones.
4. Elija **Associate action** (Asociar acción).
5. En la página siguiente aparece un mensaje de confirmación.

Ha creado la acción de servicio en AWS Service Catalog. El siguiente paso de este tutorial es utilizar la acción de servicio como usuario final.

## Paso 4: Probar la experiencia del usuario final

Los usuarios finales pueden realizar acciones de servicio en los productos aprovisionados. Para los fines de este tutorial, el usuario final debe tener al menos un producto aprovisionado. El producto aprovisionado debe lanzarse desde la versión del producto que asoció con la acción de servicio en el paso anterior.

Para obtener acceso a la acción de servicio como usuario final

1. Inicie sesión en la consola de AWS Service Catalog como usuario final.
2. En el panel de AWS Service Catalog, en el panel de navegación, seleccione **Provisioned products list** (Lista de productos aprovisionados). La lista muestra los productos que se aprovisionan para la cuenta del usuario final.
3. En la página **Provisioned products list** (Lista de productos aprovisionados), elija la instancia que está aprovisionada.

4. En la página Detalles de producto aprovisionado, elija Acciones en la parte superior derecha y, a continuación, seleccione la acción AWSAWS-RestartEC2instance.
5. Confirme que desea ejecutar la acción personalizada. Recibirá una confirmación de que se ha enviado la acción.

## Paso 5: Administrar las acciones de servicio con AWS CloudFormation

Puede crear acciones de servicio y sus asociaciones con los recursos de AWS CloudFormation. Para obtener más información, consulte lo indicado en la Guía del usuario de AWS CloudFormation:

- [AWS::ServiceCatalog::CloudFormationProducto ProvisioningArtifactProperties](#)
- [AWS::ServiceCatalog::ServiceActionAsociación](#)

### Note

Si administra las asociaciones de acciones de servicio con recursos de AWS CloudFormation, no añada ni elimine acciones de servicio mediante el comando AWS Command Line Interface o AWS Management Console. Cuando actualiza una pila, se sustituyen todos los cambios en las acciones del servicio que se hayan realizado fuera de AWS CloudFormation.

## Paso 6: Solución de problemas

Si la ejecución de la acción de servicio produce un error, puede encontrar el mensaje de error en la sección Outputs (Salidas) del evento de ejecución de acción de servicio en la página Provisioned product (Producto aprovisionado). A continuación, puede consultar las explicaciones de los mensajes de error comunes que puede encontrar.

### Note

El texto exacto de los mensajes de error está sujeto a cambios, por lo que debe evitar usarlos en cualquier tipo de proceso automatizado.

### Internal Failure (Error interno)

AWS Service Catalog experimentó un error interno. Inténtelo de nuevo más tarde. Si el error persiste, póngase en contacto con el servicio de atención al cliente.

Se ha producido un error (ThrottlingException) al llamar a la StartAutomationExecution operación

La ejecución de la acción del servicio se limitó por el servicio backend, como SSM.

Access denied while assuming the role (Acceso denegado al asumir el rol)

AWS Service Catalog no pudo asumir el rol especificado en la definición de la acción del servicio. Asegúrese de que la entidad principal servicecatalog.amazonaws.com o una entidad principal regional como servicecatalog.us-east-1.amazonaws.com esté incluida en la lista de la política de confianza del rol.

Se produjo un error (AccessDeniedException) al llamar a la StartAutomationExecution operación: el usuario no está autorizado a realizar: ssm: StartAutomationExecution en el recurso.

El rol especificado en la definición de la acción de servicio no tiene permisos para invocar ssm: StartAutomationExecution Asegúrese de que el rol tiene los permisos de SSM adecuados.

No se encuentra ningún recurso con el tipo **TargetType** en el producto aprovisionado

El producto aaprovisionado no contiene ningún recurso que coincida con el tipo de destino especificado en el documento de AWS, como AWS::EC2::Instance. Compruebe el producto aaprovisionado para estos recursos o confirme que el documento es correcto.

Document with that name does not exist (El documento con ese nombre no existe)

El documento especificado en la definición de acción del servicio no existe.

Failed to describe SSM Automation document (Se ha producido un error al describir el documento de automatización de SSM)

AWS Service Catalog encontró una excepción desconocida de al intentar describir el documento especificado.

Failed to retrieve credentials for role (Se ha producido un error al recuperar las credenciales para el rol)

AWS Service Catalog encontró un error desconocido al asumir el rol especificado.

El parámetro tiene el valor «**InvalidValue**» y no se encuentra en **{ValidValue1}**, **{ValidValue2}**

El valor del parámetro pasado a SSM no está en la lista de valores permitidos para el documento. Confirme que los parámetros proporcionados son válidos e inténtelo de nuevo.

Error de tipo de parámetro. El valor proporcionado para no **ParameterName** es una cadena válida.

El valor del parámetro pasado a SSM no es válido para el tipo del documento.

Parameter is not defined in service action definition (El parámetro no está definido en la definición de acción del servicio)

Se ha pasado un parámetro a AWS Service Catalog que no está definido en la definición de la acción del servicio. Solo puede utilizar parámetros definidos en la definición de acción del servicio.

El paso falla cuando está ejecutando/cancelando la acción. **Mensaje de error**. Por favor, consulte la guía de solución de problemas del servicio de automatización para obtener más detalles de diagnóstico.

Se ha producido un error en un paso del documento de automatización de SSM. Consulte el error en el mensaje para solucionar más problemas.

Los siguientes valores para el parámetro no están permitidos porque no están en el producto aprovisionado: **InvalidResourceId**

El usuario solicitó la acción en un recurso que no está en el producto aprovisionado.

TargetType no definido para el documento de automatización de SSM

Las acciones de servicio requieren que los documentos de automatización de SSM tengan una TargetType definición. Compruebe su documento de automatización de SSM.

## Adición de productos de AWS Marketplace a la cartera

Puede agregar productos de AWS Marketplace a las carteras para ponerlos a disposición de los usuarios finales de AWS Service Catalog.

AWS Marketplace es una tienda online donde encontrará una amplia selección de software y servicios a los que puede suscribirse para comenzar a utilizarlos de inmediato. AWS Marketplace contiene diversos tipos de productos, tales como bases de datos, servidores de aplicaciones, herramientas de pruebas, herramientas de monitorización, herramientas de administración de

contenidos y software de inteligencia empresarial. AWS Marketplace está disponible en <https://aws.amazon.com/marketplace>. Tenga en cuenta que no puede añadir productos de software como servicio (SaaS) de AWS Marketplace a AWS Service Catalog.

Para distribuir un producto AWS Marketplace a los usuarios finales AWS Service Catalog, usted copia el producto con la plantilla AWS CloudFormation a AWS Service Catalog y, a continuación, añade el producto a una cartera.

#### Note

AWS Service Catalog no admite la distribución de productos AWS Marketplace a los usuarios finales AWS Service Catalog mediante una plantilla de producto de Terraform Open Source o Terraform Cloud.

AWS Marketplace admite AWS Service Catalog directamente o puede suscribirse y agregar los productos manualmente. Recomendamos agregar los productos mediante la funcionalidad diseñada expresamente para AWS Service Catalog.

## Administración de productos de AWS Marketplace mediante AWS Service Catalog

Puede agregar los productos de AWS Marketplace a los que se ha suscrito directamente a AWS Service Catalog mediante una interfaz personalizada. En [AWS Marketplace](#), elija Service Catalog (Catálogo de servicios). Para obtener más información, consulte la página sobre [cómo copiar productos en AWS Service Catalog](#) en la AWS Marketplace sección de ayuda y preguntas frecuentes de.

## Administración y adición manual de productos de AWS Marketplace

Los pasos siguientes permiten suscribirse a un producto de AWS Marketplace, definirlo en una plantilla de AWS CloudFormation y agregar esta última a una cartera de AWS Service Catalog.

Para suscribirse a un producto de AWS Marketplace

1. Vaya a AWS Marketplace en <https://aws.amazon.com/marketplace>.
2. Examine los productos o realice una búsqueda para encontrar el que desea agregar a la cartera de AWS Service Catalog. Elija el producto para ver la página de detalles del producto.

3. Elija Continuar para ver la página de tramitación y, a continuación, elija la pestaña Lanzamiento manual.

La información de la página de tramitación incluye los tipos de instancias Amazon Elastic Compute Cloud (Amazon EC2) admitidas, las regiones de AWS admitidas y el identificador de imagen de máquina de Amazon (AMI) que el producto utiliza para cada región de AWS. Tenga en cuenta que algunas opciones afectarán a los costos. Esta información se utiliza para personalizar la plantilla de AWS CloudFormation en los siguientes pasos.

4. Elija Accept Terms para suscribirse al producto.

Después de suscribirse a un producto, puede obtener acceso a la información de la página de tramitación de AWS Marketplace en cualquier momento; para ello, elija Your Software (Su software) y, a continuación, elija el producto.

Para definir el producto de AWS Marketplace en una plantilla de AWS CloudFormation

Para completar los pasos siguientes, utilizará una de las plantillas de muestra de AWS CloudFormation como punto de partida y personalizará la plantilla para que represente el producto de AWS Marketplace. Para obtener acceso a las plantillas de ejemplo, consulte el artículo sobre [plantillas de ejemplo](#) en la Guía del usuario de AWS CloudFormation.

1. En la página Plantillas de ejemplo de la Guía del usuario de AWS CloudFormation, elija la AWS región para su producto. La AWS región debe ser compatible con el producto de AWS Marketplace. Puede ver las regiones compatibles en la página de tramitación del producto de AWS Marketplace.
2. Para ver una lista de plantillas de ejemplo de servicios que son adecuadas para la región, elija el enlace Servicios.
3. Para comenzar, puede utilizar cualquiera de los ejemplos que sea adecuado para sus necesidades. En los pasos de este procedimiento se utiliza la plantilla Amazon EC2 instance in a security group. Para ver la plantilla de ejemplo, elija View y, a continuación, guarde localmente una copia de la plantilla para poder editarla. El archivo local debe tener la extensión `.template`.
4. Abra el archivo de la plantilla en un editor de texto.
5. Personalice la descripción de la parte superior de la plantilla. La descripción puede ser parecida a la siguiente:

```
"Description": "Launches a LAMP stack from AWS Marketplace",
```

6. Personalice el parámetro InstanceType de forma que incluya únicamente los tipos de instancias EC2 que son compatibles con el producto. Si la plantilla incluye tipos de instancias EC2 no compatibles, el producto no se lanzará para los usuarios finales.
  - a. En la página de tramitación del producto de AWS Marketplace, consulte los tipos de instancias EC2 compatibles en la sección Información sobre precios.

### On-Demand Plans for Amazon EC2

Select a region, operating system, instance type, and vCPU to view rates

Region	Operating system
US East (N. Virginia) ▼	Linux ▼
Instance type	vCPU
All ▼	All ▼

Viewing 364 of 364 available instances

Q

< 1 2 3 4 5 6 7 ... 19 >

Instance name ▲	On-Demand hourly rate ▼	vCPU ▼	Memory ▼	Storage ▼	Network performance ▼
a1.medium	\$0.0255	1	2 GiB	EBS Only	Up to 10 Gigabit
a1.large	\$0.051	2	4 GiB	EBS Only	Up to 10 Gigabit
a1.xlarge	\$0.102	4	8 GiB	EBS Only	Up to 10 Gigabit
a1.2xlarge	\$0.204	8	16 GiB	EBS Only	Up to 10 Gigabit
a1.4xlarge	\$0.408	16	32 GiB	EBS Only	Up to 10 Gigabit
a1.metal	\$0.408	16	32 GiB	EBS Only	Up to 10 Gigabit
t4g.nano	\$0.0042	2	0.5 GiB	EBS Only	Up to 5 Gigabit

- b. En la plantilla, cambie el tipo de instancia predeterminado por el tipo de instancia EC2 compatible que desee.
- c. Modifique la lista AllowedValues de forma que incluya únicamente los tipos de instancias EC2 que son compatibles con el producto.
- d. Elimine de la lista AllowedValues los tipos de instancias EC2 que no desee que utilicen los usuarios finales cuando lancen el producto.

Cuando haya terminado de editar el parámetro InstanceType, puede que tenga un aspecto similar al ejemplo siguiente:

```
"InstanceType" : {
  "Description" : "EC2 instance type",
  "Type" : "String",
  "Default" : "m1.small",
  "AllowedValues" : [ "t1.micro", "m1.small", "m1.medium", "m1.large",
    "m1.xlarge", "m2.xlarge", "m2.2xlarge", "m2.4xlarge", "c1.medium", "c1.xlarge",
    "c3.large", "c3.large", "c3.xlarge", "c3.xlarge", "c3.4xlarge", "c3.8xlarge" ],
  "ConstraintDescription" : "Must be a valid EC2 instance type."
},
```

7. En la sección Mappings de la plantilla, edite los mapeos de AWSInstanceType2Arch de modo que solo se incluyan los tipos de instancias EC2 y las arquitecturas que sean compatibles.
  - a. Edite la lista de mapeos y elimine todos los tipos de instancias EC2 que no están incluidas en la lista AllowedValues para el parámetro InstanceType.
  - b. Edite el valor Arch de cada tipo de instancia EC2 de modo que sea el tipo de arquitectura que es compatible con el producto. Los valores válidos son PV64, HVM64 y HVMG2. Para saber qué arquitectura es compatible con el producto, consulte la página de detalles del producto en AWS Marketplace. Para saber qué arquitecturas son compatibles con las familias de instancias EC2, consulte la [Matriz de tipos de instancias de la AMI de Amazon Linux](#).

Cuando haya terminado de editar los mapeos de AWSInstanceType2Arch, puede que tengan un aspecto similar al ejemplo siguiente:

```
"AWSInstanceType2Arch" : {
  "t1.micro" : { "Arch" : "PV64" },
  "m1.small" : { "Arch" : "PV64" },
  "m1.medium" : { "Arch" : "PV64" },
  "m1.large" : { "Arch" : "PV64" },
  "m1.xlarge" : { "Arch" : "PV64" },
  "m2.xlarge" : { "Arch" : "PV64" },
  "m2.2xlarge" : { "Arch" : "PV64" },
  "m2.4xlarge" : { "Arch" : "PV64" },
  "c1.medium" : { "Arch" : "PV64" },
  "c1.xlarge" : { "Arch" : "PV64" },
}
```

```

    "c3.large"      : { "Arch" : "PV64" },
    "c3.xlarge"    : { "Arch" : "PV64" },
    "c3.2xlarge"   : { "Arch" : "PV64" },
    "c3.4xlarge"   : { "Arch" : "PV64" },
    "c3.8xlarge"   : { "Arch" : "PV64" }
  }

```

8. En la sección Mappings de la plantilla, edite los mapeos de `AWSRegionArch2AMI` con el fin de asociar cada AWS región de AWS con la arquitectura y el identificador de AMI correspondientes para el producto.
  - a. En la página de tramitación del producto de AWS Marketplace, consulte el identificador de AMI que su producto utiliza para cada AWS región de AWS, como en el siguiente ejemplo:

Region	ID	
US East (N. Virginia)	ami- <del>4379408</del>	<a href="#">Launch with EC2 Console</a>
US West (Oregon)	ami- <del>985488ad</del>	<a href="#">Launch with EC2 Console</a>
US West (N. California)	ami- <del>934865d7</del>	<a href="#">Launch with EC2 Console</a>
EU (Frankfurt)	ami- <del>24ce8579</del>	<a href="#">Launch with EC2 Console</a>
EU (Ireland)	ami- <del>6672787</del>	<a href="#">Launch with EC2 Console</a>
Asia Pacific (Singapore)	ami- <del>860243d2</del>	<a href="#">Launch with EC2 Console</a>
Asia Pacific (Sydney)	ami- <del>1d94227</del>	<a href="#">Launch with EC2 Console</a>
Asia Pacific (Tokyo)	ami- <del>9ee548ae</del>	<a href="#">Launch with EC2 Console</a>
South America (Sao Paulo)	ami- <del>853a9c6</del>	<a href="#">Launch with EC2 Console</a>

- b. En la plantilla, quite los mapeos de las AWS regiones no compatibles.
- c. Edite el mapeo de cada región para eliminar las arquitecturas no compatibles (PV64, HVM64 o HVMG2) y sus identificadores de AMI asociados.
- d. Para cada mapeo restante de AWS región y arquitectura, especifique el identificador de AMI correspondiente de la página de detalles del producto de AWS Marketplace.

Cuando haya terminado de editar los mapeos de `AWSRegionArch2AMI`, puede que el código tenga un aspecto similar al ejemplo siguiente:

```

"AWSRegionArch2AMI" : {
  "us-east-1"      : {"PV64" : "ami-nnnnnnnn"},
  "us-west-2"     : {"PV64" : "ami-nnnnnnnn"},

```

```
"us-west-1"      : {"PV64" : "ami-nnnnnnnn"},
"eu-west-1"     : {"PV64" : "ami-nnnnnnnn"},
"eu-central-1"  : {"PV64" : "ami-nnnnnnnn"},
"ap-northeast-1": {"PV64" : "ami-nnnnnnnn"},
"ap-southeast-1": {"PV64" : "ami-nnnnnnnn"},
"ap-southeast-2": {"PV64" : "ami-nnnnnnnn"},
"sa-east-1"     : {"PV64" : "ami-nnnnnnnn"}
}
```

A partir de ahora, puede utilizar la plantilla para agregar el producto a una cartera de AWS Service Catalog. Si desea realizar cambios adicionales, consulte [Trabajo con plantillas de AWS CloudFormation](#) para obtener más información sobre las plantillas.

Para agregar el producto de AWS Marketplace a una cartera de AWS Service Catalog

1. Inicie sesión en la AWS Management Console y vaya a la consola de administración AWS Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. En la página Carteras, elija la cartera que desee agregar al producto de AWS Marketplace.
3. En la página de detalles de la cartera, elija Subir nuevo producto.
4. Escriba el producto solicitado y los detalles de soporte.
5. En la página Version details, seleccione Upload a template file, haga clic en Browse y elija el archivo de plantilla.
6. Escriba el título y la descripción de la versión.
7. Elija Siguiente.
8. En la página Revisar, compruebe que el resumen es correcta y, a continuación, elija Confirmar y actualizar. El producto se agregará a la cartera. Ahora ya está disponible para los usuarios finales que tienen acceso a la cartera.

## Uso AWS CloudFormation StackSets

### Note

AutoTags actualmente no son compatibles con AWS CloudFormation StackSets.

Puedes utilizarlos AWS CloudFormation StackSets para lanzar AWS Service Catalog productos en varias cuentas Regiones de AWS y. Puede especificar el orden en el que los productos se implementan secuencialmente en Regiones de AWS. En varias cuentas, los productos se implementan en paralelo. En el lanzamiento, los usuarios pueden especificar la tolerancia a errores y el número máximo de cuentas en las que se puede realizar la implementación en paralelo. Para obtener más información, consulte [Trabajar con AWS CloudFormation StackSets](#).

## Diferencias entre conjuntos de pilas e instancias de pila

Un conjunto de pilas permite crear pilas en las cuentas de AWS entre AWS regiones mediante una única plantilla de AWS CloudFormation .

Una instancia de pila se refiere a una pila en una cuenta de destino de una AWS región y está asociada a un solo conjunto de pilas.

Para obtener más información, consulte [Conceptos deStackSets](#).

## Restricciones de conjunto de pilas

En AWS Service Catalog puede utilizar restricciones de conjunto de pilas para configurar las opciones de implementación del producto.

AWS Service Catalogadmite restricciones de conjuntos de productos en dos categoríasAWS GovCloud (US) Regions: AWS GovCloud (EE. UU., oeste) y AWS GovCloud (EE. UU., este).

Para obtener más información, consulte [Restricciones de lanzamientoAWS Service Catalog](#).

## Administración de presupuestos

Puede utilizar Presupuestos de AWS para realizar un seguimiento de los costos y el uso del servicio en AWS Service Catalog. Puede asociar presupuestos con productos y carteras de AWS Service Catalog.

### Note

AWS Service Catalog no admite presupuestos para los productos de Terraform Open Source

Presupuestos de AWS ofrece la posibilidad de definir presupuestos personalizados que alertan cuando los costos o el uso superan o se prevé que superen el importe presupuestado. La

información sobre Presupuestos de AWS está disponible en <https://aws.amazon.com/aws-cost-management/aws-budgets>.

## Tareas

- [Requisitos previos](#)
- [Crear un presupuesto](#)
- [Asociación de un presupuesto](#)
- [Visualización de un presupuesto](#)
- [Desasociación de un presupuesto](#)

## Requisitos previos

Antes de utilizar Presupuestos de AWS, debe activar las etiquetas de asignación de costos en la consola de AWS Billing and Cost Management. Para obtener más información, consulte [Activación de etiquetas de asignación de costos definidas por el usuario](#) en la Guía del usuario de AWS Billing and Cost Management.

### Note

Las etiquetas tardan hasta 24 horas en activarse.

También debe habilitar el acceso de los usuarios a la consola de AWS Billing and Cost Management para todos los usuarios o grupos que vayan a utilizar la característica Presupuestos. Para ello, cree una nueva política para los usuarios.

Para permitir a los usuarios de crear presupuestos, también debe permitir a los usuarios ver la información de facturación. Si desea utilizar notificaciones de Amazon SNS, puede proporcionar a los usuarios la capacidad de crear notificaciones de Amazon SNS, tal y como se muestra en el ejemplo de política siguiente.

Para crear la política de presupuestos

1. Abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación, seleccione Políticas.
3. En el panel de contenido, elija Create policy (Crear política).

4. Seleccione la pestaña JSON y copie el texto del siguiente documento de política JSON. Pegue el texto en el cuadro de texto JSON.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1435216493000",
      "Effect": "Allow",
      "Action": [
        "aws-portal:ViewBilling",
        "aws-portal:ModifyBilling",
        "budgets:ViewBudget",
        "budgets:ModifyBudget"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "Stmt1435216552000",
      "Effect": "Allow",
      "Action": [
        "sns:*"
      ],
      "Resource": [
        "arn:aws:sns:us-east-1"
      ]
    }
  ]
}
```

5. Cuando haya terminado, elija Review policy (Revisar la política). El validador de políticas notifica los errores de sintaxis.
6. En la página Review (Revisar), asigne un nombre a la política. Revise el Summary (Resumen) de la política para ver los permisos concedidos por la política y, a continuación, elija Create policy (Crear política) para guardar el trabajo.

La nueva política aparece en la lista de las políticas administradas y está lista para asociarse a los grupos y usuarios. Para obtener más información, consulte [Crear y asociar una política administrada por el cliente](#) en la Guía del usuario de AWS Identity and Access Management.

## Crear un presupuesto

En la consola del administrador de AWS Service Catalog, las páginas Lista de productos y Carteras enumeran los productos y carteras existentes y le permiten realizar acciones en ellas. Para crear un presupuesto, primero decida a qué producto o cartera desea asociar el presupuesto.

Para crear un presupuesto

1. Abra la consola de Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. Elija Lista de productos o Carteras.
3. Seleccione el producto o la cartera a la que desea añadir un presupuesto.
4. Abra el menú Acciones y, a continuación, elija Crear presupuesto.
5. En la página Budget creation (Creación de presupuesto) asocie un tipo de etiqueta al presupuesto.

Hay dos tipos de etiquetas: AutoTags y TagOptions. AutoTags identifican la cartera, el producto y el usuario que lanzó un producto. AWS Service Catalog aplica estas etiquetas automáticamente a los recursos aprovisionados. A TagOption es un par clave-valor definido por el administrador que se administra en AWS Service Catalog

Para que los gastos que se producen en una cartera o producto se reflejen en el presupuesto asociado, deben tener la misma etiqueta. Tenga en cuenta que una clave de etiqueta que se utiliza por primera vez puede tardar 24 horas en activarse. Para obtener más información, consulte [the section called “Requisitos previos”](#).

6. Seleccione Crear en AWS Budgets. Le dirigirá a la página Establecer su presupuesto. Continúe con la configuración del presupuesto siguiendo los pasos que se indican en [Creación de un presupuesto](#).

### Note

Después de crear un presupuesto, debe asociarlo al producto o a la cartera.

## Asociación de un presupuesto

Cada cartera o producto puede tener un presupuesto asociado. Cada presupuesto se puede asociar a varias carteras y productos.

Cuando asocia un presupuesto a un producto o cartera, podrá ver información sobre el presupuesto en la página de detalles de dicho producto o cartera. Para que el gasto que se produce en el producto o la cartera se refleje en el presupuesto, debe asociar las mismas etiquetas tanto en el presupuesto como en el producto o la cartera.

### Note

Si elimina un presupuesto desde AWS Budgets, las asociaciones existentes con productos y carteras de AWS Service Catalog seguirán existiendo, AWS Service Catalog no podrá mostrar ninguna información sobre el presupuesto eliminado.

Para asociar un presupuesto

1. Abra la consola de Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. Elija Lista de productos o Carteras.
3. Seleccione el producto o la cartera a la que desea asociar el presupuesto.
4. Abra el menú Acciones y, a continuación, elija Asociar presupuesto.
5. En la página Asociación de presupuesto, seleccione un presupuesto existente y elija Continuar.
6. La tabla Carteras o Productos ahora incluye datos del presupuesto que acaba de añadir.

## Visualización de un presupuesto

Si un presupuesto está asociado a un producto, puede ver información sobre el presupuesto en la página Productos y Detalles del producto. Si un presupuesto está asociado a una cartera, puede ver información sobre el presupuesto en las páginas Carteras y Detalles de la cartera.

Las páginas Carteras y Productos muestran información del presupuesto de los recursos existentes. Puede ver columnas que muestran Current vs. budget (Actual vs. presupuesto) y Forecast vs. budget (Previsto vs. presupuesto).

Cuando seleccione un producto o una cartera, será dirigido a una página de detalles. Las páginas de Detalles de la cartera y Detalles del producto tienen una sección con información pormenorizada

sobre el presupuesto asociado. Puede ver la cantidad presupuestada, el gasto actual y el gasto previsto. También tiene la opción de ver los detalles del presupuesto y editarlo.

## Desasociación de un presupuesto

Puede desasociar un presupuesto de una cartera o un producto.

### Note

Si elimina un presupuesto desde Presupuestos de AWS, las asociaciones existentes con productos y carteras de AWS Service Catalog seguirán existiendo, pero AWS Service Catalog no podrá mostrar ninguna información sobre el presupuesto eliminado.

Para desasociar un presupuesto

1. Abra la consola de Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. Elija Lista de productos o Carteras.
3. Seleccione el producto o la cartera de la que desea desasociar un presupuesto.
4. Elija Acciones. En el menú desplegable, seleccione Disociar el presupuesto. Aparece una alerta de confirmación.
5. Cuando confirme que desea disociar el presupuesto del producto o la cartera, seleccione Confirmar.

# Administración de productos aprovisionados

AWS Service Catalog proporciona una interfaz para administrar los productos aprovisionados. Puede consultar, actualizar y terminar todos los productos aprovisionados del catálogo en función del nivel de acceso. Consulte las secciones siguientes para obtener ejemplos de procedimientos.

## Temas

- [Administración de todos los productos aprovisionados como administrador](#)
- [Cambio del propietario del producto aprovisionado](#)
- [Actualizar plantillas para productos aprovisionados](#)
- [Tutorial: Identificación de la asignación de recursos del usuario](#)
- [Gestión de los errores de estado del producto Terraform Open Source](#)
- [Administrar el archivo de estado del producto de Terraform Open Source](#)

## Administración de todos los productos aprovisionados como administrador

Para administrar todos los productos aprovisionados de la cuenta, se requiere acceso `AWSServiceCatalogAdminFullAccess` o de nivel equivalente IAM a las operaciones de escritura del producto aprovisionado. Para obtener más información, consulte [Administración de identidad y acceso en AWS Service Catalog](#).

### Tip

Para el encadenamiento estático de productos aprovisionados, debe hacer referencia a los resultados de los productos aprovisionados en una plantilla de producto-artefacto antes de aprovisionar el producto aprovisionado. Para obtener más información, como el siguiente ejemplo, consulte lo siguiente:

- [AWS::ServiceCatalog::CloudFormationProvisionedProduct](#) en la Guía del usuario de AWS CloudFormation.
- [DescribeProvisioningParameters \(ProvisioningArtifactOutputKeys\)](#) en la Guía del AWS Service Catalog desarrollador.

Para consultar y administrar todos los productos aprovisionados

1. Abra la consola de AWS Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.  
Si ya ha iniciado sesión en la consola AWS Service Catalog, seleccione Service Catalog y, a continuación, Usuario final.
2. Si es preciso, vaya a la sección Productos aprovisionados.
3. En la sección Productos aaprovisionados, seleccione la lista Ver: y seleccione el nivel de acceso que desee ver: Usuario, Rol o Cuenta. Se mostrarán todos los productos aprovisionados del catálogo.
4. Elija un producto aprovisionado que desee consultar, actualizar o terminar. Para obtener más información acerca de la información facilitada en esta vista, consulte [Visualización de información sobre productos aprovisionados](#).

## Cambio del propietario del producto aaprovisionado

Puede cambiar el propietario de un producto aaprovisionado en cualquier momento. Debe conocer el ARN del usuario o rol que desea establecer como nuevo propietario.

De forma predeterminada, esta característica está disponible para los administradores que utilizan la política administrada `AWSServiceCatalogAdminFullAccess`. Puede habilitarlo para los usuarios finales concediéndoles el permiso `servicecatalog:UpdateProvisionedProductProperties` de acceso en AWS Identity and Access Management (IAM).

Para cambiar el propietario de un producto aaprovisionado

1. En la consola de AWS Service Catalog, seleccione Provisioned products list (Lista de productos aaprovisionados).
2. Localice el producto aaprovisionado que desea actualizar, elija los tres puntos que hay junto a él y seleccione Cambiar el propietario del producto aaprovisionado. También puede encontrar la opción Change owner (Cambiar propietario) en la página de detalles del producto aaprovisionado, en el menú Actions (Acciones).
3. En el cuadro de diálogo, escriba el ARN del usuario o rol que desea establecer como nuevo propietario. Un ARN comienza por `arn:` e incluye otra información separada por dos puntos o barras diagonales, por ejemplo, `arn:aws:iam::123456789012:user/NewOwner`.
4. Elija Enviar. Verá un mensaje de realización correcta cuando se haya actualizado el propietario.

## Véase también

- [UpdateProvisionedProductProperties](#)

## Actualizar plantillas para productos aaprovisionados

Puede cambiar la plantilla actual de un producto aaprovisionado a una plantilla diferente. Por ejemplo, si tiene un producto de EC2 en Service Catalog, puede actualizar ese producto de EC2 para retener el mismo ID de producto aaprovisionado, pero cambiar la plantilla por un bucket de S3.

### Note

La actualización de plantillas no es compatible con los productos Terraform Open Source o Terraform Cloud aaprovisionados. Si desea utilizar una plantilla diferente para un producto de Terraform existente, debe eliminar el producto y, a continuación, crear un nuevo producto con la plantilla deseada.

Para actualizar un producto aaprovisionado

1. Elija Productos aaprovisionados en el menú de navegación de la izquierda.
2. En Productos aaprovisionados, seleccione un producto aaprovisionado y seleccione Acciones, Actualizar.

Tenga en cuenta que también puede seleccionar Acciones y Actualizar en la página de Detalles del producto aaprovisionado.

3. (Opcional) En Detalles del producto, seleccione Cambiar producto.

En Cambiar producto, tenga en cuenta esta advertencia:

Al cambiar el producto se actualizará el producto aaprovisionado a una plantilla de producto diferente. Esto puede finalizar con los recursos y crear nuevos recursos.

Puede actualizar un producto aaprovisionado a una versión diferente dentro del mismo producto.

4. (Opcional) En Productos, seleccione el producto que desea actualizar con una plantilla diferente. A continuación, seleccione Cambiar.

En Detalles del producto, tenga en cuenta esta advertencia:

[Nombre del producto] se actualizará de [nombre de la plantilla actual] a [nombre de la nueva plantilla]. Sin embargo, el nombre del producto aprovisionado, [nombre del producto aprovisionado], no cambiará.

Puede actualizar un producto aprovisionado a una versión diferente dentro del mismo producto.

5. En Versiones del producto, seleccione la versión del producto que desee.
6. En Parámetros, seleccione los parámetros adecuados.
7. Seleccione Actualizar.

En Detalles del producto aprovisionado, puede ver los detalles de la actualización. El nombre del producto aprovisionado no cambia, pero el producto aprovisionado ahora tiene una plantilla diferente.

## Tutorial: Identificación de la asignación de recursos del usuario

Puede identificar al usuario que ha aprovisionado un producto y los recursos asociados con ese producto en la consola de AWS Service Catalog. Este tutorial le ayuda a adaptar este ejemplo a sus propios productos aprovisionados.

Para administrar todos los productos aprovisionados de la cuenta, se requiere acceso `AWSServiceCatalogAdminFullAccess` o de nivel equivalente a las operaciones de escritura del producto aprovisionado. Para obtener más información, consulte [Administración de identidades y accesos](#) en la AWS Service Catalog Guía del administrador.

Para identificar al usuario que ha aprovisionado un producto y los recursos asociados

1. Abra <https://console.aws.amazon.com/servicecatalog>.
2. Elija Productos aprovisionados en el menú de navegación de la izquierda.
3. En el menú desplegable del Filtro de acceso, seleccione Cuenta.

Service Catalog > Provisioned products

**Provisioned products (0)** [Info](#)

Search provisioned products

Access Filter Account **1**

Name	Created	ID	Product name	Version name	Status

Account  
User  
Account  
Role

- En la vista de la Cuenta, seleccione y abra un producto aprovisionado para ver sus detalles.

**Provisioned products (1/6)** [Info](#)

Search provisioned products

Access Filter Account

Name	Created	Product name	Version name	Status
s3bucket-03252118	Thu, Mar 25, 2021, 5:28:40 PM EDT	s3bucket	2	Available

Puede ver los detalles del producto aprovisionado.

**Provisioned product details**

Product description  
-

Provisioned product ID pp-4ssmsm2d4cvs	User name SCAdminAllow	Status Available
Product name shsen-test	User ARN arn:aws:iam::776643078058:user/SCAdminAllow	Version name -
Created Thu, Jul 15, 2021, 9:49:54 AM PDT		

▼ More details

Product ID prod-y7bsnu3cn7eso	Type CFN_STACK	Support email contact -
Version ID pa-2d5inxhjryy9d	Product owner 53440542	Support link -

Support description  
-

- Desplácese hacia abajo en la sección Eventos. Tenga en cuenta los valores de Provisioned product ID y CloudformationStackARN.

Events (4) <a href="#">Info</a>		
<input type="text" value="Search events"/> <span style="float: right;">Sort by <span style="border: 1px solid #ccc; padding: 2px;">Newest</span> &lt; 1 &gt; ⚙</span>		
<b>▼ UPDATE_PROVISIONED_PRODUCT</b>		
Date created	CloudFormationStackARN	Status
Thu, May 27, 2021, 5:06:38 PM EDT	Copy to clipboard	<span style="color: green;">✔ Succeeded</span>
Record ID	Product name	Product version
rec- <a href="#">[redacted]</a>	ssmImport	1
Provisioning artifact ID		
pa- <a href="#">[redacted]</a>		
Output key	Output value	Output description
CloudformationStackARN	<a href="#">arn:aws:cloudformation:us-east-1:[account number]:stack/SC-[product name]-[id]-11eb-b851-0a8a0480d74d</a>	The ARN of the launched Cloudformation Stack

6. Utilice el ID del producto provisionado para identificar el registro de AWS CloudTrail que se corresponde con este lanzamiento e identificar al usuario que ha realizado la solicitud (por lo general, se especifica mediante una dirección de correo electrónico durante la federación). En este ejemplo, es "steve".

```
{
  "eventVersion": "1.03", "userIdentity":
  {
    "type": "AssumedRole",
    "principalId": "[id]:steve",
    "arn": "arn:aws:sts::[account number]:assumed-role/SC-usertest/steve",
    "accountId": [account number],
    "accessKeyId": [access key],
    "sessionContext":
    {
      "attributes":
      {
        "mfaAuthenticated": [boolean],
        "creationDate": [timestamp]
      },
      "sessionIssuer":
      {
        "type": "Role",
        "principalId": "AROAJEXAMPLELH3QXY",
        "arn": "arn:aws:iam::[account number]:role/[name]",
        "accountId": [account number],
        "userName": [username]
      }
    }
  },
}
```

```

"eventTime":"2016-08-17T19:20:58Z","eventSource":"servicecatalog.amazonaws.com",
"eventName":"ProvisionProduct",
"awsRegion":"us-west-2",
"sourceIPAddress":[ip address],
"userAgent":"Coral/Netty",
"requestParameters":
{
  "provisioningArtifactId":[id],
  "productId":[id],
  "provisioningParameters":[Shows all the parameters that the end user entered],
  "provisionToken":[token],
  "pathId":[id],
  "provisionedProductName":[name],
  "tags":[],
  "notificationArns":[]
},
"responseElements":
{
  "recordDetail":
  {
    "provisioningArtifactId":[id],
    "status":"IN_PROGRESS",
    "recordId":[id],
    "createdTime":"Aug 17, 2016 7:20:58 PM",
    "recordTags":[],
    "recordType":"PROVISION_PRODUCT",
    "provisionedProductType":"CFN_STACK",
    "pathId":[id],
    "productId":[id],
    "provisionedProductName":"testSCproduct",
    "recordErrors":[],
    "provisionedProductId":[id]
  }
},
"requestID":[id],
"eventID":[id],
"eventType":"AwsApiCall",
"recipientAccountId":[account number]
}

```

7. Utilice el valor `CloudFormationStackARN` para identificar los eventos de AWS CloudFormation y buscar información sobre los recursos creados. También puede utilizar el API

de AWS CloudFormation para obtener esta información. Para obtener más información, consulte [Referencia de la API de AWS CloudFormation](#).

Tenga en cuenta que puede realizar los pasos del 1 al 4 con el API de AWS Service Catalog o la AWS CLI. Para obtener más información, consulte la [Guía para desarrolladores de la AWS Service Catalog](#) [AWS Service Catalog Command Line Reference](#).

## Gestión de los errores de estado del producto Terraform Open Source

Los errores `ProvisionProduct` de Terraform Open Source se envían al estado `TAINTED`, lo que permite que cada producto aprovisionado siga a `UpdateProvisionedProduct`. Cuando esto ocurre:

- `UpdateProvisionedProduct` no intenta actualizar o corregir las etiquetas, ni crear o modificar un grupo de recursos.
- `UpdateProvisionedProduct` no tiene en cuenta los errores de operaciones de aprovisionamiento anteriores a la hora de decidir si el producto aprovisionado debe configurarse en `AVAILABLE` o `TAINTED`.

AWS Service Catalog solo aplica etiquetas durante `ProvisionProduct`. Cualquier error de etiquetado que se deba a un error en la operación `ProvisionProduct` no se resuelve automáticamente.

### Ejemplos de errores de estado

Ejemplo 1: AWS Service Catalog no crea un grupo de recursos durante `ProvisionProduct`

En el siguiente escenario, tiene un producto aprovisionado en el estado `AVAILABLE` aunque no haya un grupo de recursos de apoyo y sin ninguna etiqueta aplicada a los recursos.

1. Se inicia la acción `ProvisionProduct`.
2. El motor de aprovisionamiento de Terraform responde a `ProvisionProduct` con una falla en el flujo de trabajo y no proporciona una `ResourceIdentifier`.
3. El flujo de trabajo `ProvisionProduct` no crea un grupo de recursos y, a continuación, establece el estado del producto aprovisionado en `ERROR`.

4. A continuación, inicie la operación `UpdateProvisionedproduct`.
5. El motor de aprovisionamiento de Terraform responde indicando que se ha realizado correctamente.
6. Como resultado, el flujo de trabajo `UpdateprovisionedProduct` establece el estado del producto a `aprovisionado` en `AVAILABLE`, pero no crea un grupo de recursos ni intenta aplicar ninguna etiqueta.

## Ejemplo 2: AWS Service Catalog crea nuevos recursos durante `UpdateProvisionedProduct`

En el siguiente escenario, tiene un producto a `aprovisionado` en el estado `AVAILABLE` aunque a los nuevos recursos no se les haya aplicado ninguna etiqueta.

1. Se inicia la acción `ProvisionProduct`.
2. El motor de aprovisionamiento de Terraform responde indicando que se ha realizado correctamente y proporciona un `ResourceIdentifier`.
3. El flujo de trabajo `ProvisionProduct` crea un grupo de recursos y aplica etiquetas a todos los recursos identificados.
4. Se inicia `UpdateProvisionedProduct` con un artefacto nuevo que crea nuevos recursos.
5. El motor de aprovisionamiento de Terraform responde indicando que se ha realizado correctamente.
6. El flujo de trabajo `UpdateProvisionedProduct` establece el estado del producto a `aprovisionado` en los nuevos recursos, `AVAILABLE` pero no intenta aplicarles etiquetas adicionales.

## Solución de error de estado

AWS Service Catalog garantiza que se cree un grupo de recursos para todos los productos a `aprovisionados` establecidos en `TAINTED` de `ProvisionProduct`. Si el motor de aprovisionamiento de Terraform no devuelve un grupo de recursos `ResourceIdentifier`, o si AWS Service Catalog no crea un grupo de recursos, entonces el producto a `aprovisionado` se establece en el estado `ERROR`, lo que le obliga a finalizarlo.

# Administrar el archivo de estado del producto de Terraform Open Source

Cada producto aprovisionado por Terraform Open Source tiene un archivo de estado único. Existe una relación 1:1 entre el producto aprovisionado y su archivo de estado. Los archivos se almacenan en un bucket de Amazon S3 denominado `sc-terraform-engine-state-  
${AWS::AccountId}-${AWS::Region}`. El archivo de estado se guarda con la clave de objeto `AccountID` o `ProvisionedProductID`.

El acceso a los archivos estatales está limitado a las plantillas `GetStateFile` AWS Lambda de lanzamiento y a Amazon EC2. Los administradores AWS Service Catalog no tienen acceso directo a los archivos de estado de Amazon S3. Los administradores deben acceder a los archivos mediante Amazon EC2. De forma predeterminada, los administradores AWS Service Catalog pueden ver la lista de archivos de estado, pero no pueden leer ni escribir el contenido del archivo. Solo el motor de aprovisionamiento de Terraform puede leer o escribir el contenido del archivo.

# Administración de etiquetas en AWS Service Catalog

AWS Service Catalog proporciona etiquetas que le permiten categorizar los recursos. Existen dos tipos de etiquetas: AutoTags y TagOptions.

AutoTags son etiquetas que identifican información sobre el origen de un recurso provisionado en AWS Service Catalog y que se aplican automáticamente en AWS Service Catalog a los recursos provisionados.

TagOptions son pares clave-valor gestionados en AWS Service Catalog que sirven como plantillas para crear etiquetas. AWS

Temas

- [AWS Service Catalog AutoTags](#)
- [AWS Service Catalog TagOption Biblioteca](#)

## AWS Service Catalog AutoTags

### Note

AWS Service Catalog es compatible con AutoTags los productos de código abierto de Terraform.

AutoTags son etiquetas que identifican información sobre el origen de un recurso provisionado en AWS Service Catalog y que se aplican automáticamente en AWS Service Catalog a los recursos provisionados.

AutoTags incluyen etiquetas para los identificadores únicos de la cartera, el producto, el usuario, la versión del producto y el producto provisionado. Esto proporciona un conjunto de etiquetas que reflejan la estructura de AWS Service Catalog que los clientes han configurado en el catálogo. AutoTags no se tienen en cuenta para el límite de 50 etiquetas del cliente.

### Note

AWS Service Catalog es compatible con AutoTags los productos de código abierto de Terraform.

AWS Service Catalog AutoTags puede ayudar a proporcionar un etiquetado coherente para sus recursos, lo que resulta útil a la hora de establecer presupuestos para una cartera, un producto o un usuario. También puede utilizarlos AutoTags para identificar recursos para las operaciones posteriores al lanzamiento, como el establecimiento AWS Config de reglas. AutoTags para ver los recursos aprovisionados, consulte la sección Etiquetas de los servicios descendentes que se utilizan para el aprovisionamiento, como Amazon AWS CloudFormation EC2 y Amazon S3.

#### Note

AWS Service Catalogno se actualiza AutoTags después de aplicarlo AutoTags a los recursos aprovisionados. Si actualizas el producto aprovisionado a otro producto, artefacto aprovisionado o nueva ruta de lanzamiento, el existente AutoTags seguirá mostrando los valores originales.

### AutoTag detalles

- `aws:servicecatalog:portfolioArn`: el ARN de la cartera desde la que se lanzó el producto aaprovisionado.
- `aws:servicecatalog:productArn`: el ARN del producto desde el que se lanzó el producto aaprovisionado.
- `aws:servicecatalog: - provisioningPrincipalArn` El ARN del principal de aprovisionamiento (usuario) que creó el producto aprovisionado.
- `aws:servicecatalog: - El ARN provisionedProductArn` del producto aprovisionado.
- `aws:servicecatalog: provisioningArtifactIdentifier` - El ID del artefacto de aprovisionamiento original (versión del producto).

## AWS Service Catalog TagOption Biblioteca

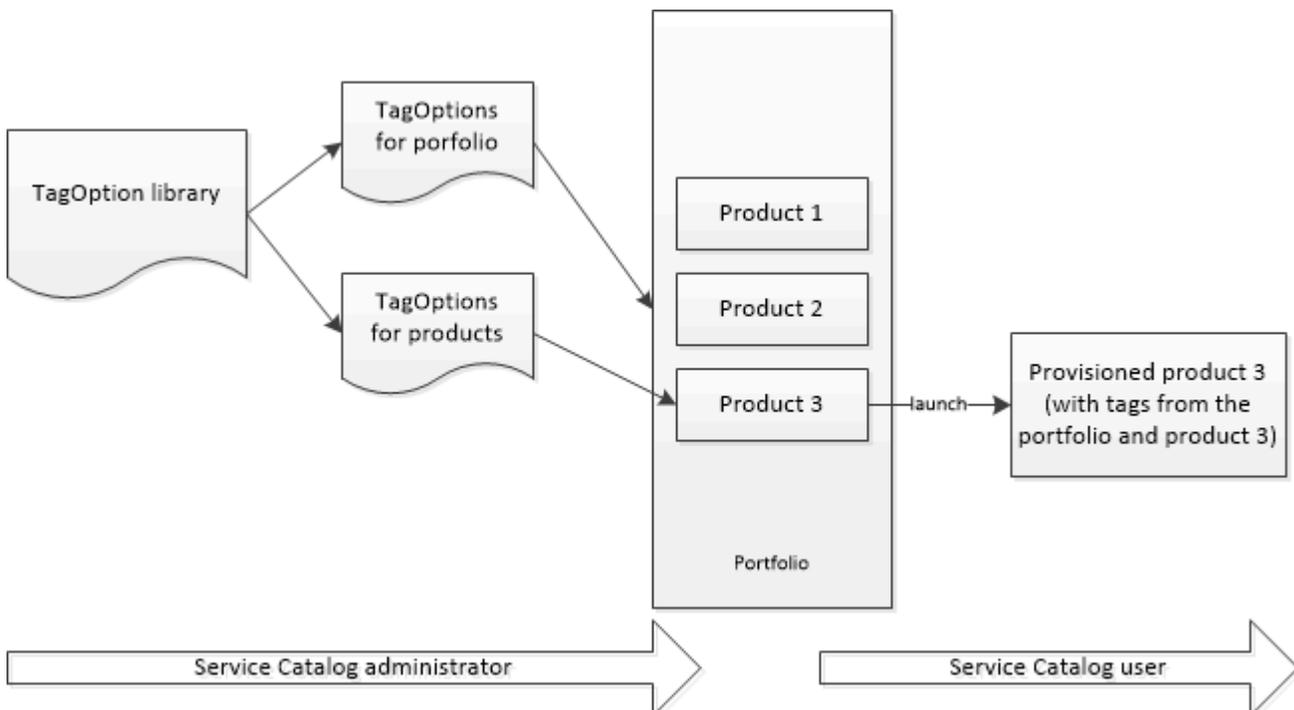
Para permitir a los administradores gestionar fácilmente las etiquetas de los productos aprovisionados, AWS Service Catalog proporciona una TagOption biblioteca. A TagOption es un par clave-valor gestionado en. AWS Service Catalog No es una AWS etiqueta, pero sirve como plantilla para crear una AWS etiqueta basada en. TagOption

AWS Service Catalogno es compatible con TagOptions los productos Terraform Open Source o Terraform Cloud.

La TagOption biblioteca facilita la aplicación de lo siguiente:

- Utilizar una taxonomía coherente
- Etiquetar correctamente los recursos de AWS Service Catalog
- Utilizar opciones definidas y seleccionables por el usuario para las etiquetas permitidas

Los administradores pueden TagOptions asociarse a carteras y productos. Durante el lanzamiento de un producto (aprovisionamiento), AWS Service Catalog agrega la cartera y el producto TagOptions asociados y los aplica al producto aprovisionado, como se muestra en el siguiente diagrama.



Con la TagOption biblioteca, puede desactivar TagOptions y conservar sus asociaciones con carteras o productos, y reactivarlas cuando las necesite. Este enfoque no solo ayuda a mantener la integridad de la biblioteca, sino que también le permite administrar lo TagOptions que pueda usarse de forma intermitente o solo en circunstancias especiales.

La administración se realiza TagOptions con la AWS Service Catalog consola o la API de la TagOption biblioteca. Para obtener más información, consulte la [Referencia de la API de Catálogo](#).

## Contenido

- [Lanzamiento de un producto con TagOptions](#)
- [Gestionando TagOptions](#)

- [Uso TagOptions con políticas AWS Organizations de etiquetas](#)

## Lanzamiento de un producto con TagOptions

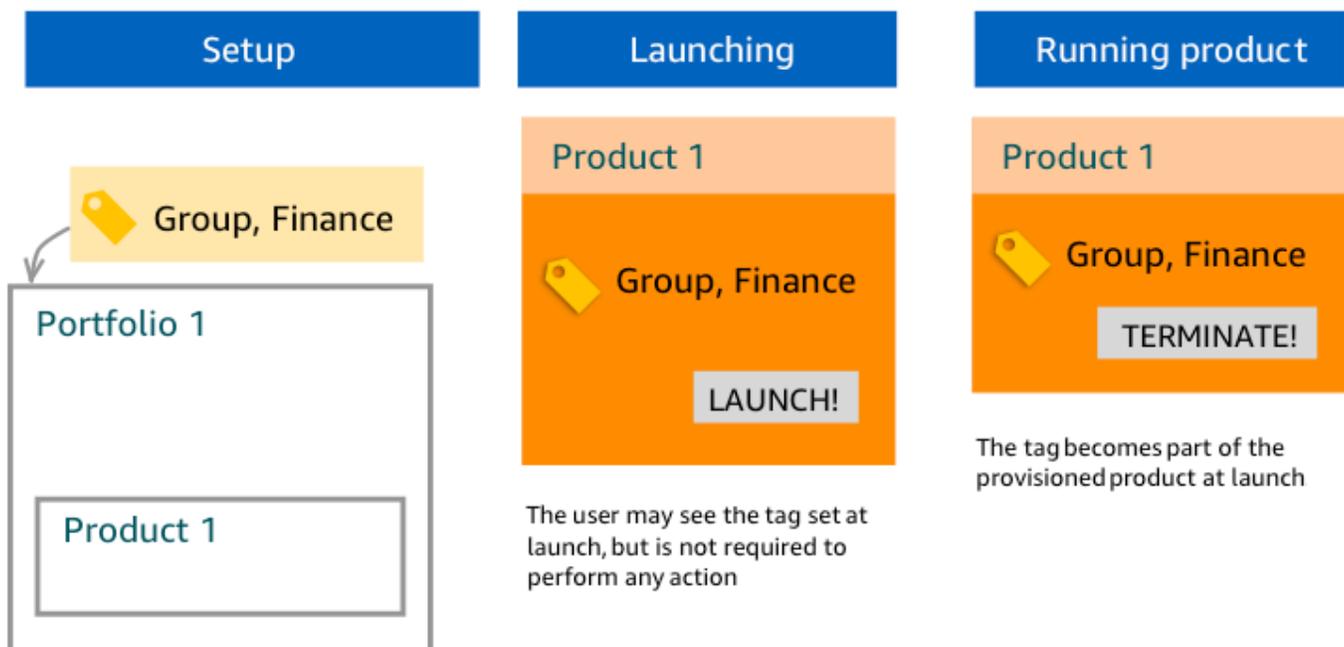
Cuando un usuario lanza un producto que lo tiene TagOptions, AWS Service Catalog realiza las siguientes acciones en tu nombre:

- Recopila todo TagOptions para el producto y la cartera de lanzamiento.
- Garantiza que solo TagOptions se utilicen claves únicas en una etiqueta del producto aprovisionado. Los usuarios obtienen una lista de valores de opción múltiple para la clave. Una vez que el usuario ha elegido un valor, este se convierte en una etiqueta en el producto aprovisionado.
- Permite a los usuarios agregar etiquetas sin conflictos al producto durante el provisionamiento.

Los siguientes casos de uso demuestran cómo TagOptions funcionan durante el lanzamiento.

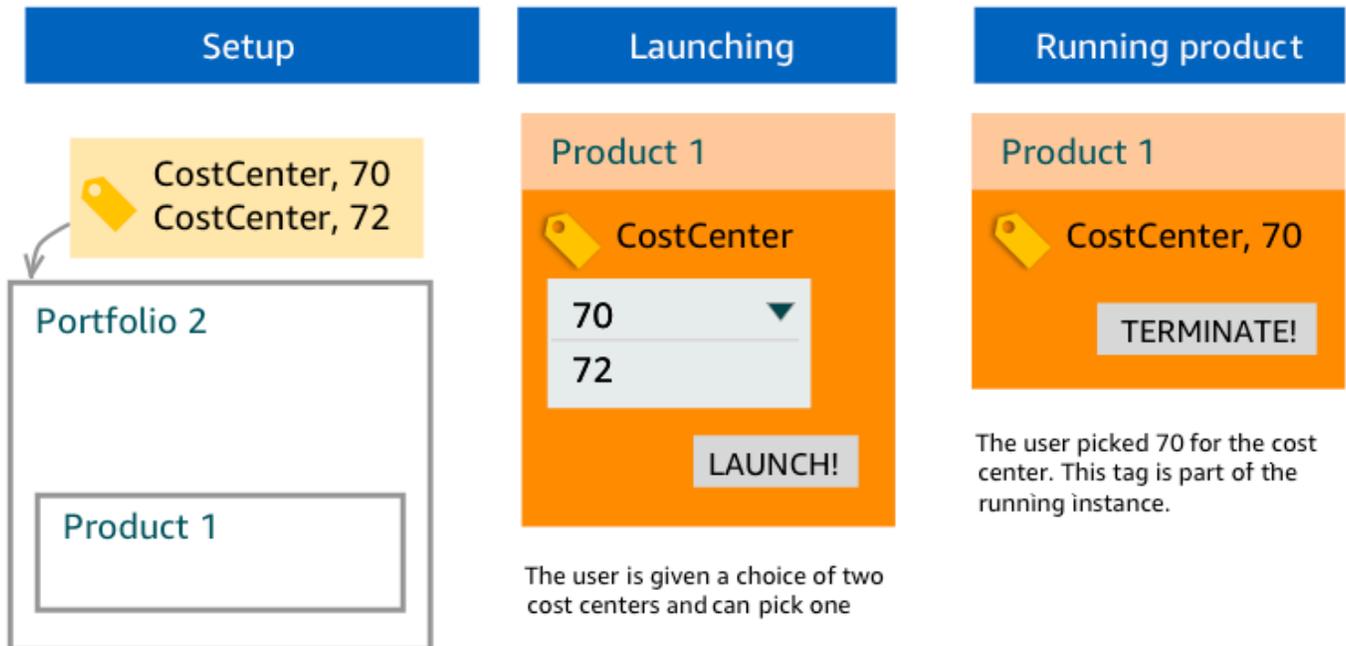
### Ejemplo 1: Una TagOption clave única

Un administrador crea TagOption[Group=Finance] y lo asocia a Portfolio1, que tiene Product1 sin número. TagOptions Cuando un usuario lanza el producto aprovisionado, el único TagOption pasa a ser Tag [Group=Finance], de la siguiente manera:



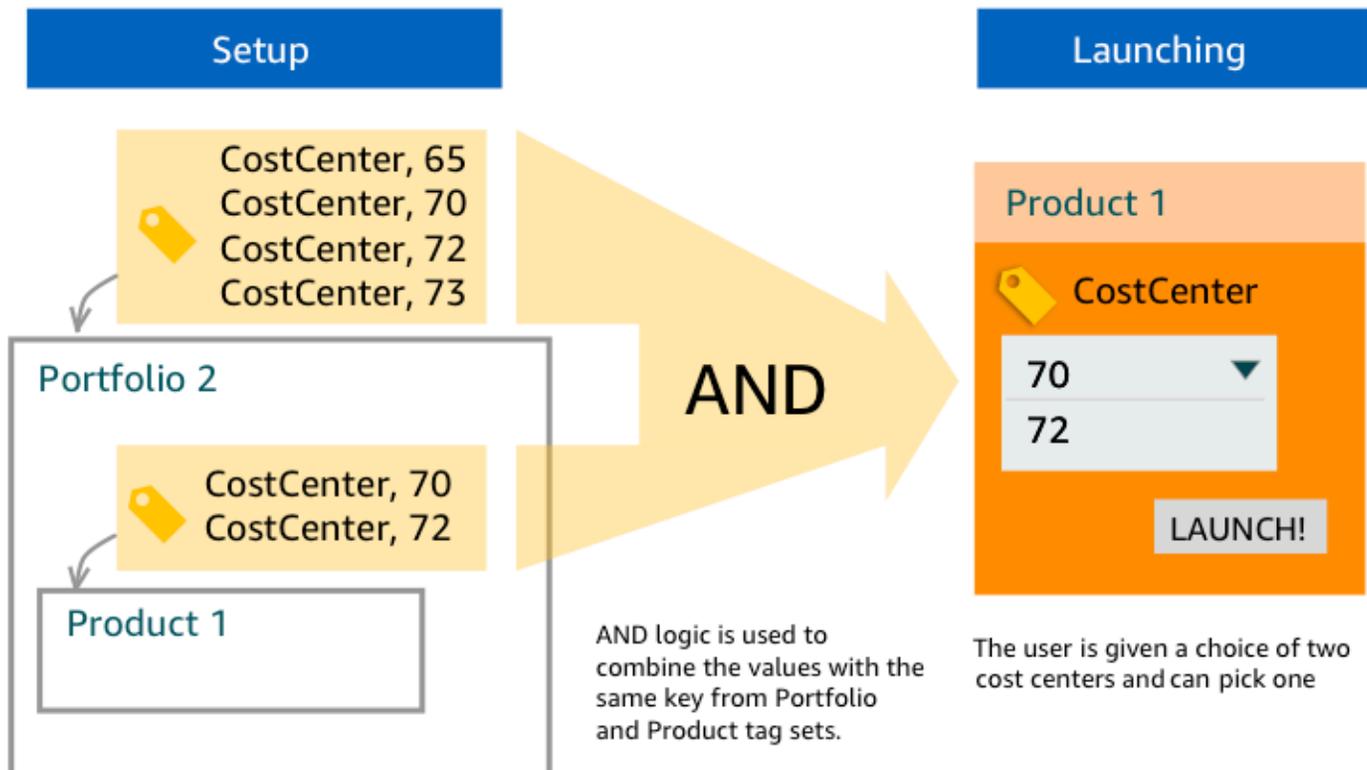
## Ejemplo 2: Un conjunto de TagOptions con la misma clave en una cartera

Un administrador ha colocado dos TagOptions con la misma clave en una cartera y no hay ninguna TagOptions con la misma clave en ningún producto de esa cartera. Durante el lanzamiento, el usuario debe seleccionar uno de los dos valores asociados con la clave. A continuación, el producto aprovisionado se etiqueta con la clave y el valor seleccionado por el usuario.



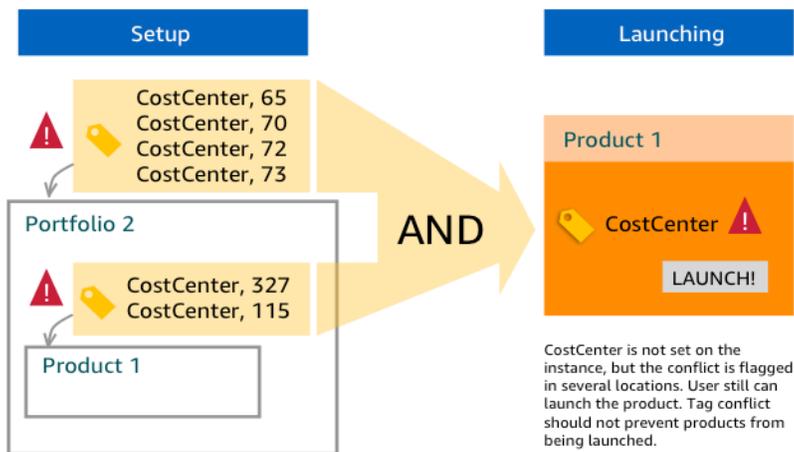
## Ejemplo 3: Un conjunto TagOptions con la misma clave tanto en la cartera como en un producto de esa cartera

Un administrador ha colocado varios TagOptions con la misma clave en una cartera y también hay varios TagOptions con la misma clave en el producto de esa cartera. AWS Service Catalog crea un conjunto de valores a partir de la agregación (lógica y operativa) de TagOptions. Cuando el usuario lanza el producto, ve este conjunto de valores y realiza en él su selección. El producto aprovisionado se etiqueta con la clave y el valor seleccionado por el usuario.



#### Ejemplo 4: Varios TagOptions con la misma clave y valores contradictorios

Un administrador ha colocado varios TagOptions con la misma clave en una cartera y también hay varios TagOptions con la misma clave en el producto de esa cartera. AWS Service Catalog crea un conjunto de valores a partir de la agregación (lógica y operativa) de TagOptions. Si en la agregación no se encuentran valores para la clave, AWS Service Catalog crea una etiqueta con la misma clave y un valor de `sc-tagconflict-portfolioid-productid`, donde *portfolioid* y *productid* son los nombres de recurso de Amazon (ARN) de la cartera y del producto. De este modo se garantiza que el producto aprovisionado se etiquete con la clave correcta y con un valor que el administrador puede encontrar y corregir.



## Gestionando TagOptions

Como administrador, puede realizar las siguientes acciones para administrar TagOptions la TagOptions biblioteca:

- Crear o eliminar
- Activar o desactivar
- Asociar o desasociar
- Edición

Para crear TagOptions en la consola

1. Abra la consola de Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. En el menú de navegación de la izquierda, selecciona TagOptionsbiblioteca.
3. En Crear nuevo TagOption, introduce una clave y un valor y, a continuación, selecciona Añadir.

Una vez creada la nueva, TagOption se agrupa por par clave-valor y se ordena alfabéticamente en la lista. TagOptions

Para crear una TagOption mediante la API, consulte. AWS Service Catalog [CreateTagOption](#)

Para eliminar TagOptions en la consola

1. Abra la consola de Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.

2. En el menú de navegación de la izquierda, selecciona TagOptions biblioteca y, a continuación, selecciona Acciones.
3. Para confirmar la eliminación, elija Eliminar.

Para activar o desactivar una o varias TagOptions en la consola

1. Abra la consola de Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. En el menú de navegación de la izquierda, selecciona la TagOptions biblioteca y, a continuación, selecciona Acciones.
3. Para activarla, elige la inactiva TagOption que desees. A continuación, seleccione Acciones y seleccione Activar en el menú desplegable y confirme su selección.

Para desactivarlo, elige el activo TagOption que desees. A continuación, seleccione Acciones y seleccione Desactivar en el menú desplegable y confirme su selección.

Para asociar o desasociar uno o varios de ellos TagOptions a una cartera de la consola

1. Abra la consola de Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. En el menú de navegación de la izquierda, seleccione Cartera y, a continuación, abra la cartera que desee asociar o disociar.
3. Elija la TagOptionspestaña y seleccione una o varias TagOptions para asociarlas o desasociarlas a la cartera.
4. Elija Acciones. A continuación, seleccione Asociar o Disociar y confirme su selección.

Para asociar o desasociar uno o varios TagOptions productos de la consola

1. Abra la consola AWS Service Catalog en: <https://console.aws.amazon.com/servicecatalog/>.
2. En el panel de navegación de la izquierda, bajo Administración, seleccione Productos. A continuación, abra el producto que desee asociar o disociar.
3. Elija la TagOptionspestaña y seleccione una o varias TagOptions para asociarlas o desasociarlas a la cartera.
4. Elija Acciones. A continuación, seleccione Asociar o Disociar y confirme su selección.

**Note**

Para TagOptions asociarlo a una cartera o un producto mediante la AWS Service Catalog API, consulte [AssociateTagOptionWithResource](#).

Para eliminar (desasociar) TagOptions mediante la AWS Service Catalog API, consulte [DisassociateTagOptionFromResource](#).

Para editar los valores de TagOptions la consola

1. Abra la consola de Service Catalog en <https://console.aws.amazon.com/servicecatalog/>.
2. En el menú de navegación de la izquierda, selecciona TagOptionsbiblioteca.
3. Elija un valor TagOption y abra el valor. (El valor tiene un hipervínculo). A continuación, elija Editar.
4. En el campo Valor, edite el valor y seleccione Guardar cambios.

## Uso TagOptions con políticas AWS Organizations de etiquetas

En este tema se proporciona una breve descripción de las políticas de etiquetas para AWS Organizations y TagOptions paraAWS Service Catalog. También sugiere cómo evitar conflictos de etiquetado cuando se utilizan ambas características simultáneamente.

TagOptions para AWS Service Catalog aplicarlas a los productos aprovisionados (CloudFormationpilas), y etiquetar las políticas para AWS Organizations aplicarlas a AWS cuentas y unidades organizativas (OU) o a una raíz organizativa. Por ejemplo, si adjunta una política de etiquetas a una OU, la misma política de etiquetas se aplica a todas las cuentas de esa OU. Si usa ambas características de etiquetado simultáneamente, debe configurarlas para que no entren en conflicto.

### Políticas de etiquetas

Las políticas de etiquetas te permiten definir reglas sobre cómo usar las etiquetas en los recursos de AWS de sus cuentas en AWS Organizations. Puede utilizar las políticas de etiquetas para crear y mantener un enfoque coherente a la hora de etiquetar los recursos de AWS a nivel de cuenta.

Las políticas de etiquetas proporcionan una forma sencilla de garantizar que los usuarios apliquen etiquetas coherentes, auditen los recursos etiquetados y mantengan una categorización adecuada

de los recursos. También puede definir cómo deben escribirse en mayúsculas las claves de las etiquetas y los valores que desea permitir. Por ejemplo, puede exigir que todas las instancias de EC2 de una cuenta tengan una clave de etiqueta definida como **CostCenter** y valores para que esa etiqueta sea **Data Insights** o **Marketing**.

Las políticas de etiquetado le permiten seleccionar opciones para hacer cumplir las reglas de etiquetado, evitar operaciones no conformes con las etiquetas y especificar los tipos de recursos a los que se aplica la aplicación. Si no elige una opción de aplicación, las políticas de etiquetas le permiten crear o modificar las etiquetas no conformes, pero las notifican como no conformes en la consola AWS Organizations.

Para obtener más información sobre cómo configurar la aplicación del etiquetado a nivel de cuenta, consulte las [Políticas de etiquetas](#) en AWS Organizations.

## TagOptions

TagOptions son una función de etiquetado que AWS Service Catalog se aplica a los productos provisionados a nivel de CloudFormation pila si se aplican a un producto asociado. AWS Service Catalog proporciona una TagOptions biblioteca en la que puede definir los pares clave-valor que desea asociar a sus productos. AWS Service Catalog Al lanzar un AWS Service Catalog producto, debe elegir TagOption valores para las TagOption claves existentes asociadas a esa cartera o producto para lanzar ese producto. Como los TagOptions establece a nivel de cartera o producto, puedes aplicar una taxonomía coherente para etiquetar las carteras compartidas entre cuentas y regiones.

[Para obtener más información sobre cómo configurarlo AWS Service Catalog, consulta TagOptions Biblioteca. AWS Service Catalog TagOption](#)

## Evitar conflictos entre las políticas de AWS Organizations etiquetas y AWS Service Catalog TagOptions

Si configura políticas de etiquetas AWS Organizations para las cuentas de su organización, recomendamos lo siguiente:

- Comparta los requisitos de las etiquetas conformes con los administradores, que también administran TagOptions AWS Service Catalog carteras y productos.
- Comparta los requisitos de las etiquetas conformes con los usuarios finales que puedan lanzar productos AWS Service Catalog y añada etiquetas de usuario final opcionales a los lanzamientos de sus productos.

Supongamos que quiere lanzar un producto AWS Service Catalog que utilice la TagOption clave `city` y que tiene una política de etiquetas que exige que las etiquetas contengan valores de ciudades de EE. UU., como **Atlanta**, **San Francisco** o `city Austin` AWS Service Catalog no te permite lanzar un producto sin haber seleccionado TagOption los valores de TagOption las claves requeridas para el producto.

En este caso, si tienes TagOption valores para la TagOption clave `city` que incluyen ciudades de Sudamérica, por ejemplo **Buenos Aires**, no AWS Service Catalog lanzarás el producto. **Rio de Janeiro** En su lugar, debes seleccionar un TagOption valor que incluya una ciudad de EE. UU. durante el lanzamiento para cumplir con la política de etiquetas.

En la siguiente tabla se muestran escenarios que describen cómo resolver los problemas de etiquetado que pueden surgir al utilizar políticas de etiquetas y TagOptions al mismo tiempo.

Escenario	Motivo	Solución
<p>El producto no se puede iniciar debido a que las etiquetas no cumplen con las normas si la política de etiquetas establece su cumplimiento.</p>	<p>Especifica TagOptions con claves y valores lo que no has añadido a la lista permitida de etiquetas compatibles de tu política de etiquetas.</p> <p>Añadir etiquetas personalizadas opcionales que no se ajusten a su política de etiquetas.</p>	<p>Si configuras un esquema de uso de mayúsculas específico o en la aplicación del uso de mayúsculas en las claves de tu política de etiquetas, asegúrate de que las claves de TagOptions etiquetas y las claves de etiquetas personalizadas opcionales sean coherentes con lo que especificaste en tu política de etiquetas.</p> <p>Tenga en cuenta que si la casilla de aplicación del uso de mayúsculas y minúsculas no está marcada en su política de etiquetas, todas las claves de etiquetas en minúsculas son compatibles y garantiza que sus TagOptions claves</p>

Escenario	Motivo	Solución
		<p>de etiqueta y las claves de etiquetas personalizadas opcionales sean coherentes (por ejemplo, todas en minúsculas) con lo que exige su política de etiquetas.</p>
<p>El producto no se puede lanzar debido a que las mayúsculas de las etiquetas no están escritas correctamente.</p>	<p>Especificar el uso de mayúsculas en TagOptions las claves no es coherente con las normas de aplicación del uso de mayúsculas de la política de etiquetas.</p>	<p>Configure correctamente sus políticas de etiquetas. Si no especifica el cumplimiento de las mayúsculas de las claves de etiqueta, las mayúsculas de las claves de etiqueta por defecto son todas minúsculas.</p> <p>Además, si no especificas el cumplimiento de las mayúsculas de las claves de etiquetas en tu política de etiquetas, asegúrate de que todas las claves de TagOptions etiquetas AWS Service Catalog estén en minúsculas para cumplir con las normas de aplicación.</p> <p>Si utiliza una política de etiquetas que no tiene habilitada la conformidad con el uso de mayúsculas, esa política de etiquetas solo considera que son compatibles todas las claves de etiquetas en minúscula.</p>

Escenario	Motivo	Solución
El producto no se puede lanzar porque los valores de las etiquetas son incompatibles.	Seleccionar un valor de TagOptions etiqueta para el lanzamiento de un producto que no esté en la lista de permitidos por el cumplimiento de los valores de etiqueta de la política de etiquetas.	Asocie TagOptions a sus productos y carteras valores que sean coherentes con lo que ha exigido en la política de listas, los valores de etiqueta permitidos por el cumplimiento de los requisitos.

# Motores externos para AWS Service Catalog

En AWS Service Catalog, los motores externos se representan mediante un tipo de EXTERNAL producto. El tipo de EXTERNAL producto permite la integración de motores de aprovisionamiento de terceros, como Terraform. Puede usar motores externos para ampliar las capacidades de Service Catalog más allá de las AWS CloudFormation plantillas nativas, lo que permite el uso de otras herramientas de estructura como código (IaC).

El tipo de EXTERNAL producto le permite administrar e implementar recursos mediante la interfaz familiar de Service Catalog y, al mismo tiempo, aprovechar las funciones y la sintaxis específicas de la herramienta IaC que elija.

Para habilitar los tipos de EXTERNAL productos en Service Catalog, debe definir un conjunto de recursos estándar en su cuenta. Estos recursos se conocen como motor. Service Catalog delega tareas al motor en puntos específicos de las operaciones de aprovisionamiento y análisis de artefactos.

Un artefacto de aprovisionamiento representa la versión específica de un producto dentro de Service Catalog, lo que le permite administrar e implementar recursos coherentes.

Cuando llamas a [DescribeProvisioningParameters](#) las operaciones AWS Service Catalog de [DescribeProvisioningArtifact](#) un artefacto de aprovisionamiento para un tipo de EXTERNAL producto, Service Catalog invoca una AWS Lambda función del motor. Esto es necesario para extraer la lista de parámetros del artefacto de aprovisionamiento proporcionado y devolverlos a AWS Service Catalog. Estos parámetros se utilizarán más adelante como parte del proceso de aprovisionamiento.

Cuando EXTERNAL aprovisiona un artefacto de aprovisionamiento mediante una llamada [ProvisionProduct](#), Service Catalog primero realiza algunas acciones internamente y, a continuación, envía un mensaje a una cola de Amazon SQS en el motor. A continuación, el motor asume la función de lanzamiento proporcionada (la función de IAM que se asigna a un producto como restricción de lanzamiento), aprovisiona los recursos en función del artefacto de aprovisionamiento proporcionado e invoca la API para informar sobre el éxito o el fracaso. [NotifyProvisionProductEngineWorkflowResult](#)

Las llamadas a [UpdateProvisionedProduct](#) [TerminateProvisionedProduct](#) se gestionan de forma similar, y cada una tiene una cola y API de notificación distintas:

- [NotifyProvisionProductEngineWorkflowResult](#)
- [NotifyUpdateProvisionedProductEngineWorkflowResult](#)

- [NotifyTerminateProvisionedProductEngineWorkflowResult.](#)

## Temas

- [Consideraciones](#)
- [Análisis de parámetros](#)
- [Aprovisionando](#)
- [Actualización](#)
- [Terminando](#)
- [Etiquetado](#)

## Consideraciones

Límite de un motor externo por cuenta de hub

Solo puede usar un motor de EXTERNAL aprovisionamiento por cuenta de Service Catalog Hub. El hub-and-spoke modelo Service Catalog permite a la cuenta central crear productos básicos y compartir la cartera, mientras que las cuentas radiales importan carteras y aprovechan los productos.

Este límite se debe a que solo se EXTERNAL puede enrutar a un motor de una cuenta. Si un administrador quiere tener varios motores externos, debe configurar los motores externos (junto con las carteras y los productos) en diferentes cuentas centrales.

Los motores externos solo admiten funciones de lanzamiento con restricciones de lanzamiento

EXTERNAL Los artefactos de aprovisionamiento solo admiten el aprovisionamiento con funciones de lanzamiento que se especifican mediante restricciones de lanzamiento. Una restricción de lanzamiento especifica la función de IAM que asume Service Catalog cuando un usuario final lanza, actualiza o finaliza un producto. [Para obtener más información sobre las restricciones de lanzamiento, consulte AWS Service Catalog Restricciones de lanzamiento.](#)

## Análisis de parámetros

EXTERNAL Los artefactos de aprovisionamiento pueden ser de cualquier formato. Esto significa que, al crear un tipo de EXTERNAL producto, el motor debe extraer la lista de parámetros del artefacto de aprovisionamiento proporcionado y devolverlos a Service Catalog. Para ello, se crea una función Lambda en su cuenta que pueda aceptar el siguiente formato de solicitud, procesar el artefacto de aprovisionamiento y devolver el siguiente formato de respuesta.

**⚠ Important**

Se debe asignar un nombre a la función Lambda.  
**ServiceCatalogExternalParameterParser**

Sintaxis de la solicitud:

```
{
  "artifact": {
    "path": "string",
    "type": "string"
  },
  "launchRoleArn": "string"
}
```

Campo	Tipo	Obligatorio	Descripción
artefacto	objeto	Sí	Detalles del artefacto que se va a analizar.
artefacto/ruta	cadena	Sí	Ubicación desde donde el analizador descarga el artefacto . Por ejemplo, paraAWS_S3, esta es la URI de Amazon S3.
artefacto/tipo	cadena	Sí	Tipo de artefacto . Valor permitido :AWS_S3.
LaunchRole	cadena	No	El nombre del recurso de Amazon (ARN) de la función de lanzamiento que se debe asumir al descargar el artefacto

Campo	Tipo	Obligatorio	Descripción
			. Si no se proporciona ninguna función de lanzamiento, se utiliza la función de ejecución de Lambda.

### Sintaxis de la respuesta:

```
{
  "parameters": [
    {
      "key": "string",
      "defaultValue": "string",
      "type": "string",
      "description": "string",
      "isNoEcho": boolean
    },
  ]
}
```

Campo	Tipo	Obligatorio	Descripción
parameters	list	Sí	La lista de parámetros que Service Catalog solicita al usuario final al aprovisionar un producto o actualizar un producto aprovisionado. Si no hay ningún parámetro definido en el artefacto, se devuelve una lista vacía.

Campo	Tipo	Obligatorio	Descripción
key	cadena	Sí	La clave de parámetro .
defaultValue	cadena	No	El valor predeterminado del parámetro si el usuario final no proporciona ningún valor.
type	cadena	Sí	El tipo esperado del valor del parámetro para el motor. Por ejemplo, una cadena, un booleano o un mapa. Los valores permitidos son específicos de cada motor. Service Catalog pasa cada valor de parámetro al motor en forma de cadena.
Descripción	cadena	No	Descripción del parámetro. Se recomienda que sea fácil de usar.

Campo	Tipo	Obligatorio	Descripción
isNoEcho	boolean	no	Determina si el valor del parámetro no se repite en los registros. El valor predeterminado es false (los valores de los parámetros se repiten).

## Aprovisionando

Para la [ProvisionProduct](#) operación, Service Catalog delega el aprovisionamiento real de los recursos al motor. El motor se encarga de interactuar con la solución de iAC que elija (como Terraform) para aprovisionar los recursos tal como se definen en el artefacto. El motor también es responsable de notificar el resultado a Service Catalog.

Service Catalog envía todas las solicitudes de aprovisionamiento a una cola de Amazon SQS de su cuenta denominada `ServiceCatalogExternalProvisionOperationQueue`

Sintaxis de la solicitud:

```
{
  "token": "string",
  "operation": "string",
  "provisionedProductId": "string",
  "provisionedProductName": "string",
  "productId": "string",
  "provisioningArtifactId": "string",
  "recordId": "string",
  "launchRoleArn": "string",
  "artifact": {
    "path": "string",
    "type": "string"
  },
  "identity": {
    "principal": "string",
    "awsAccountId": "string",
    "organizationId": "string"
  }
}
```

```

    },
    "parameters": [
      {
        "key": "string",
        "value": "string"
      }
    ],
    "tags": [
      {
        "key": "string",
        "value": "string"
      }
    ]
  }
}

```

Campo	Tipo	Obligatorio	Descripción
token	cadena	Sí	El token que identific a esta operación. El token debe devolverse a Service Catalog para notificar los resultados de la ejecución.
operación	cadena	Sí	Este campo debe ser PROVISION_PRODUCT para esta operación.
provisionedProductId	cadena	Sí	ID del producto aprovisionado.
provisionedProduct Name	cadena	Sí	Nombre del producto aprovisionado.
ID del producto	cadena	Sí	ID del producto.
provisioningArtifactId	cadena	Sí	ID del artefacto de aprovisionamiento.

Campo	Tipo	Obligatorio	Descripción
recordId	cadena	Sí	ID del registro de Service Catalog para esta operación.
launchRoleArn	cadena	Sí	Nombre de recurso de Amazon (ARN) para la función de IAM que se utilizará para el aprovisionamiento de recursos.
artefacto	objeto	Sí	Detalles del artefacto que define cómo se aprovisionan los recursos.
artefacto/ruta	cadena	Sí	Ubicación desde donde el motor descarga el artefacto . Por ejemplo, paraAWS_S3, esta es la URI de Amazon S3.
artefacto/tipo	cadena	Sí	Tipo de artefacto . Valor permitido :AWS_S3.
identity	cadena	No	El campo no se utiliza actualmente.
parameters	list	Sí	Lista de pares clave-valor de parámetros que el usuario ingresó en Service Catalog como entradas para esta operación.

Campo	Tipo	Obligatorio	Descripción
tags	list	Sí	Lista key-value-pairs del usuario introducido en Service Catalog como etiquetas para aplicarlas a los recursos aprovisionados.

Notificación de resultados del flujo de trabajo:

Invoca la [NotifyProvisionProductEngineWorkflowResult](#) API con el objeto de respuesta especificado en la página de detalles de la API.

## Actualización

Para la [UpdateProvisionedProduct](#) operación, Service Catalog delega la actualización real de los recursos en el motor. El motor se encarga de interactuar con la solución de iAC que elijas (como Terraform) para actualizar los recursos tal y como se definen en el artefacto. El motor también es responsable de notificar el resultado a Service Catalog.

Service Catalog envía todas las solicitudes de actualización a una cola de Amazon SQS de su cuenta denominada `ServiceCatalogExternalUpdateOperationQueue`.

Sintaxis de la solicitud:

```
{
  "token": "string",
  "operation": "string",
  "provisionedProductId": "string",
  "provisionedProductName": "string",
  "productId": "string",
  "provisioningArtifactId": "string",
  "recordId": "string",
  "launchRoleArn": "string",
  "artifact": {
    "path": "string",
    "type": "string"
  }
},
```

```

"identity": {
  "principal": "string",
  "awsAccountId": "string",
  "organizationId": "string"
},
"parameters": [
  {
    "key": "string",
    "value": "string"
  }
],
"tags": [
  {
    "key": "string",
    "value": "string"
  }
]
}

```

Campo	Tipo	Obligatorio	Descripción
token	cadena	Sí	El token que identifica esta operación. El token debe devolverse a Service Catalog para notificar los resultados de la ejecución.
operación	cadena	Sí	Este campo debe ser UPDATE_PROVISION_PRODUCT para esta operación.
provisionedProductId	cadena	Sí	ID del producto provisionado.
provisionedProduct Name	cadena	Sí	Nombre del producto provisionado.

Campo	Tipo	Obligatorio	Descripción
ID del producto	cadena	Sí	ID del producto.
provisioningArtifactId	cadena	Sí	ID del artefacto de aprovisionamiento.
recordId	cadena	Sí	ID del registro de Service Catalog para esta operación.
launchRoleArn	cadena	Sí	Nombre de recurso de Amazon (ARN) para la función de IAM que se utilizará para el aprovisionamiento de recursos.
artefacto	objeto	Sí	Detalles del artefacto que define cómo se aprovisionan los recursos.
artefacto/ruta	cadena	Sí	Ubicación desde donde el motor descarga el artefacto . Por ejemplo, paraAWS_S3, esta es la URI de Amazon S3.
artefacto/tipo	cadena	Sí	Tipo de artefacto . Valor permitido :AWS_S3.
identity	cadena	No	El campo no se utiliza actualmente.

Campo	Tipo	Obligatorio	Descripción
parameters	list	Sí	Lista de pares clave-valor de parámetros que el usuario ingresó en Service Catalog como entradas para esta operación.
tags	list	Sí	Lista key-value-pairs del usuario introducido en Service Catalog como etiquetas para aplicarlas a los recursos aprovisionados.

Notificación de resultados del flujo de trabajo:

Invoca la [NotifyUpdateProvisionedProductEngineWorkflowResult](#) API con el objeto de respuesta especificado en la página de detalles de la API.

## Terminando

Para la [TerminateProvisionedProduct](#) operación, Service Catalog delega la terminación real de los recursos en el motor. El motor se encarga de interactuar con la solución de IaC que elija (como Terraform) para eliminar los recursos tal y como se definen en el artefacto. El motor también es responsable de notificar el resultado a Service Catalog.

Service Catalog envía todas las solicitudes de finalización a una cola de Amazon SQS de su cuenta denominada `ServiceCatalogExternalTerminateOperationQueue`

Sintaxis de la solicitud:

```
{
  "token": "string",
  "operation": "string",
  "provisionedProductId": "string",
  "provisionedProductName": "string",
```

```

"recordId": "string",
"launchRoleArn": "string",
"identity": {
  "principal": "string",
  "awsAccountId": "string",
  "organizationId": "string"
}
}

```

Campo	Tipo	Obligatorio	Descripción
token	cadena	Sí	El token que identifica esta operación. El token debe devolverse a Service Catalog para notificar los resultados de la ejecución.
operación	cadena	Sí	Este campo debe ser <code>TERMINATE_PRODUCT</code> para esta operación.
provisionedProductId	cadena	Sí	ID del producto provisionado.
provisionedProduct Name	cadena	Sí	Nombre del producto provisionado.
recordId	cadena	Sí	ID del registro de Service Catalog para esta operación.
launchRoleArn	cadena	Sí	Nombre de recurso de Amazon (ARN) para la función de IAM que se utilizará para el

Campo	Tipo	Obligatorio	Descripción
			aprovisionamiento de recursos.
identity	cadena	No	El campo no se utiliza actualmente.

Notificación de resultados del flujo de trabajo:

Invoca la [NotifyTerminateProvisionedProductEngineWorkflowResultAPI](#) con el objeto de respuesta especificado en la página de detalles de la API.

## Etiquetado

Para administrar etiquetas a través de Resource Groups, su función de lanzamiento necesitará las siguientes declaraciones de permiso adicionales:

```
{
  "Effect": "Allow",
  "Action": [
    "resource-groups:CreateGroup",
    "resource-groups:ListGroupResources"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "tag:GetResources",
    "tag:GetTagKeys",
    "tag:GetTagValues",
    "tag:TagResources",
    "tag:UntagResources"
  ],
  "Resource": "*"
}
```

 **Note**

La función de lanzamiento también necesita permisos de etiquetado en los recursos específicos del artefacto, por ejemplo. `ec2:CreateTags`

# Monitorización en AWS Service Catalog

Puedes monitorizar tus AWS Service Catalog recursos con Amazon CloudWatch, que recopila y procesa datos sin procesar para AWS Service Catalog convertirlos en métricas legibles. Estas estadísticas se registran durante un periodo de dos semanas, para que pueda obtener acceso a información histórica y obtener una mejor perspectiva del desempeño de su servicio. Los datos de métricas de AWS Service Catalog se envían automáticamente a CloudWatch en periodos de un minuto. Para obtener más información al respecto CloudWatch, consulta la [Guía del CloudWatch usuario de Amazon](#).

Para ver una lista de las métricas y dimensiones disponibles, consulte [AWS Service Catalog CloudWatch Métricas](#).

La supervisión es un aspecto importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de AWS Service Catalog y sus soluciones de AWS. Debe recopilar datos de monitorización de todas las partes de su solución de AWS para que le resulte más sencillo depurar un error que se produce en distintas partes del código, en caso de que ocurra. Antes de empezar a monitorear AWS Service Catalog, debe crear un plan de monitoreo que incluya respuestas a las siguientes preguntas:

- ¿Cuáles son los objetivos de la supervisión?
- ¿Qué recursos va a supervisar?
- ¿Con qué frecuencia va a supervisar estos recursos?
- ¿Qué herramientas de monitoreo va a utilizar?
- ¿Quién se encargará de realizar las tareas de monitoreo?
- ¿Quién debería recibir una notificación cuando surjan problemas?

## Herramientas de monitorización

AWS proporciona varias herramientas que puede usar para monitorizar AWS Service Catalog. Puede configurar algunas de estas herramientas para que monitoricen por usted, pero otras herramientas requieren intervención manual. Le recomendamos que automatice las tareas de monitorización en la medida de lo posible.

## Herramientas de monitorización automatizadas

Puedes usar CloudWatch las alarmas de Amazon para monitorear AWS Service Catalog y reportar interrupciones.

CloudWatch las alarmas controlan una única métrica durante un período de tiempo que usted especifique y realizan una o más acciones en función del valor de la métrica en relación con un umbral determinado durante varios períodos de tiempo. La acción es una notificación enviada a un tema del Servicio de Notificación Simple (Amazon SNS) o a una política de Auto Scaling de Amazon EC2. CloudWatch las alarmas no invocan acciones simplemente porque se encuentran en un estado determinado; el estado debe haber cambiado y se ha mantenido durante un número específico de períodos. Para obtener información sobre cómo crear una alarma, consulta [Cómo crear CloudWatch alarmas en Amazon](#). Para obtener más información sobre el uso de CloudWatch las métricas de Amazon con AWS Service Catalog, consulta [AWS Service Catalog CloudWatch Métricas](#).

## AWS Service Catalog CloudWatch Métricas

Puedes monitorizar tus AWS Service Catalog recursos con Amazon CloudWatch, que recopila y procesa datos sin procesar para AWS Service Catalog convertirlos en métricas legibles. Estas estadísticas se registran durante un periodo de dos semanas, para que pueda obtener acceso a información histórica y obtener una mejor perspectiva del desempeño de su servicio. Los datos de métricas de AWS Service Catalog se envían automáticamente a CloudWatch en periodos de un minuto. Para obtener más información CloudWatch, consulta la [Guía del CloudWatch usuario de Amazon](#).

### Temas

- [Habilitar CloudWatch las métricas](#)
- [Métricas y dimensiones disponibles](#)
- [Visualización de las métricas de AWS Service Catalog](#)

## Habilitar CloudWatch las métricas

CloudWatch Las métricas de Amazon están habilitadas de forma predeterminada.

## Métricas y dimensiones disponibles

Las métricas y dimensiones que se AWS Service Catalog envían a Amazon CloudWatch se muestran a continuación.

### Métricas de AWS Service Catalog

El espacio de nombres de AWS/ServiceCatalog incluye las siguientes métricas.

Métrica	Descripción
ProvisionedProductLaunch	<p>El número de productos aprovisionados lanzado para un producto determinado y el artefacto de aprovisionamiento en un periodo especificado.</p> <p>Unidades: recuento</p> <p>Estadísticas válidas: mínimo, máximo, suma, promedio</p>

### Dimensiones de las métricas de AWS Service Catalog

AWS Service Catalog envía las siguientes dimensiones a Amazon CloudWatch.

Dimensión	Descripción
State	<p>Esta dimensión filtra los datos solicitados de todos los productos aprovisionados lanzados con este estado especificado. Esto le ayuda a clasificar los datos por el estado del lanzamiento.</p> <p>Estado válido: SUCCEEDED, FAILED</p>
ProductId	<p>Esta dimensión filtra únicamente los datos solicitados para el ID de producto identificado. Esto le ayuda a seleccionar un producto exacto desde el que efectuar el lanzamiento.</p>
ProvisioningArtifactId	<p>Esta dimensión filtra únicamente los datos solicitados para el ID de artefacto de aprovisionamiento identificado.</p>

Dimensión	Descripción
	ado. Esto le ayuda a seleccionar una versión exacta de productos desde la que efectuar el lanzamiento.

## Visualización de las métricas de AWS Service Catalog

Puedes ver CloudWatch las métricas de Amazon en la CloudWatch consola de Amazon, que proporciona una visualización detallada y personalizable de tus recursos, así como del número de tareas en ejecución en un servicio.

### Temas

- [Visualización de AWS Service Catalog métricas en Amazon CloudWatch Console](#)

## Visualización de AWS Service Catalog métricas en Amazon CloudWatch Console

Puedes ver AWS Service Catalog las métricas en la CloudWatch consola de Amazon. La CloudWatch consola de Amazon proporciona una vista detallada de AWS Service Catalog las métricas y puedes adaptarlas a tus necesidades. Para obtener más información sobre Amazon CloudWatch, consulta la [Guía del CloudWatch usuario de Amazon](#).

Para ver las métricas en la CloudWatch consola de Amazon

1. Abre la CloudWatch consola de Amazon en <https://console.aws.amazon.com/cloudwatch/>.
2. En la sección Metrics (Métricas) del panel de navegación izquierdo, elija Service Catalog (Catálogo de servicios).
3. Seleccione las métricas que desea ver.

## Registrar llamadas a la API de AWS Service Catalog mediante AWS CloudTrail

AWS Service Catalog está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en AWS Service Catalog. CloudTrail captura todas las llamadas a la API AWS Service Catalog como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de AWS Service Catalog y las llamadas desde el código a las operaciones de la API de AWS Service Catalog. Si crea una ruta, puede habilitar la entrega

continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para AWS Service Catalog. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por usted CloudTrail, puede determinar a AWS Service Catalog qué dirección IP se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la [Guía AWS CloudTrail del usuario](#).

## AWS Service Catalog información en CloudTrail

CloudTrail está habilitada en tu AWS cuenta al crearla. Cuando se produce una actividad en AWS Service Catalog, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte [Visualización de eventos con el historial de CloudTrail eventos](#).

Para mantener un registro continuo de eventos en la cuenta de AWS, incluidos los eventos de AWS Service Catalog, cree un registro de seguimiento. Un rastro permite CloudTrail entregar 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 de AWS. 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. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- [Introducción a la creación de registros de seguimiento](#)
- [Servicios e integraciones compatibles con AWS CloudTrail](#)
- [Configuración de notificaciones de Amazon SNS para AWS CloudTrail](#)
- [Recibir archivos de registro de AWS CloudTrail de varias regiones](#) y [Recepción de archivos de registro de AWS CloudTrail de varias cuentas](#)

CloudTrail [registra](#) todas AWS Service Catalog las acciones. Por ejemplo, las llamadas a las [CreatePortfolio](#) [UpdateProvisionedProduct](#) acciones [CreateProduct](#) y las llamadas generan entradas en los archivos de CloudTrail registro.

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

- Si la solicitud se realizó con credenciales de usuario AWS Identity and Access Management (IAM) o credenciales de usuario raíz.
- 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 el [elemento userIdentity de CloudTrail](#).

## Descripción de las entradas de los archivos de registro de AWS Service Catalog

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico. En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que muestra la CreateApplication API.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "account",
    "arn": "arn:aws:iam::12345789012:user/dev-haw",
    "accountId": "12345789012",
    "accessKeyId": "keyId",
    "userName": "dev-haw"
  },
  "eventTime": "2020-09-23T21:07:58Z",
  "eventSource": "servicecatalog-appregistry.amazonaws.com",
  "eventName": "CreateApplication",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "205.251.233.48",
  "userAgent": "aws-cli/1.18.140 Python/3.6.11
Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 boto3/1.17.63",
  "requestParameters": {
    "name": "hawTestCT",
    "clientToken": "6f36d650-a086-47cf-810a-fbfb2f8ad33"
  },
}
```

```
"responseElements": {
  "application": {
    "applicationArn": "arn:aws:servicecatalog:us-
east-1:12345789012:application/app-02ocuq2cie2328pv64ya78e22f",
    "applicationId": "app-02ocuq2cie2328pv64ya78e22f",
    "creationTime": 1600895277.775,
    "lastUpdateTime": 1600895277.775,
    "name": "hawTestCT",
    "tags": {}
  }
},
"requestID": "1b6ad353-3b06-421b-bcb4-00075a782762",
"eventID": "0a2ca224-cdfd-4c4b-a4ed-163218ff5e2d",
"readOnly": false,
"eventType": "AwsApiCall",
"recipientAccountId": "12345789012"
}
```

# Preferencias de marca de la consola

AWS Service Catalog permite a los administradores especificar las preferencias de marca de la consola para las cuentas. Los administradores pueden usar la marca de la consola para especificar el nombre de la empresa, la imagen del logotipo y un color principal y secundario (de acento) para diversos componentes del sitio. Estas preferencias de marca son visibles tanto para los administradores como para los usuarios finales cuando utilizan la consola.

Las preferencias de marca de la consola mejoran la apariencia de la cuenta y cumplen los siguientes objetivos:

- Crea una transición visual perfecta entre la consola y las aplicaciones internas
- Distingue las cuentas utilizadas por diferentes equipos internos de la misma empresa
- Diferencia las cuentas en varios entornos como el desarrollo, la puesta en escena o la producción

## Note

Los administradores especifican las preferencias de marca de la consola para las cuentas.

Para especificar las preferencias de marca de la consola

1. En el menú de navegación izquierdo, elija Preferencias.
2. Seleccione Editar para las preferencias de marca del modo claro o del modo oscuro.
3. Cargue un Logotipo, introduzca el Nombre de marca y, a continuación, seleccione el Color principal y el Color secundario.
4. Seleccione Guardar.

Para ver una lista de las regiones en las que AWS Service Catalog admite la marca de la consola, consulte [Región de AWSSoporte para la marca de la consola](#).

## Compatibilidad de Región de AWS con las preferencias de marca de la consola

Compatibilidad de AWS Service Catalog con las preferencias de marca de la consola en las Regiones de AWS que se muestran en la tabla siguiente.

Región de AWS name	Identidad de Región de AWS
Este de EE. UU. (Norte de Virginia)	us-east-1
Este de EE. UU. (Ohio)	us-east-2
Oeste de EE. UU. (Norte de California)	us-west-1
Oeste de EE. UU. (Oregón)	us-west-2
África (Ciudad del Cabo)	af-south-1
Asia-Pacífico (Hong Kong)	ap-east-1
Asia-Pacífico (Yakarta)	ap-southeast-3
Asia Pacífico (Mumbai)	ap-south-1
Asia-Pacífico (Osaka)	ap-northeast-3
Asia-Pacífico (Seúl)	ap-northeast-2
Asia-Pacífico (Singapur)	ap-southeast-1
Asia Pacífico (Sídney)	ap-southeast-2
Asia-Pacífico (Tokio)	ap-northeast-1
Canadá (centro)	ca-central-1
Europa (Fráncfort)	eu-central-1
Europa (Irlanda)	eu-west-1

Región de AWS name	Identidad de Región de AWS	
Europa (Londres)	eu-west-2	
Europa (Milán)	eu-south-1	
Europa (París)	eu-west-3	
Europa (Estocolmo)	eu-north-1	
Medio Oriente (Baréin)	me-south-1	
América del Sur (São Paulo)	sa-east-1	
AWS GovCloud (Este de EE. UU.)	us-gov-east-1	
AWS GovCloud (Estados Unidos-Oeste)	us-gov-west-1	

## Historial de documentos

En la siguiente tabla se describen los cambios importantes en la documentación de AWS Service Catalog. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

- Versión de la API: 2014-11-12
- Última actualización de la documentación: 16 de mayo de 2024

Cambio	Descripción	Fecha
<a href="#">Motores externos para AWS Service Catalog</a>	AWS Service Catalog añade nueva documentación para motores externos. Los motores externos se representan mediante un tipo de EXTERNAL producto. El tipo de EXTERNAL producto permite la integración de motores de aprovisionamiento de terceros, como Terraform. Puede usar motores externos para ampliar las capacidades de Service Catalog más allá de las AWS CloudFormation plantillas nativas, lo que permite el uso de otras herramientas de estructura como código (IaC). Para obtener más información, consulte <a href="#">Motores externos</a> para. AWS Service Catalog	16 de mayo de 2024
<a href="#">Actualización de seguridad de IAM</a>	AWS Service Catalog actualiza la AWSServiceCatalogSyncServiceRolePolicy política	7 de mayo de 2024

para cambiarla a `connections` en `codeconnections`. Para más información, consulte [Políticas administradas de AWS para AWS Service Catalog AppRegistry](#).

## Actualizaciones anteriores

En la siguiente tabla se describe el historial de publicación de la documentación AWS Service Catalog anterior al 25 de abril de 2024.

Característica	Descripción	Fecha de lanzamiento de la nueva versión
AWS Service Catalog	Para obtener más información sobre los cambios de Hashicorp en las licencias de Terraform y la actualización al tipo de producto externo, consulte <a href="#">Actualizar los productos existentes de Terraform Open Source y los productos aaprovisionados al tipo de producto externo</a> .	20 de octubre de 2023
AWS Service Catalog	Para obtener información sobre cómo <a href="#">compartir una cartera AWS Organizations</a> y AWS Service Catalog permitir su sincronización AWS Organizations, consulta la <a href="#">AWSServiceCatalogOrganizationsDataSyncServiceRolePolicy</a> política y la función	14 de abril de 2023

Característica	Descripción	Fecha de lanzamiento de la nueva versión
	<a href="#">AWSServiceRoleForServiceCatalogOrgsDataSync</a> vinculada al servicio.	
AWS Service Catalog	Para obtener información sobre cómo <a href="#">administrar los productos conectados AWS Service Catalog a git</a> y permitir la sincronización de las plantillas de un repositorio externo con tus AWS Service Catalog productos, consulta la función vinculada a la <a href="#">AWSServiceCatalogSyncServiceRolePolicy</a> política y al servicio. <a href="#">AWSServiceRoleForServiceCatalogSync</a>	18 de noviembre de 2022
AWS Service Catalog AppRegistry	Para obtener información sobre cómo AppRegistry almacenar tus AWS aplicaciones, sus colecciones de recursos asociadas y los grupos de atributos de las aplicaciones, consulta. <a href="#">AWS Service Catalog AppRegistry</a>	15 de junio de 2022
AWS Service Management Connector	Para obtener más información sobre Connectors for Jira Service Management ServiceNow, consulte <a href="#">AWS Service Management Connector</a> .	9 de junio de 2022

Característica	Descripción	Fecha de lanzamiento de la nueva versión
Conector para Jira Service Management	Para obtener más información sobre las actualizaciones del Conector para Jira Service Management, consulte el <a href="#">conector de administración de servicios de AWS para Jira Service Management</a> .	25 de mayo de 2021
Conector para ServiceNow	Para obtener más información sobre las actualizaciones del conector ServiceNow, consulte <a href="#">AWS Service Management Connector for ServiceNow</a> .	7 de abril de 2021
Conector para ServiceNow	Para obtener más información sobre las actualizaciones del conector ServiceNow, consulte <a href="#">AWS Service Management Connector for ServiceNow</a> .	24 de septiembre de 2020
AWS Service Quotas	Para obtener información sobre cómo AWS Service Catalog funciona con AWS Service Quotas, consulta las cuotas de <a href="#">servicio AWS Service Catalog predeterminadas</a> .	24 de marzo de 2020

Característica	Descripción	Fecha de lanzamiento de la nueva versión
Biblioteca de introducción	Para obtener más información sobre la biblioteca de plantillas de productos bien diseñadas que ofrece, consulte AWS Service Catalog <a href="#">Biblioteca de introducción</a>	10 de marzo de 2020
Guía de versión	Para obtener más información acerca de la guía de versión del producto, consulte <a href="#">Guía de la versión</a> .	17 de diciembre de 2019
Conector para Jira Service Desk	Para empezar a usar el conector para Jira Service Desk, consulte el <a href="#">conector de administración de servicios de AWS para Jira Service Desk</a> .	21 de noviembre de 2019
Conector para ServiceNow	Para obtener más información sobre las actualizaciones del conector ServiceNow, consulte <a href="#">AWS Service Management Connector for ServiceNow</a> .	18 de noviembre de 2019
Nuevo capítulo de seguridad	Para obtener más información sobre la seguridad en AWS Service Catalog, consulte <a href="#">Seguridad en AWS Service Catalog</a> .	31 de octubre de 2019

Característica	Descripción	Fecha de lanzamiento de la nueva versión
Cambio del propietario del producto aprovisionado	Para obtener información sobre cómo cambiar el propietario de los productos aprovisionados, consulte <a href="#">Cambio del propietario del producto aprovisionado</a> .	31 de octubre de 2019
Nueva restricción de actualización de recursos	Para obtener más información acerca de cómo utilizar la restricción RESOURCE_UPDATE para actualizar las etiquetas en los productos aprovisionados, consulte <a href="#">Restricciones de actualización de etiquetas de AWS Service Catalog</a> .	17 de abril de 2019
Conector para ServiceNow	Para empezar a utilizar el conector para ServiceNow, consulte el <a href="#">conector de administración de AWS servicios para ServiceNow</a> .	19 de marzo de 2019
Support para AWS CloudFormation StackSets	Para empezar a usarlo AWS CloudFormation StackSets, consulte <a href="#">Uso AWS CloudFormation StackSets</a> .	14 de noviembre de 2018
Acciones de autoservicio	Para comenzar a utilizar acciones de autoservicio, consulte <a href="#">Acciones de servicio de AWS CloudFormation</a> .	17 de octubre de 2018

Característica	Descripción	Fecha de lanzamiento de la nueva versión
CloudWatch Métricas de Amazon	Para obtener más información sobre CloudWatch las métricas de Amazon, consulta <a href="#">AWS Service Catalog Amazon CloudWatch</a> .	26 de septiembre de 2018
Support para TagOptions	Para administrar etiquetas, consulte <a href="#">AWS Service Catalog TagOptionBiblioteca</a> .	28 de junio de 2017
Importación de una cartera	Para importar una cartera compartida desde otra AWS cuenta, consulta <a href="#">Importación de una cartera</a> .	16 de febrero de 2016
Actualización de la información de permisos	Para conceder acceso a la vista de la consola de usuario final, consulte <a href="#">Acceso a la consola para usuarios finales</a> .	16 de febrero de 2016
Versión inicial	Esta es la versión inicial de la Guía AWS Service Catalog del administrador.	9 de julio de 2015

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