Guía del administrador

AWS Service Catalog

AWS Service Catalog: Guía del administrador

Table of Contents

¿Qué es Service Catalog?

Service Catalog permite a las organizaciones crear y administrar catálogos de servicios de TI AWS aprobados. Estos servicios de TI pueden incluir desde imágenes de máquinas virtuales, servidores, software, bases de datos, entre otras opciones, para completar la arquitectura 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.

- Self-service descubrimiento y lanzamiento

  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 aprovisionado.

- Fine-grain control de acceso

  Los administradores recopilan las carteras de productos de su catálogo, añaden restricciones y etiquetas de recursos para utilizarlas en el aprovisionamiento y, a continuación, conceden acceso a la cartera a través de usuarios y AWS Identity and Access Management grupos (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 Detalles del producto de Service Catalog.

El API de Service Catalog proporciona control mediante programación de todas las acciones del usuario final como alternativa al uso de la Consola de administración de AWS. 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 gobernar 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.

Users

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 del catálogo preparan CloudFormation plantillas, configuran las restricciones y gestionan las funciones de IAM de los productos a fin de proporcionar una gestión avanzada de los recursos.
- Usuarios finales: reciben AWS credenciales de su departamento o gerente de TI y las utilizan Consola de administración de AWS para lanzar productos a los que tienen acceso. 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 AWS recursos, como instancias EC2, volúmenes de almacenamiento, bases de datos, configuraciones de monitoreo y componentes de red, o AWS Marketplace productos empaquetados. Un producto puede ser una instancia de procesamiento única que ejecute AWS Linux, una aplicación web de varios niveles completamente configurada que se ejecute en su propio entorno o cualquier otra instancia intermedia.

Para crear un producto, importe una AWS CloudFormation plantilla. AWS CloudFormation las plantillas definen los AWS recursos necesarios para el producto, las relaciones entre los recursos y los parámetros que los usuarios finales pueden introducir al lanzar el producto para configurar 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 a escala en AWS. Puede acceder a las funciones clave de Service Catalog, como la catalogación de plantillas de Terraform estandarizadas y previamente aprobadas, el control de acceso, el aprovisionamiento con privilegios mínimos, el control de versiones, el etiquetado y el uso compartido en miles de cuentas. 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 Primeros pasos con un producto de Terraform.

Productos aprovisionados

AWS CloudFormation Las pilas facilitan la gestión del ciclo de vida de su producto, ya que le permiten aprovisionar, etiquetar, actualizar y finalizar su instancia de producto como una sola unidad. Una AWS CloudFormation pila incluye una AWS CloudFormation plantilla, escrita en formato JSON o YAML, y su colección de recursos asociada. Un producto aprovisionado es una pila. Cuando un usuario final lanza un producto, la instancia del producto que se ha aprovisionado mediante Service Catalog es una pila con los recursos necesarios para ejecutar el producto. Para obtener más información, consulte la AWS CloudFormation Guía del usuario de .

Carteras

Una cartera es una colección de productos que contiene 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 sus carteras con otras AWS cuentas y permitir que el administrador de esas cuentas las distribuya con restricciones adicionales, como limitar las instancias de EC2 que 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. Aplica permisos AWS Identity and Access Management (IAM) para controlar quién puede ver y modificar su catálogo. Es posible asignar permisos de IAM a usuarios de IAM, grupos y roles.

Cuando un usuario lanza un producto con un rol de IAM asignado, Service Catalog utiliza dicha función para lanzar los recursos en la nube del producto mediante 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 las formas en que se pueden implementar AWS recursos específicos para un producto. Puede usarlas para aplicar límites a los productos para el control de costos o de dirección. Existen diferentes tipos de AWS Service Catalog restricciones: restricciones de lanzamiento, restricciones de notificación y restricciones de plantilla.

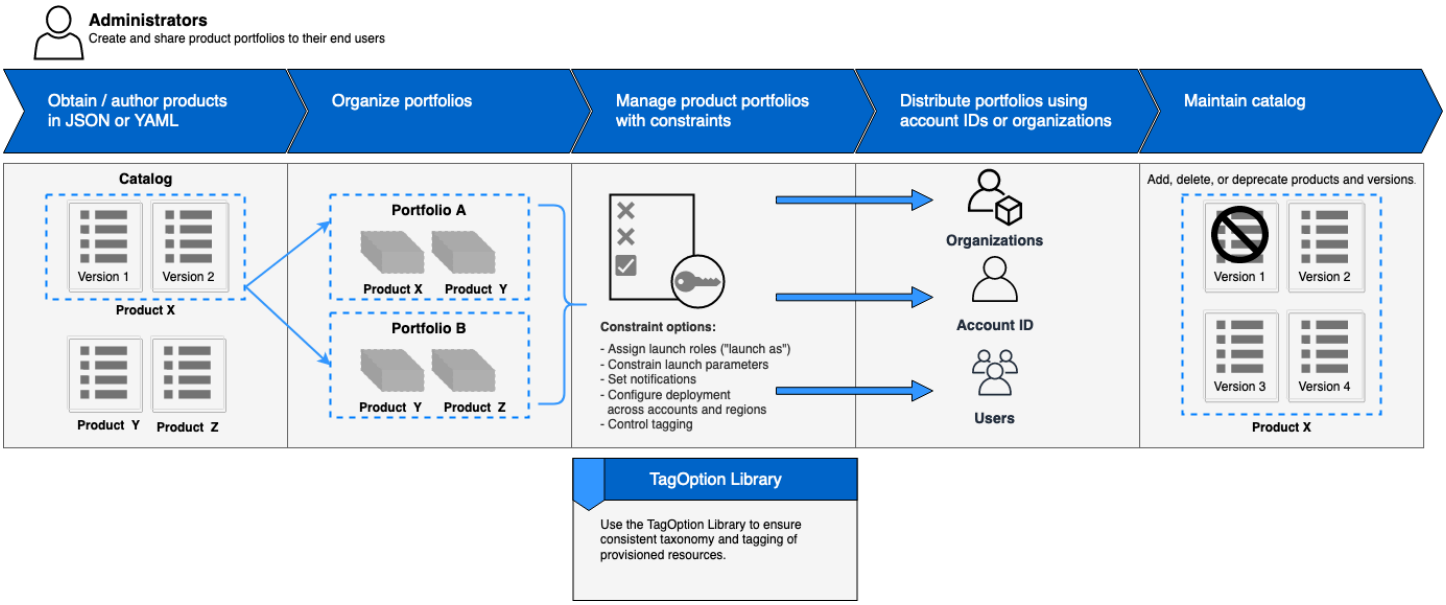
Las restricciones de lanzamiento permiten especificar una función de un producto en una cartera. Utilice este rol para provisionar los recursos durante el lanzamiento, de modo que pueda restringir los permisos del usuario sin que esto afecte a la capacidad de los usuarios de provisionar productos del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

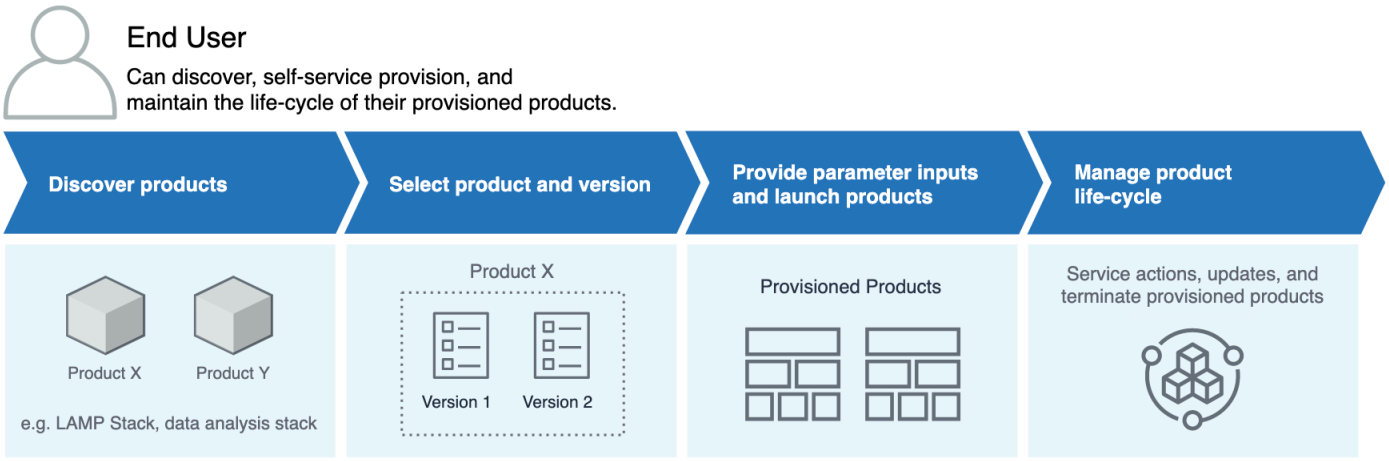
Flujo de trabajo inicial del administrador

Este diagrama 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.



AWS Service Catalog cuotas de servicio predeterminadas

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

AWS Organizations

- AWS Service Catalog administradores delegados 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.

Configuración de los pasos

Temas

- Inscríbase en una Cuenta de AWS

Inscríbase en una Cuenta de AWS

Para empezar AWS, necesitas un Cuenta de AWS. Para obtener información sobre cómo crear un Cuenta de AWS, consulte Cómo empezar con un Cuenta de AWS en la Guía de AWS Account Management referencia.

Otorgar permisos a AWS Service Catalog los administradores

Como administrador del catálogo, necesita acceso a la vista de la consola de AWS Service Catalog administrador 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
- Añadir restricciones de lanzamiento para definir las funciones de IAM que AWS Service Catalog asumen los usuarios finales cuando 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 Nombre de usuario, escriba **`ServiceCatalogAdmin`**.

   c. Seleccione Programmatic access y Consola de administración de AWS access.

   d. Elija Siguiente: permisos.

3. Elija Adjuntar directamente políticas existentes.

4. Elija Crear política 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 AWS recursos en la Guía de Referencia general de AWS referencia.

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 se AWS Service Catalog almacenan 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`** y a las políticas de **`ServiceCatalogAdmin-AdditionalPermissions`**, y después elija Siguiente: 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.

Conceder permisos a los usuarios AWS Service Catalog finales

Antes de que el usuario final pueda utilizarlos AWS Service Catalog, debe conceder acceso a la vista de la consola para el usuario AWS Service Catalog final. Para conceder acceso, se adjuntan políticas al usuario, grupo o rol de IAM que el usuario final utiliza. En el siguiente procedimiento, se adjunta 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 Crear grupo.
4. En el panel de navegación, seleccione Usuarios.
5. Elija Añadir usuarios y haga lo siguiente:
    a. En User name (Nombre de usuario), escriba un nombre para el usuario.
    b. Seleccione Contraseña: acceso a la consola de AWS administración.
    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 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. AWS Service Catalog Esta configuración única 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 está ubicado en la misma región en la que se realizó la llamada 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 0000000000000, se AWS Service Catalog supone que el ARN de SQS correcto es. `arn:aws:sqs:us-east-1:0000000000000:ServiceCatalogTerraformOSProvisionOperationQueue`

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 Lambda del analizador de parámetros creada AWS Service Catalog por los motores proporcionados tiene una política de acceso que otorga permisos `lambda:Invoke` entre cuentas únicamente al director del servicio: AWS Service Catalog

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "servicecatalog.amazonaws.com"
            },
            "Action": "lambda:InvokeFunction",
            "Resource": "arn:aws:lambda:us-
east-1:111122223333:function:ServiceCatalogTerraformOSParameterParser"
        }
    ]
}
```

Este debería ser el único permiso necesario para que la integración funcione correctamente. AWS Service Catalog Sin embargo, puede restringirlo aún más utilizando la clave de contexto de `aws:SourceAccount` Confused Deputy. Al AWS Service Catalog enviar 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:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "servicecatalog.amazonaws.com"
            },
            "Action": "lambda:InvokeFunction",
```

```
            "Resource": "arn:aws:lambda:us-
east-1:111122223333: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 Amazon SQS de entrada a la operación de aprovisionamiento creadas AWS Service Catalog por los motores proporcionados tienen una política de acceso que concede permisos `sqs:SendMessage` entre cuentas (y el KMS asociado) únicamente al director del servicio: AWS Service Catalog

JSON

```
{
    "Version":"2012-10-17",
    "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-1:111122223333: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:ReEncryptFrom",
                "kms:ReEncryptTo",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-east-1:111122223333:key/key_id"
        }
    ]
}
```

Este debería ser el único permiso necesario para que la integración funcione correctamente. AWS Service Catalog Sin embargo, puede restringirlo aún más utilizando la clave de contexto de `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:

JSON

```
{
    "Version":"2012-10-17",
    "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-1:111122223333: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:ReEncryptFrom",
                "kms:ReEncryptTo",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-east-1:111122223333: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, crea una cartera y, a continuación, un producto. Como usuario final, debe verificar que puede acceder a la consola del usuario final e iniciar 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 CloudFormation plantilla que define los AWS recursos 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 AWS recursos 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

Biblioteca de introducción

AWS Service Catalog proporciona una biblioteca de introducción con plantillas de productos bien diseñadas para que pueda empezar 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

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

- Los permisos necesarios para usar CloudFormation plantillas. Para obtener más información, consulte Controlar el 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 “Gestión de identidad y acceso”.

Más información

Para obtener más información acerca del marco de Well-Architected, consulte AWS Well-Architected.

Cómo empezar con un CloudFormation producto

Cuando empiece a usar 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, crea una cartera y, a continuación, un producto. Como usuario final, debe verificar que puede acceder a la consola del 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 CloudFormation plantilla que define los AWS recursos 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 3: crear una cartera de
- 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 a los usuarios finales acceso a la cartera
- Paso 8: probar la experiencia del usuario final

Paso 1: Descarga la CloudFormation plantilla

Puede usar CloudFormation plantillas para configurar y aprovisionar carteras y productos. Estas 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 CloudFormation . Puede usar el AWS CloudFormation editor o el editor de texto que prefiera 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 CloudFormation de plantillas requiere permisos especiales. Antes de comenzar, asegúrese de que cuenta con los permisos necesarios. Para obtener más información, consulte Requisitos previos en Biblioteca de introducción.

Descarga de la plantilla

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

```
                    running the Amazon Linux AMI. The AMI is chosen based on the
region
                    in which the stack is run. This example creates an EC2 security
                    group for the instance to give you SSH access. **WARNING** This
                    template creates an Amazon EC2 instance. You will be billed for the
AWS resources used if you create a stack from this template.",

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

   "InstanceType" : {
     "Description" : "EC2 instance type.",
     "Type" : "String",
     "Default" : "t2.micro",
     "AllowedValues" : [ "t2.micro", "t2.small", "t2.medium", "m3.medium",
"m3.large",
       "m3.xlarge", "m3.2xlarge" ]
   },

   "SSHLocation" : {
     "Description" : "The IP address range that can SSH to the EC2 instance.",
     "Type": "String",
     "MinLength": "9",
     "MaxLength": "18",
     "Default": "0.0.0.0/0",
     "AllowedPattern": "(\\d{1,3})\\.(\\d{1,3})\\.(\\d{1,3})\\.(\\d{1,3})/(\\d{1,2})",
     "ConstraintDescription": "Must be a valid IP CIDR range of the form x.x.x.x/x."
  }
 },

 "Metadata" : {
   "AWS::CloudFormation::Interface" : {
     "ParameterGroups" : [{
       "Label" : {"default": "Instance configuration"},
       "Parameters" : ["InstanceType"]
     },{
       "Label" : {"default": "Security configuration"},
       "Parameters" : ["KeyName", "SSHLocation"]
     }],
     "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 AWS Service Catalog restricciones.

  El `KeyName` parámetro le permite especificar un nombre de key pair de Amazon Elastic Compute Cloud (Amazon EC2) que los usuarios finales deben proporcionar cuando lanzan su producto. AWS Service Catalog El par de claves se crea en el siguiente paso.
- Metadatos (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`.

- Mapeos (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 AWS regiones y la imagen de máquina de Amazon (AMI) correspondiente a cada una. AWS Service Catalog utiliza este mapeo para determinar qué AMI usar en función de la AWS región que el usuario seleccione en Consola de administración de AWS.
- 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 EC2 instancia que ejecute Amazon Linux y un grupo de seguridad que permita el acceso SSH a la instancia. La sección Propiedades del recurso de la EC2 instancia utiliza la información que el usuario escribe para configurar el tipo de instancia y un nombre clave para el acceso por SSH.

  CloudFormation usa la AWS región actual para seleccionar el ID de AMI de las asignaciones definidas 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 Guía del usuario de CloudFormation .

Paso 2: Crear un par de claves

Para que tus usuarios finales puedan lanzar el producto que se basa en la plantilla de ejemplo de este tutorial, debes crear un EC2 key pair de Amazon. 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, asegúrate de haber iniciado sesión en la AWS consola y consulta Amazon EC2 Key Pairs en la Guía del EC2 usuario de Amazon.

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

```
. . .
  "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. De lo contrario, lleve a cabo los pasos que figuran a continuación.

Creación de un par de claves

1. Abre la EC2 consola de Amazon 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 de

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 Carteras 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, ya podrá 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.

Cómo 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 Engineering Tools 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 Detalles de soporte, introduzca:
   - 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 CloudFormation (restricciones de plantilla). Para obtener más información, consulte Uso de AWS Service Catalog restricciones.

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 EC2 usuario de Amazon.

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 de IAM que AWS Service Catalog asume cuando un usuario final lanza un producto.

Para este paso, debe añadir una restricción de lanzamiento al producto de escritorio Linux para poder AWS Service Catalog utilizar los recursos de IAM que componen la plantilla del producto. AWS CloudFormation

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. Servicios incluidos en la AWS CloudFormation plantilla del producto
3. Acceso de lectura a la AWS CloudFormation plantilla 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 aprovisionado. 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 puedan utilizar el producto Linux Desktop. Por ejemplo, la `ServiceCatalogEndUserAccess` política concede los permisos de IAM mínimos necesarios para acceder a la vista de la consola del usuario AWS Service Catalog final.

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`— Permite AWS Service Catalog todos los permisos para crear, leer, actualizar, eliminar, enumerar y etiquetar CloudFormation pilas.
   - `ec2`— Permite permisos AWS Service Catalog completos 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 AWS recurso que desee implementar, este permiso puede cambiar.
   - `ec2`— Crea una nueva política administrada para su AWS cuenta y adjunta la política administrada especificada a la función de IAM especificada.
   - `s3`— Permite el acceso a los buckets de Amazon S3 propiedad AWS Service Catalog de. Para implementar el producto, es AWS Service Catalog necesario acceder a los artefactos de aprovisionamiento.
   - `servicecatalog`— Permite AWS Service Catalog permisos para enumerar, leer, escribir, etiquetar y lanzar recursos en nombre del usuario final.
   - `sns`— Permite 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.

   JSON

```
{
    "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, Revisar.
5. En Revisar política, ingrese **`linuxDesktopPolicy`** como Nombre.
6. Elija Crear política.
7. Seleccione Roles en el panel de navegación. Elija Crear rol y haga lo siguiente:

    a. En Seleccione una entidad de confianza, elija AWS servicio y, a continuación, en Caso de uso para otros AWS servicios, elija 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 Tipo de restricción elija Lanzar.
12. Seleccione Seleccionar el rol de IAM. A continuación, elija linuxDesktopLaunchRol y, a continuación, elija Crear.

Paso 7: conceder a los usuarios finales acceso a la cartera

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 Conceder permisos a los usuarios AWS Service Catalog finales.

Para proporcionar acceso a la cartera

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

Paso 8: probar la experiencia del usuario final

Para comprobar que el usuario final puede acceder correctamente a la vista de la consola de usuario final y lanzar el producto, inicie sesión AWS como usuario final y realice esas tareas.

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

1. Siga las instrucciones de Iniciar sesión como usuario de IAM en la Guía del usuario de IAM.
2. En la barra de menús, elija la AWS región en la que creó la `Engineering Tools` cartera. Para este tutorial, seleccione la región us-east-1.
3. Abre la AWS Service Catalog consola en https://console.aws.amazon.com/servicecatalog/para ver:

   - Products: los productos que el usuario puede utilizar.
   - Productos aprovisionados: los productos aprovisionados que el usuario ha lanzado.

Cómo 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 aprovisionado.
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, después, 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 proceso de cambio. El lanzamiento del producto tarda varios minutos. AWS Service Catalog Para ver el estado actual, actualice el navegador. Una vez que el producto se ha lanzado, el estado es Disponible.

Primeros pasos con un producto de Terraform

AWS Service Catalog permite un aprovisionamiento rápido y de autoservicio con control integrado para sus configuraciones de HashiCorp Terraform. AWS Puede utilizarla AWS Service Catalog

como una herramienta única para organizar, gobernar y distribuir sus configuraciones de Terraform a escala interna. AWS AWS Service Catalog es compatible con Terraform en varias funciones 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. AWS En ella AWS Service Catalog, los 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 seguir ofreciendo soporte a HashiCorp las tecnologías, como resultado de los recientes cambios en las licencias de Terraform, AWS Service Catalog cambié cualquier referencia anterior a Terraform Open Source por una referencia externa. 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 o administradora del catálogo, 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, 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
- Etiquetado del producto
- Comparta la cartera y el producto de Terraform con la cuenta de usuario final (cuenta radial)

En el tutorial, se comparte una cartera 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 AWS recurso contenido en el producto Terraform que creó en el tutorial es un sencillo bucket de Amazon S3.

> **Note**
>
> Antes de comenzar, asegúrese de que ha realizado las acciones que se detallan en Configuración AWS Service Catalog.

Temas

Actualizar los productos existentes de Terraform Open Source y los productos aprovisionados 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 aprovisionado. Solo podrá actualizar o cancelar los recursos de Terraform Open Source existentes, incluidos las versiones de los productos y los productos aprovisionados.

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

1. Actualice su motor de referencia de Terraform actual para incluir soporte para AWS Service Catalog los tipos de productos externos y de código abierto de Terraform. 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 de Terraform Open Source.
4. Reaprovisione esos recursos restantes para utilizar el nuevo tipo de producto externo.
5. Cancele cualquier producto aprovisionado existente que utilice el tipo de producto de 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 Terraform en AWS Service Catalog, debe instalar y configurar un motor de aprovisionamiento en su cuenta de administrador de Service Catalog (cuenta hub). 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.

En el caso de los AWS Service Catalog productos que utilizan el tipo de producto externo con HashiCorp la edición comunitaria de Terraform, 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 cómo instalar y configurar el motor de aprovisionamiento Terraform AWS proporcionado. La repo incluye la información siguiente:

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

Paso 1: descargar el archivo de configuración de Terraform

Puede usar un archivo de configuración de Terraform para crear y aprovisionar los 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, se AWS Service Catalog proporciona un archivo de configuración sencillo para que pueda empezar. La configuración crea un bucket de Amazon S3.

Descargar el archivo de configuración

AWS Service Catalog proporciona un ejemplo de archivo de `simple-s3-bucket.tar.gz`configuración para que lo utilice en este tutorial.

Información general del archivo de 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 al AWS Service Catalog aprovisionar 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, es `AWS` decir. AWS Service Catalog solo admite `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 AWS infraestructura para el aprovisionamiento. Para este tutorial, el archivo de configuración de Terraform especifica Amazon S3.
- Salida (opcional): la información o el valor obtenidos, similar a los valores obtenidos 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, se crea un producto de Terraform que contiene un bucket de Amazon S3 simple.

Cree un nuevo producto de Terraform

1. Abra la AWS Service Catalog consola en https://console.aws.amazon.com/servicecatalog/e inicie sesión como usuario administrador.
2. Vaya a la sección 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, a continuación, Elegir archivo. Seleccione el archivo que ha descargado en Paso 1: descargar el archivo de configuración de 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 aparecerá un banner de confirmación en la página del producto.

Paso 3: Crear un AWS Service Catalog portafolio

Puede crear un portafolio en su cuenta de AWS Service Catalog administrador (cuenta hub) para organizar y distribuir fácilmente los productos a las cuentas de los usuarios finales (cuentas habladas).

Para crear una cartera

1. Abre la AWS Service Catalog consola en https://console.aws.amazon.com/servicecatalog/e inicia sesión como administrador.
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.

Cómo agregar el producto a una cartera

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.

Después de añadir correctamente el producto a la cartera, AWS Service Catalog muestra un banner de confirmación en la página de la 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 AWS recursos subyacentes 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 AWS Service Catalog de Amazon S3 propio
- Acceso a las operaciones del grupo de recursos `CreateGroup`, `ListGroupResources`, `DeleteGroup` y `Tag` Estas operaciones permiten AWS Service Catalog administrar grupos de recursos y etiquetas

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

1. Mientras esté conectado a la cuenta de AWS Service Catalog administrador, siga las instrucciones para crear nuevas políticas en la pestaña JSON de 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`— Permite permisos AWS Service Catalog completos para enumerar, leer, escribir, aprovisionar y etiquetar el producto Amazon S3.
   - `s3`— Permite el acceso a los buckets de Amazon S3 propiedad AWS Service Catalog de. Para implementar el producto, AWS Service Catalog requiere acceso a los artefactos de aprovisionamiento.
   - `resourcegroups`— Permite AWS Service Catalog crear, enumerar, eliminar y etiquetar Grupos de recursos de AWS.
   - `tag`— Permite permisos AWS Service Catalog de etiquetado.

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

   Pegue el siguiente documento de políticas JSON:

   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, Revisar.
   c. En Revisar política, ingrese **`S3ResourceCreationAndArtifactAccessPolicy`** como Nombre.
   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:
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 las funciones de lanzamiento deben empezar por SCLaunch «» seguido del nombre de función deseado.

10. Elija Crear rol.

> **Important**
>
> Tras crear el rol de inicio en la cuenta de AWS Service Catalog administrador, también debe crear un rol de inicio idéntico en la cuenta del usuario AWS Service Catalog final. 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 de usuario AWS Service Catalog final

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 y 10 descritos anteriormente en Para crear un rol de lanzamiento en la cuenta de AWS Service Catalog administrador.

> **Note**
>
> Al crear un rol de inicio en la cuenta del usuario AWS Service Catalog final, asegúrese de utilizar el mismo administrador **`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.

Cómo asignar una restricción de lanzamiento al producto

1. Abra la AWS Service Catalog consola en /servicecatalog. https://console.aws.amazon.com
2. En el menú de navegación izquierdo, seleccione Cartera.
3. Seleccione la cartera de bucket de S3.
4. En la página 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 Lanzamiento.
6. Elija Introducir el nombre del rol y, a continuación, elija -S3Product. SCLaunch
7. Seleccione Crear.

> **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.

Paso 7: conceder acceso al usuario final

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

En este tutorial, se 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 el portafolio, AWS Service Catalog verifica si esos nombres principales ya existen. Si existen, asocia AWS Service Catalog automáticamente los 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 Conceder permisos a los usuarios AWS Service Catalog finales.

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 periférica.

5. Elija 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.

Cómo compartir la cartera desde la cuenta central de administración

1. Abra la AWS Service Catalog consola en. https://console.aws.amazon.com/servicecatalog/
2. En la página Carteras, seleccione la cartera de bucket de S3. En el menú Acciones, elija Compartir.
3. Seleccione AWS Organizations y, a continuación, filtre según su estructura organizativa.
4. En el panel Organización de AWS , seleccione la cuenta de usuario final (cuenta periférica).

   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 Configuración de uso compartido, seleccione Uso compartido de 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 de Terraform.

Paso 9: probar la experiencia del usuario final

Para comprobar que los usuarios finales puedan acceder correctamente a la vista de la consola de usuario final y lanzar su **`Simple S3 bucket`** producto, inicie sesión AWS como usuario final y realice las siguientes tareas.

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

- Abra la AWS Service Catalog consola en https://console.aws.amazon.com/servicecatalog/para ver:

- Products: los productos que el usuario puede utilizar.
- Productos aprovisionados: los productos aprovisionados que el usuario ha lanzado.

Cómo verificar que el usuario final puede lanzar el producto de 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 aprovisionado.
4. En la página Parámetros, escriba lo siguiente y, a continuación, elija Siguiente:
   - bucket_name: proporciona 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 En proceso de cambio. El lanzamiento del producto tarda varios minutos. AWS Service Catalog 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 de Terraform existente.
- `TerminateProvisionedProductStateMachine`— AWS Service Catalog invoca esta máquina de estados al cancelar un producto aprovisionado por Terraform existente.

Cómo ejecutar la máquina de estados de monitorización

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

   > **Note**
   >
   > AWS Service Catalog crea el ID del producto aprovisionado al aprovisionar 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. Third-party los auditores prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los programas de AWS cumplimiento.

  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. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa 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

El modelo de responsabilidad compartida de AWS 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. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres 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 privacidad de datos y los . Para obtener más información sobre la protección de datos en Europa, consulte el Centro del Reglamento General de Protección de Datos (RGPD).

Para fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure 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:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger la información confidencial almacenada en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 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) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja AWS Service Catalog o Servicios de AWS utiliza la consola, la API o los SDK. AWS CLI AWS Cualquier dato que introduzca en

etiquetas o campos de formato libre utilizados para los nombres se pueden 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 que se cifran en reposo mediante claves. Amazon-managed 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.

Identity and Access Management en AWS Service Catalog

El acceso a las credenciales AWS Service Catalog requeridas. 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”

Identity-based ejemplos de políticas 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 Consola de administración de AWS vista de la consola del usuario final los productos que tiene permiso para lanzar.

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 más 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 AWS Service Catalog Restricciones de lanzamiento.

> **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 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 AWS Service Catalog Restricciones de lanzamiento.

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: `DescribeRecord`y`ScanProvisionedProducts`, 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
- End-user acceso 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.

JSON

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

Esta política equivale funcionalmente a la siguiente política:

JSON

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

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

End-user acceso 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.

JSON

```
{
    "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).

JSON

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

JSON

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

AWS políticas gestionadas 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 otorga *`administrative`* permisos que permiten el acceso total a la vista de la consola de administración y otorga 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, así como 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 aprovisionados 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.

Consulte 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 concede *`read-only`* permisos que permiten el acceso total 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.

Consulte 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 *`contributor`* 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 disponer AWS Service Catalog de todos los permisos necesarios 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 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.

Consulte 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 *`read-only`* permisos 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.

Consulte 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.

Consulte la política: AWSServiceCatalogSyncServiceRolePolicy.

Service-linked detalles del rol

AWS Service Catalog utiliza los detalles de permiso anteriores para el rol `AWSServiceRoleForServiceCatalogSync` vinculado al servicio que se crea cuando un usuario crea o actualiza un AWS Service Catalog producto que 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 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.

Consulte la política: AWSServiceCatalogOrgsDataSyncServiceRolePolicy.

Service-linked detalles del rol

AWS Service Catalog utiliza los detalles de permiso 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 AWS Service Catalog función de sincronización de datos de Organizations 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 AWSServiceCatalogAdminFullAccessen su lugar.
- ServiceCatalogAdminReadOnlyAccess— Úselo AWSServiceCatalogAdminReadOnlyAccessen su lugar.
- ServiceCatalogEndUserFullAccess— Úselo AWSServiceCatalogEndUserFullAccessen su lugar.
- ServiceCatalogEndUserAccess— Úselo AWSServiceCatalogEndUserReadOnlyAccessen 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 AWS políticas administradas

Vea los detalles sobre las actualizaciones de las políticas AWS administradas AppRegistry desde que este servicio comenzó a rastrear 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
AWSServiceCatalogSyncServiceRolePolicy— Actualizar la política gestionada	AWS Service Catalog actualizó la `AWSServiceCatalogSyncServiceRolePolicy` política para cambiarla `codestar-connections` `acodeconnections` .	7 de mayo de 2024
AWSServiceCatalogAdminFullAccess— Actualizar la política gestionada	AWS Service Catalog actualizó la `AWSServiceCatalogAdminFullAccess` política para incluir los permisos necesarios para que el AWS Service Catalog administrador pueda crear el rol `AWSServiceRoleForServiceCatalogOrgsDataSync` vinculado al servicio (SLR) en su cuenta.	14 de abril de 2023
AWSServiceCatalogOrgsDataSyncServiceRolePolicy – Nueva política administrada	AWS Service Catalog agregó el`AWSServiceCatalogOrgsDataSyncServiceRolePolicy` , que está asociado al rol `AWSServiceRoleForServiceCat`	14 de abril de 2023

Cambio	Descripción	Fecha
	`alogOrgsDataSync` 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.	
AWSServiceCatalogAdminFullAccess— Actualizar la política gestionada	AWS Service Catalog actualizó la `AWSServiceCatalogAdminFullAccess` política para incluir todos los permisos del AWS Service Catalog administrador y crear compatibilidad con AppRegistry.	12 de enero de 2023
AWSServiceCatalogSyncServiceRolePolicy – Nueva política administrada	AWS Service Catalog agregó la `AWSServiceCatalogSyncServiceRolePolicy` política, que está asociada a la función `AWSServiceRoleForServiceCatalogSync` vinculada al servicio (SLR). Esta política permite sincronizar AWS Service Catalog las plantillas de un repositorio externo con los productos. AWS Service Catalog	18 de noviembre de 2022

Cambio	Descripción	Fecha
AWSServiceRoleForServiceCatalogSync— Nuevo rol vinculado a un servicio	AWS Service Catalog agregó el rol `AWSServiceRoleForServiceCatalogSync` vinculado al servicio (SLR). Esta función es necesaria AWS Service Catalog para usar CodeConnections y crear, actualizar y describir los artefactos de AWS Service Catalog aprovisionamiento de un producto.	18 de noviembre de 2022

Cambio	Descripción	Fecha
AWSServiceCatalogAdminFullAccess— Política gestionada actualizada	AWS Service Catalog actualizó la `AWSServiceCatalogAdminFullAccess` 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 `AWSServiceCatalogAdminFullAccess` 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 ¿Qué es ABAC para AWS? en AWS Identity and Access Management.	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 para 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 Service-linked Los roles están predefinidos AWS Service Catalog e incluyen todos los permisos que el servicio necesita 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 funciones vinculadas a servicios, consulte AWS Servicios que funcionan con IAM y busque los servicios que tengan la palabra «Sí» en la columna de funciones. Service-linked Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Service-linked permisos de rol para **`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 AWS Service Catalog aprovisionamiento de un producto.

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 AWSServiceCatalogSyncServiceRolePolicypermite 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 los permisos de los Service-linked roles en la Guía del usuario de IAM.

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

No es necesario crear manualmente el rol vinculado al `AWSServiceRoleForServiceCatalogSync` servicio. AWS Service Catalog crea automáticamente el rol vinculado al servicio cuando lo estableces CodeConnections en la Consola de administración de AWS, 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 roles vinculados al servicio, entonces AWS Service Catalog creaste el `AWSServiceRoleForServiceCatalogSync` rol 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.

Service-linked permisos de rol para **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`:

JSON

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

La política de permisos de roles denominada AWSServiceCatalogOrgsDataSyncServiceRolePolicypermite 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 los permisos de los Service-linked roles en la Guía del usuario de IAM.

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

No es necesario crear manualmente el rol vinculado al `AWSServiceRoleForServiceCatalogOrgsDataSync` servicio. AWS Service Catalog considera su acción de habilitar Compartir 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 Consola de administración de AWS, 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 un servicio 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 compatibles para AWS Service Catalog roles vinculados a servicios

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.

Nombre de la región	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

Nombre de la región	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 (US-East)	us-gov-east-1	No
AWS GovCloud (US-West)	us-gov-west-1	No

Resolución de problemas AWS Service Catalog 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 estoy autorizado a realizar lo siguiente: PassRole
- Quiero permitir que personas ajenas a mi AWS cuenta para acceder a mi AWS Service Catalog recursos

No estoy autorizado a realizar ninguna acción en AWS Service Catalog

Si Consola de administración de AWS le indica que no está autorizado a realizar una acción, debe ponerse en contacto con su administrador para obtener ayuda. El administrador es la persona que le proporcionó las credenciales de inicio de sesión. En el siguiente ejemplo, el error se produce cuando el usuario mateojackson intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio my-example-widget, pero no tiene los permisos ficticios `aws: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 estoy autorizado a realizar lo **`siguiente: 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. El administrador es la persona que le facilitó el nombre de usuario y la 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 la función 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 tenga 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 PassRole acción iam:.

Quiero permitir que personas ajenas a mi AWS cuenta para acceder a mi AWS Service Catalog recursos

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se 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 obtener 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

Third-party los auditores 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 de de .

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 basada en la seguridad y el cumplimiento de la HIPAA: este documento técnico describe cómo las empresas pueden utilizarlo para crear aplicaciones. AWS HIPAA-compliant
- 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 normas.
- AWS Security Hub CSPM— 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 AWS 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.
- Paquetes de cifrado con perfecto secreto directo (PFS), como el DHE (Ephemeral) o el ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Con él 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 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 gestionar carteras, productos y restricciones desde una consola de 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 Identity and Access Management en AWS Service Catalog.

Tareas

- Administración de carteras
- Administración de productos
- Uso de AWS Service Catalog restricciones
- AWS Service Catalog Acciones de servicio
- Uso 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
- Cómo 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.

Cómo 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 eres nuevo en ella, verás la página AWS Service Catalog de inicio. AWS Service Catalog Elija Get started para crear una cartera. Siga las instrucciones para crear la primera cartera y, a continuación, vaya a la página Carteras.

Mientras lo usa AWS Service Catalog, puede volver a la página Portafolios en cualquier momento; elija Service Catalog en la barra de navegación y, a continuación, elija Portafolios.

Ver los detalles de la cartera

En la consola AWS Service Catalog de administración, la página de detalles de la cartera muestra la configuración de una cartera. Utilice esta página para gestionar los productos de la cartera, conceder a los usuarios el acceso a los productos TagOptions y aplicar las 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. Selecciona Crear. AWS Service Catalog crea la cartera y muestra los detalles de la cartera.

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 AWS Service Catalog producto, puede cargar una CloudFormation plantilla o un archivo de configuración de Terraform. La CloudFormation plantilla se almacena en un depósito de Amazon Simple Storage Service (Amazon S3) y el nombre del depósito comienza por "cf-templates -». También debe tener permiso para recuperar objetos de buckets adicionales al aprovisionar un producto. Para obtener más información, consulte Crear productos.

Cómo añadir un nuevo producto

Los productos nuevos se agregan directamente desde la página Detalles de la cartera. Cuando crees un producto desde esta página, lo AWS Service Catalog añades a la cartera actualmente seleccionada.

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 publicador 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: en el caso de CloudFormation los productos, elija su propio archivo de CloudFormation plantilla, una plantilla de una unidad local o una URL que apunte a una plantilla almacenada en Amazon S3, a una plantilla ARN de CloudFormation Stack existente o a un archivo de plantilla almacenado en un repositorio externo.

     Para los productos de 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 (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 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): la 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 del 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 Carteras, la página Detalles de la 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 Detalles de la cartera.
2. Amplíe la sección 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 sobre los tipos de restricciones que AWS Service Catalog admite, consulteUso de AWS Service Catalog restricciones.

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: permite asignar una función de IAM al producto que se utiliza para aprovisionar los AWS recursos. Para obtener más información, consulte AWS Service Catalog Restricciones de lanzamiento.

   Notificación: le permite transmitir notificaciones de productos a un tema de Amazon SNS. Para obtener más información, consulte AWS Service Catalog Restricciones de notificación.

   Plantilla: permite limitar las opciones que los usuarios finales tienen a su disposición cuando lanzan un producto. Una plantilla es un archivo de texto con formato JSON que contiene una o varias reglas. Las reglas se añaden a la CloudFormation plantilla utilizada por el producto. 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 CloudFormation StackSets. Para obtener más información, consulte AWS Service Catalog Restricciones del conjunto de pilas.

   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. Inicie sesión en la consola de administración Consola de administración de AWS y AWS Service Catalog ábrala en https://console.aws.amazon.com/catalog/.
2. Elija Carteras y seleccione una cartera.
3. En la página 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 concederles 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 Usuarios y grupos de IAM en la Guía del usuario de IAM.

Además de acceder a una cartera, los usuarios también deben tener acceso a la consola de usuario AWS Service Catalog final. Para conceder acceso a la consola, puede aplicar los permisos de IAM. Para obtener más información, consulte Identity and Access Management 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. Elija una cartera a la que desee conceder acceso a grupos, roles o usuarios. AWS Service Catalog dirige a la página de detalles del portafolio.
4. En la página Detalles de la cartera, elija la pestaña 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 Detalles de la cartera, elija un grupo, rol o nombre de usuario.
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.

Account-to-account compartir

Para completar estos pasos, debe obtener el ID de cuenta de la AWS cuenta de destino. Puedes encontrar el ID en la página Mi cuenta Consola de administración de AWS de la cuenta de destino.

Para compartir un portafolio con una AWS cuenta

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 el ID de cuenta, introduzca el ID de AWS cuenta de la cuenta con la que está compartiendo. (Opcional) Selecciona TagOption Compartir. A continuación, elija Compartir.
4. Envía la URL al AWS Service Catalog administrador 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 el AWS Service Catalog administrador de otra AWS cuenta comparte una cartera con usted, impórtela a su cuenta para que pueda distribuir sus productos a sus usuarios finales.

No es necesario importar una cartera si la cartera se ha compartido a través de ella AWS Organizations.

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

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

Compartir con AWS Organizations

Puede compartir AWS Service Catalog carteras utilizando AWS Organizations.

En primer lugar, debe decidir si está compartiendo desde la cuenta de administración o desde una cuenta de administrador delegado. Si no desea compartir desde su cuenta de administración, 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 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.)

Cómo 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 un portafolio con una organización mediante la estructura organizativa

1. Abra la AWS Service Catalog consola 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 la organización, una unidad organizativa (OU) principal, una OU secundaria o una AWS cuenta 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 AWS cuentas para ver una lista de todas las AWS cuentas de su organización.

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

1. Abre la AWS Service Catalog consola 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.

   Introduce el ID del nodo organizativo que has seleccionado, que encontrarás en la AWS Organizations consola en https://console.aws.amazon.com/organizations/.

Compartir desde una cuenta de administrador delegado

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

Un administrador delegado puede compartir AWS Service Catalog los recursos de su organización del mismo modo que lo hace una cuenta de administración. Están autorizados para 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 administración. 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 “Cómo 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 traslada una cuenta dentro de su organización, es posible que cambien AWS Service Catalog las carteras compartidas con la cuenta.

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, necesitas el ID de AWS cuenta del consumidor. Busca el ID de la AWS cuenta en Mi cuenta en la consola.

> **Note**
>
> Si a TagOption tiene un valor único, lo AWS aplica 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. Elige compartir con otra AWS cuenta u organización.

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 principales ya existen. Si existen, asocia AWS Service Catalog automáticamente los directores de IAM coincidentes a la cartera compartida para conceder el acceso a los usuarios.

> **Note**
>
> Al asociar una entidad principal a una cartera, puede producirse una posible escalada de privilegios cuando esa cartera se comparte con otras cuentas. En el caso de un usuario de una cuenta receptora que no sea AWS Service Catalog administrador, pero que aún

pueda crear directores (usuarios/funciones), ese usuario puede crear un director de IAM que coincida con la asociación de nombres principales de la cartera. Aunque es posible que este usuario no sepa a qué nombres principales están asociados AWS Service Catalog, es posible que pueda adivinar quién es el usuario. Si esta posible ruta de escalación es motivo de preocupación, se AWS Service Catalog recomienda utilizarla `PrincipalType` como`IAM`. Con esta configuración, el `PrincipalARN` ya debe existir en la cuenta del destinatario antes de poder asociarla.

Al añadir o eliminar nombres principales en la cuenta principal, esos cambios se aplican AWS Service Catalog automáticamente 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 del nombre principal solo está disponible para AWS Organizations.

Cómo 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.

Cómo 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 Activar para iniciar el uso compartido principal. AWS Service Catalog a continuación, comparte los nombres principales 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 los principales (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`**.

Cómo compartir e importar carteras

Para que tus AWS Service Catalog productos estén disponibles para usuarios que no pertenecen a la tuya Cuentas de AWS, como los usuarios que pertenecen a otras organizaciones o a otros miembros Cuentas de AWS de tu organización, compartes tus carteras con ellos. Puede compartir de varias formas, como account-to-account compartir, compartir de forma organizativa e implementar catálogos mediante conjuntos apilados.

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.

Si quieres usar conjuntos apilados para desplegar una copia de tu catálogo, consulta Cómo configurar un catálogo de productos estándar AWS Service Catalog de la empresa en varias regiones y múltiples cuentas.

Al compartir una cartera o AWS Organizations 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. account-to-account

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, el administrador con el que compartes una cartera, no puede cambiar los productos ni las restricciones, pero puede añadir acceso AWS Identity and Access Management (IAM) para los usuarios finales. Para obtener más información, consulte Conceder acceso a los usuarios.

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

- Agregue usuarios, grupos y funciones a la cartera importada.

- Al añadir productos de la cartera importada a una cartera local, una cartera independiente que el administrador del destinatario crea y que pertenece a su AWS cuenta. A continuación, el administrador destinatario agrega los usuarios, grupos y roles a la cartera local. Cualquier restricción que se haya aplicado a los productos de la cartera compartida también está presente 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 aprovisionado 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 se AWS Service Catalog utiliza para aprovisionar AWS recursos (como EC2 instancias de Amazon 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 AWS Service Catalog Restricciones de lanzamiento. La AWS cuenta propietaria de la función de lanzamiento aprovisiona los AWS recursos y esta cuenta incurre en los cargos por el uso de esos recursos. Para obtener más información, consulte AWS Service Catalog Precios.

En este vídeo se muestra cómo compartir carteras entre cuentas en. AWS Service Catalog

Comparta (https://www.youtube.com/embed/BVSohYOppjk% 22% 3EShare) las carteras entre las cuentas de. 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 esa 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 sincroniz ados 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 restricciones de lanzamiento a un producto compartid	En una cartera local, el administrador puede aplicar restricci ones de lanzamien to que afecten al lanzamiento local del producto.	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
	o o las elimina de él, el cambio se propaga a todas las instancia s importadas del producto. Si el administrador destinatario agrega un producto importado a una cartera local, la restricci ón de lanzamien to importada no se aplica a la cartera compartida.		

Elemento de la cartera compartida	Relación con la cartera importada	El administrador destinatario puede	El administrador destinatario no puede
Restricciones de plantilla	Se heredan. 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. Si el administrador destinatario agrega un producto importado a una cartera local, las restricciones de plantilla importadas no se trasladan a la cartera local.	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 que están presentes en la cuenta de AWS del administrador.	No se usa.

Administración de productos

Puede crear productos, actualizar productos creando una nueva versión basada en una plantilla actualizada y agrupar los productos en carteras para distribuírselos 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.

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 desde la página de lista de productos de la AWS Service Catalog consola de administración.

Cómo 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 desde la página de productos de la AWS Service Catalog consola de administración.

> **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 Primeros pasos con un producto de Terraform.

Para crear un AWS Service Catalog producto nuevo

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 los CloudFormation tipos de productos Terraform Cloud y External (compatible con 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 buscar los que necesitan.
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.
     - Use un archivo de plantilla local: cargue una CloudFormation plantilla o un archivo de configuración tar.gz de Terraform desde una unidad local.
     - Usar una URL de Amazon S3: especifique una URL que apunte a una plantilla de 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, el de GitHub Enterprise o el de Bitbucket. AWS Service Catalog te permite sincronizar los productos con los archivos de plantilla. En el caso de los productos de 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.
   - Nombre de la versión (opcional): 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 otras versiones.
- Guía: se gestiona en la pestaña de versiones de la página 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): la 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 del enlace Soporte.

6. Administrar etiquetas (opcional): además de usar etiquetas para categorizar sus recursos, también puede usarlas para autentificar 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 el tutorial: Cómo crear una canalización que se implemente en. AWS Service Catalog

Puede definir las propiedades de los parámetros en su plantilla 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 CloudFormation .

Resolución 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 depósito que comienza por "cf-templates-*" y donde AWS Service Catalog se almacena la plantilla de artefactos de aprovisionamiento.
- El depósito interno que comienza por "sc-*" y donde se almacenan los metadatos. AWS Service Catalog 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 (incluso las carteras compartidas) reciben automáticamente la nueva versión.

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 le dirigirá a la página Añadir ***name-of-product*** a la cartera.
3. Elija una cartera y, a continuación, haga clic en la 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 numerosos productos que sean una combinación de tipos de productos CloudFormation y los 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 (CloudFormation o Teraform). Por ejemplo, si actualiza un CloudFormation producto, no puede reemplazar la CloudFormation plantilla existente por un archivo de configuración tar.gz de Terraform. Debe actualizar el archivo de CloudFormation plantilla existente con un archivo de CloudFormation plantilla nuevo.

Los usuarios finales que actualmente están ejecutando un producto aprovisionado de la versión anterior del producto pueden actualizarlo para obtener la versión más reciente. Cuando está disponible una nueva versión de un producto, los usuarios pueden utilizar el comando Actualizar

productos aprovisionados de las páginas Lista de productos aprovisionados o Detalles de productos aprovisionados.

Antes de crear una nueva versión de un producto, le AWS Service Catalog recomienda que pruebe las actualizaciones del producto en CloudFormation o en el motor Terraform para asegurarse de que funcionan correctamente.

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 Detalles del producto.
3. En la página 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.

     Utilice un archivo de plantilla local: cargue una CloudFormation plantilla o un archivo de configuración tar.gz de Terraform desde una unidad local.

     Usar una URL de Amazon S3: especifique una URL que apunte a una plantilla de 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, el de GitHub Enterprise o el de Bitbucket. AWS Service Catalog te permite sincronizar productos con archivos de plantilla. En el caso de los productos de 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 el tutorial: Cómo crear una canalización que se implemente en. 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 hace referencia a los productos con este tipo de conexión de plantillas como Git-syncedproductos. 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

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 Catalog`AWSServiceCatalogAdminFullAccess` gestionada al habilitar los productos sincronizados en el repositorio.

JSON

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

Creación de una conexión de cuenta

Antes de sincronizar un archivo de plantilla con un AWS Service Catalog producto, debes crear y autorizar una conexión única de cuenta a cuenta. 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 la SLR, consulte las funciones deService-linked . AWS Service Catalog

Para crear un producto nuevo Git-synced

1. En el panel de navegación izquierdo, elija Lista de productos y, a continuación, Crear un producto.
2. Introducción de los detalles del producto.
3. En Detalles de la versión, elija Especificar su repositorio de código mediante un AWS CodeStar proveedor y, a continuación, elija 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 de 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 Git-synced productos

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 conexión de AWS CodeStar 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 ya existente AWS Service Catalog producto 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.

Visualización de las conexiones de Git-synced productos

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 Consola de administración de AWS

1. En el menú de navegación izquierdo, elija Lista de productos.
2. Seleccione el producto de la lista.
3. En la página Producto, vaya a la sección 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 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
```

Actualización de las conexiones Git-synced de los productos

Puede actualizar las conexiones de cuentas y Git-synced los productos existentes 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 Git-synced productos.

Para actualizar los productos existentes a Git-synced productos

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 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. Seleccione Save changes (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 puede utilizar la AWS Service Catalog consola o AWS CLI el

- 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 de AWS Service Catalog previamente conectado.

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

1. En el panel de navegación izquierdo de la AWS Service Catalog consola, selecciona Lista de productos y, a continuación, selecciona 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. Seleccione Save changes (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 las conexiones Git-synced de los productos

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 Git-synced producto mediante el AWS Service Catalog consola

1. En el Consola de administración de AWS, selecciona Lista de productos en el panel de navegación izquierdo.
2. Seleccione un producto de la lista.
3. En la página Producto, vaya a la sección Detalles de la fuente del producto.
4. Seleccione Desconectar.
5. Confirme la acción y, a continuación, seleccione Desconectar.

Para desconectar un Git-synced producto mediante AWS CLI

Desde AWS CLI, ejecute el `$ aws servicecatalog update-product` comando. 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 Git-synced producto con 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 Git-synced

AWS Service Catalog admite los Git-synced productos tal y Regiones de AWS como se indica en la siguiente tabla.

Región de AWS nombre	Región de AWS identidad	Support para Git-synced productos
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	No
Asia-Pacífico (Hong Kong)	ap-east-1	No
Asia-Pacífico (Yakarta)	ap-southeast-3	No
Asia-Pacífico (Nueva Zelanda)	ap-southeast-6	No
Asia-Pacífico (Mumbai)	ap-south-1	Sí
Asia-Pacífico (Osaka)	ap-northeast-3	No
Asia-Pacífico (Seúl)	ap-northeast-2	Sí

Región de AWS nombre	Región de AWS identidad	Support para Git-synced productos
Asia-Pacífico (Singapur)	ap-southeast-1	Sí
Asia-Pacífico (Sídney)	ap-southeast-2	Sí
Asia-Pacífico (Tokio)	ap-northeast-1	Sí
Canadá (centro)	ca-central-1	Sí
Oeste de Canadá (Calgary)	ca-west-1	No
Europa (Fráncfort)	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 (US-East)	us-gov-east-1	No
AWS GovCloud (US-West)	us-gov-west-1	No

Eliminación de productos

Al eliminar un producto, se AWS Service Catalog eliminan todas las versiones del producto de todas las carteras que contienen el producto.

AWS Service Catalog permite eliminar un producto mediante la AWS Service Catalog consola o AWS CLI. Para eliminar correctamente un producto, primero debe disociar todos los recursos asociados al

producto. Entre los ejemplos de asociaciones de recursos de productos se incluyen las asociaciones de carteras TagOptions, los presupuestos y las acciones de servicio.

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

Para eliminar un producto mediante la AWS Service Catalog consola

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, consulta la tabla de asociaciones, que muestra todos los recursos asociados al producto. AWS Service Catalog intenta desasociar 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 el AWS CLI
- Resolver las disociaciones de recursos fallidas al eliminar un producto

Eliminar productos mediante el AWS CLI

AWS Service Catalog le permite usar AWS Command Line Interface(AWS CLI) para eliminar productos de su cartera. AWS CLI Se trata de una herramienta de código abierto que permite interactuar con los AWS servicios mediante comandos de la consola de la línea de comandos. La función AWS Service Catalog force-delete requiere un AWS CLI alias, que es un atajo que se puede crear AWS CLI para abreviar los comandos o scripts que se utilizan con frecuencia.

Requisitos previos

- Instalar y configurar la AWS CLI. Para obtener más información, consulte Instalación o actualización de la versión más reciente de la AWS CLI y Configuración básica. Utilice una AWS CLI versión mínima de 1.11.24 o 2.0.0.
- 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 AWS CLI alias para agrupar las llamadas a la `Disassociation` API, 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 AWS CLI alias para eliminar AWS Service Catalog productos

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

Cree un **`alias`** archivo en la carpeta AWS CLI de configuración

1. En la AWS CLI consola, navegue hasta 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 sin extensión con el nombre `alias`. 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 AWS CLI consola, vaya a la carpeta AWS CLI de configuración y abra el `alias` archivo.
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.

Utilice la ventana del terminal para añadir el force-delete-product alias al **`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 AWS Service Catalog productos, consulta los siguientes recursos:

- Creación y uso de AWS CLI alias en la guía del usuario AWS Command Line Interface (CLI).
- AWS CLI repositorio de alias (repositorio git).
- Eliminación de productos AWS Service Catalog.
- AWS re: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 pudo 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 cómo desasociar los recursos de productos que actualmente no tiene permiso para desvincular.

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 CloudFormation plantilla, 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 aprovisionado 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 AWS Service Catalog consola, selecciona 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 AWS Service Catalog restricciones

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

- AWS Service Catalog Restricciones de lanzamiento
- AWS Service Catalog Restricciones de notificación
- AWS Service Catalog Restricciones de actualización de etiquetas
- AWS Service Catalog Restricciones del conjunto de pilas
- AWS Service Catalog Restricciones de plantilla

AWS Service Catalog Restricciones de lanzamiento

Una restricción de lanzamiento especifica la función AWS Identity and Access Management (IAM) que AWS Service Catalog asume un usuario final cuando lanza, actualiza o cancela un producto. Una función de IAM es un conjunto de permisos que un usuario o AWS servicio puede asumir temporalmente para utilizar los servicios. AWS Para obtener un ejemplo introductorio, consulte:

- CloudFormation tipo de producto: Paso 6: agregar una restricción de lanzamiento para asignar un rol de IAM.
- Tipo de producto de 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 CloudFormation los AWS servicios que utilizan los productos 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 Identity and Access Management 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 política administrada `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess` CloudFormation
- Los servicios de la AWS CloudFormation plantilla del producto
- Acceso de lectura a la AWS CloudFormation plantilla en un bucket de Amazon S3 propiedad del servicio.

Para productos de 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 (supuesto AWS Service Catalog para crear grupos de recursos y asignar etiquetas)

La política de confianza del rol de IAM debe AWS Service Catalog permitir asumir el rol. En el siguiente procedimiento, la política de confianza se establecerá automáticamente al seleccionar AWS Service Catalog el tipo de función. Si no utiliza la consola, consulte la sección Creación de políticas de confianza para AWS los servicios que asumen funciones en Cómo utilizar las políticas de confianza con las funciones 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 los usuarios finales de AWS Service Catalog .

> **Note**
>
> Para ver los productos y recursos de Cloudformation aprovisionados en la AWS Service Catalog consola, los usuarios finales necesitan CloudFormation acceso de lectura. Para ver los productos y recursos aprovisionados 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 Paso 5: crear roles de lanzamiento en Primeros pasos 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 Roles de servicio de AWS junto a AWS Service Catalog elija 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 permisos 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 AWS Service Catalog que hay que asumir el rol cuando un usuario final lanza 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 y si una cuenta utiliza 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 aquellos APIs 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, el AWS Service Catalog usuario final pertenece a la cuenta 1111. Cuando el administrador de 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.

Los siguientes elementos AWS Service Catalog APIs están protegidos por la protección de Confused Deputy:

- `LaunchConstraint`

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

La `sourceArn` protección AWS Service Catalog solo admite plantillas ARNs, como «`arn:<aws-partition>:servicecatalog:<region>:<accountId>:`». No admite un recurso ARNs específico.

Cómo verificar la restricción de lanzamiento

Para comprobar que AWS Service Catalog utiliza la función de lanzamiento del producto y lo aprovisiona correctamente, inicie el producto desde la AWS Service Catalog consola. Para probar una restricción antes de distribuírsela 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 AWS Service Catalog consola, elija Service Catalog, End user.
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.

AWS Service Catalog Restricciones de notificación

> **Note**
>
> AWS Service Catalog no admite las 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 Amazon SNS en https://console.aws.amazon.com/sns/ la versión 3/home.
2. Seleccione Crear tema.
3. Escriba el nombre del tema y, a continuación, elija Create topic.
4. Seleccione Crear subscripción.
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 como Notificación. Elija Continuar.
5. Elija Choose a topic from your account y seleccione el tema de SNS que ha creado en Topic Name.
6. Seleccione Enviar.

AWS Service Catalog Restricciones de actualización de etiquetas

> **Note**
>
> AWS Service Catalog no admite las restricciones de actualización de etiquetas para los productos de código abierto de Terraform.

Con las restricciones de actualización de etiquetas, AWS Service Catalog los administradores pueden permitir o impedir que los usuarios finales actualicen las etiquetas de los recursos asociados a un producto aprovisionado. Si se autoriza la actualización de etiquetas, se aplicarán nuevas etiquetas asociadas a la cartera o al producto a los recursos aprovisionados durante la actualización de un producto aprovisionado.

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. Seleccione Enviar.

AWS Service Catalog Restricciones del conjunto de pilas

> **Note**
>
> - AWS Service Catalog no admite las restricciones de conjuntos de pilas para los productos de código abierto de Terraform.
> - AutoTags actualmente no son compatibles con CloudFormation StackSets.

Una restricción de conjunto de pilas le permite configurar las opciones de despliegue de productos mediante 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.

AWS Service Catalog Restricciones de plantilla

> **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. Aplicas restricciones de plantilla a un producto de una AWS Service Catalog cartera. Una cartera debe contener uno o varios productos para que sea posible definir restricciones de plantilla.

Una restricción de plantilla consiste en una o más reglas que limitan los valores permitidos para los parámetros que se definen en la plantilla subyacente CloudFormation del producto. Los parámetros de una plantilla de CloudFormation definen el conjunto de valores que los usuarios pueden especificar al crear una pila. Por ejemplo, un parámetro podría definir los distintos tipos de instancias entre los que los usuarios pueden elegir al lanzar una pila que incluye EC2 instancias.

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 la plantilla incluyen tipos de EC2 instancias que son demasiado grandes para los usuarios que deberían usar solo tipos de instancias pequeños (como `t2.micro` `ot2.small`), puedes añadir una restricción de plantilla para limitar los tipos de instancias que pueden elegir los usuarios finales. Para obtener más información sobre los parámetros CloudFormation de la plantilla, consulta Parámetros en la Guía del CloudFormation usuario.

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.

Las reglas de restricción de plantillas se definen mediante un editor de reglas o escribiéndolas como texto JSON en la consola de AWS Service Catalog administración. Para obtener más información sobre las reglas, su sintaxis y ejemplos, consulte Reglas de restricciones de plantilla.

Para probar una restricción antes de distribuírsela 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 Carteras, 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 creador de reglas.

   - Para editar el código JSON de la regla, elija la pestaña Editor de texto de restricción. En esta pestaña se proporcionan varios ejemplos para ayudarle a comenzar.

     Para crear las reglas mediante una interfaz de creador de reglas, elija la pestaña Creador de reglas. 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 en una AWS Service Catalog cartera describen cuándo los usuarios finales pueden utilizar la plantilla y qué valores pueden especificar para los parámetros que se declaran en la CloudFormation plantilla utilizada para crear el producto que están intentando utilizar. Las reglas son útiles para impedir que los usuarios finales especifiquen accidentalmente un valor incorrecto. Por ejemplo, puede añadir una regla para comprobar si los usuarios finales especificaron una subred válida en una VPC determinada o `m1.small` usaron tipos de instancia para entornos de prueba. CloudFormation usa reglas para validar los valores de los parámetros antes de crear los recursos para el 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, CloudFormation evalúa la afirmación para comprobar si el valor del parámetro de subred está en esa VPC antes de crear o actualizar la pila. Si el valor del parámetro no es válido, no podrá crear ni actualizar la pila CloudFormation inmediatamente. Si los usuarios no especifican una VPC, CloudFormation no comprueba 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"
      }
    ]
  }
}
```

AWS Service Catalog Acciones de servicio

> **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 de los usuarios finales y, al mismo tiempo, cumplir con las medidas de cumplimiento 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 AWS Systems Manager documentos proporcionan acceso a acciones predefinidas que implementan las AWS mejores prácticas, como detener y reiniciar Amazon EC2, y también puede definir acciones personalizadas.

En este tutorial se 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 presupone que dispone de todos los permisos de AWS administrador AWS Service Catalog, con los que ya está familiarizado y que ya dispone de un conjunto básico de productos, carteras y usuarios. Si no está familiarizado con este tutorial AWS Service Catalog, complete la configuración y Introducción las tareas antes de seguir con él.

Temas

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 acceder a la función de acciones de AWS Service Catalog servicio y realizar un reinicio de Amazon EC2.

Para actualizar los permisos

1. Abra la consola AWS Identity and Access Management (IAM) en. https://console.aws.amazon.com/iam/
2. En el menú, localice los grupos de usuarios.
3. Elija los grupos que los usuarios finales utilizarán para acceder a AWS Service Catalog los recursos. 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, agregamos permisos a la política existente seleccionando la política personalizada creada para los permisos de AWS Service Catalog aprovisionamiento y rescisión 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:

   JSON

```
{
 "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. Abre 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 Crear acción, elija un AWS Systems Manager documento para definir la acción del servicio. La acción de reinicio de instancia Amazon EC2 está definida por un documento AWS Systems Manager , por lo que mantenemos la opción predeterminada en el menú desplegable Documentos de Amazon.
5. Busque y elija la acción AWS-Restart EC2 Instance.

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 de acciones del servicio, elija AWS-Restart yEC2instance, a continuación, seleccione 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 AWS Service Catalog consola como usuario final.
2. En el AWS Service Catalog panel de control, en el panel de navegación, seleccione la 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, elija la instancia que está aprovisionada.
4. En la página de detalles del producto aprovisionado, selecciona Acciones en la parte superior derecha y, a continuación, selecciona la acción AWS EC2instance-Restart.
5. Confirme que desea ejecutar la acción personalizada. Recibirá una confirmación de que se ha enviado la acción.

Paso 5: Administrar las acciones del servicio con AWS CloudFormation

Puede crear acciones de servicio y sus asociaciones con AWS CloudFormation los recursos. Para obtener más información, consulte lo indicado en la Guía del usuario de AWS CloudFormation :

- AWS::ServiceCatalog::CloudFormationProduct ProvisioningArtifactProperties
- AWS::ServiceCatalog::ServiceActionAsociación

> **Note**
>
> Si gestionas las asociaciones de acciones de servicio con CloudFormation recursos, no añadas ni quites acciones de servicio a través del AWS Command Line Interface o Consola de administración de AWS. Cuando actualiza una pila, se sustituyen todos los cambios en las acciones del servicio que se hayan realizado fuera de CloudFormation .

Paso 6: solucionar problemas

Si la ejecución de la acción de servicio produce un error, puede encontrar el mensaje de error en la sección Outputs del evento de ejecución de acción de servicio en la página Provisioned product. 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 se produjo 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 la función especificada en la definición de la acción de 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 aprovisionado no contiene ningún recurso que coincida con el tipo de destino especificado en el documento SSM, como AWS: :EC2: :Instance. Compruebe el producto aprovisionado 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 SSM 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 la función especificada.

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 AWS Service Catalog que no está definido en la definición de la acción de servicio. Solo puede utilizar parámetros definidos en la definición de acción del servicio.

El paso falla cuando se trata de una executing/canceling acción. ***Error message.*** 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.

Uso CloudFormation StackSets

> **Note**
>
> AutoTags actualmente no son compatibles con CloudFormation StackSets.

Puedes utilizarlos 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 CloudFormation StackSets.

Diferencias entre conjuntos de pilas e instancias de pila

Un conjunto de pilas te permite crear pilas en AWS cuentas de todas AWS las regiones mediante una sola CloudFormation plantilla.

Una instancia de pila se refiere a una pila en una cuenta de destino de una región de AWS y está asociada a un solo conjunto de pilas.

Para obtener más información, consulte Conceptos de StackSets.

Restricciones de conjunto de pilas

En AWS Service Catalog, puede usar las restricciones de los conjuntos de pilas para configurar las opciones de implementación del producto.

AWS Service Catalog admite las restricciones de conjuntos de productos en dos categorías AWS GovCloud (US) Regions: AWS GovCloud (EE. UU., oeste) y AWS GovCloud (EE. UU., este).

Para obtener más información, consulte Restricciones de conjuntos de pilas de AWS Service Catalog.

Administración de presupuestos

Puedes usar AWS Budgets para hacer un seguimiento interno de los costos y el uso de tus servicios. AWS Service Catalog Puede asociar los presupuestos a AWS Service Catalog productos y carteras.

> **Note**
>
> AWS Service Catalog no admite presupuestos para los productos de código abierto de Terraform.

AWS Los presupuestos le permiten establecer presupuestos personalizados que le avisen cuando sus costos o su uso superen (o se prevea que superen) el importe presupuestado. La información sobre AWS los presupuestos está disponible en. https://aws.amazon.com/aws-cost-management/aws-budgets

Tareas

- Requisitos previos
- Cómo crear un presupuesto
- Asociación de un presupuesto
- Visualización de un presupuesto
- Desasociación de un presupuesto

Requisitos previos

Antes de usar AWS Budgets, debe activar las etiquetas de asignación de costes en la Administración de facturación y costos de AWS consola. Para obtener más información, consulte Activación de etiquetas de asignación de costos definidas por el usuario en la Guía del usuario Administración de facturación y costos de AWS .

> **Note**
>
> Las etiquetas tardan hasta 24 horas en activarse.

También debe permitir el acceso de los usuarios a la Administración de facturación y costos de AWS consola para todos los usuarios o grupos que vayan a utilizar la función Presupuestos. Para ello, cree una nueva política para los usuarios.

Para permitir a los usuarios 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.

   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-1:123456789012:*"
            ]
        }
    ]
```

```
}
```

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 .

Cómo crear un presupuesto

En la AWS Service Catalog consola de administración, las páginas de listas de productos y carteras contienen información sobre los productos y carteras existentes y le permiten tomar medidas al respecto. 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.

   Existen dos tipos de etiquetas: AutoTags y TagOptions. AutoTags identificar 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. AWS Budgets Elija Crear en. 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 eliminas un presupuesto de AWS Budgets, seguirán existiendo asociaciones con AWS Service Catalog productos y carteras. 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 Productos o Carteras 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 Lista de 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 secciones con información detallada 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 de AWS los presupuestos, seguirán existiendo asociaciones con AWS Service Catalog productos y carteras. 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 gestionar 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 los productos aprovisionados como administrador

Para administrar todos los productos aprovisionados de la cuenta, se requieren permisos de acceso `AWSServiceCatalogAdminFullAccess` o de nivel equivalente de IAM para las operaciones de escritura del producto aprovisionado. Para obtener más información, consulte Identity and Access Management 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, incluyendo ejemplos, consulte lo siguiente:
>
> - AWS::ServiceCatalog::CloudFormationProvisionedProduct en la Guía del usuario de AWS CloudFormation .
> - DescribeProvisioningParameters (ProvisioningArtifactOutputKeys) en la Guía AWS Service Catalog para desarrolladores.

Cómo consultar y administrar todos los productos aprovisionados

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

   Si ya ha iniciado sesión en la AWS Service Catalog consola, seleccione Service Catalog y, a continuación, Usuario final.
2. Si es preciso, vaya a la sección Productos aprovisionados.
3. En la sección Productos aprovisionados, 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 aprovisionado

Puede cambiar el propietario de un producto aprovisionado 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 `servicecatalog:UpdateProvisionedProductProperties` permiso de acceso AWS Identity and Access Management (IAM).

Cómo cambiar el propietario de un producto aprovisionado

1. En la AWS Service Catalog consola, selecciona la lista de productos aprovisionados.
2. Localice el producto aprovisionado que desea actualizar, elija los tres puntos que hay junto a él y seleccione Cambiar el propietario del producto aprovisionado.También puede encontrar la opción Change owner (Cambiar propietario) en la página de detalles del producto aprovisionado, 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. Seleccione Enviar. Verá un mensaje de realización correcta cuando se haya actualizado el propietario.

Véase también

- UpdateProvisionedProductProperties

Actualizar plantillas para productos aprovisionados

Puede cambiar la plantilla actual de un producto aprovisionado 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 aprovisionado, 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 aprovisionados. 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.

Cómo actualizar un producto aprovisionado

1. Elija Productos aprovisionados en el menú de navegación de la izquierda.
2. En Productos aprovisionados, seleccione un producto aprovisionado y seleccione Acciones, Actualizar.

   Tenga en cuenta que también puede seleccionar Acciones y Actualizar en la página Detalles del producto aprovisionado.
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 aprovisionado a una plantilla de producto diferente. Esto puede finalizar con los recursos y crear nuevos recursos.

   Puede actualizar un producto aprovisionado 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. Elija 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.

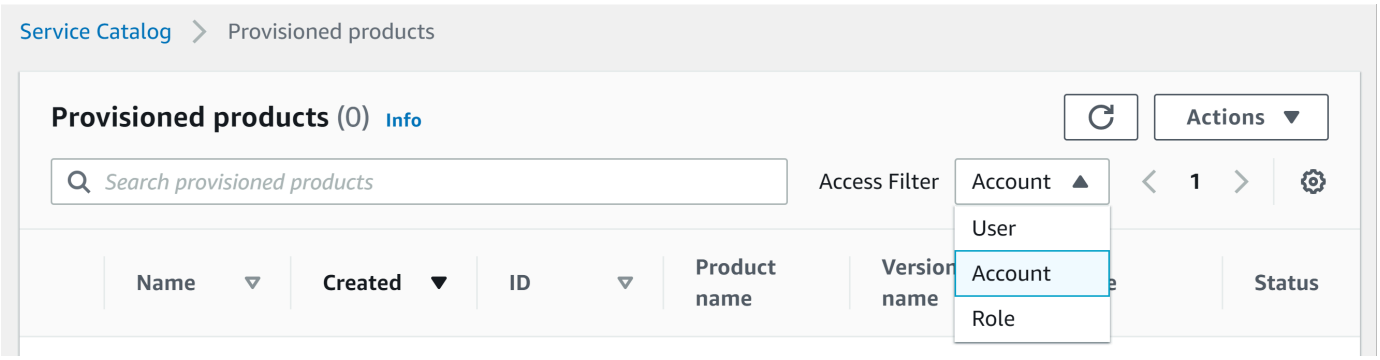
Tutorial: Identificación de la asignación de recursos del usuario

Puede identificar al usuario que aprovisionó un producto y los recursos asociados al producto mediante la AWS Service Catalog consola. Este tutorial le ayuda a adaptar este ejemplo a sus propios productos aprovisionados.

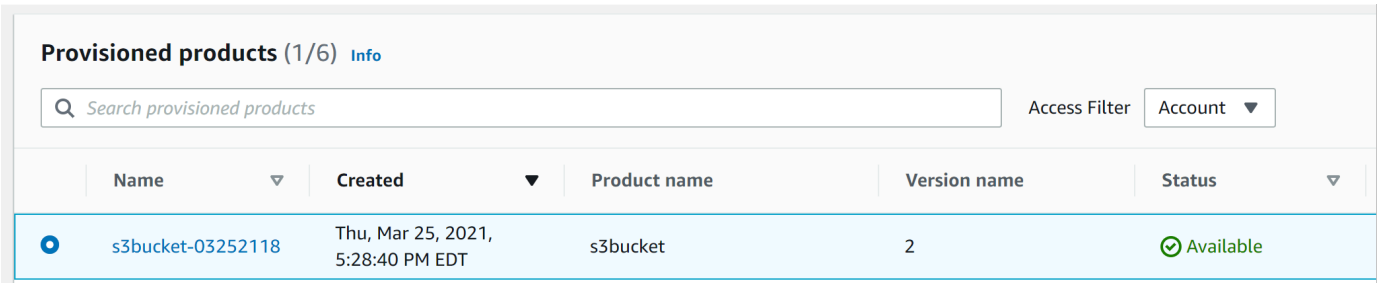
Para administrar todos los productos aprovisionados de la cuenta, se requiere acceso `AWSServiceCatalogAdminFullAccess` o de nivel equivalente a las operaciones de escritura del producto aprovisionado. Para obtener más información, consulte Administración de identidades y accesos en la Guía del administrador de AWS Service Catalog .

Cómo identificar al usuario que ha aprovisionado un producto y los recursos asociados

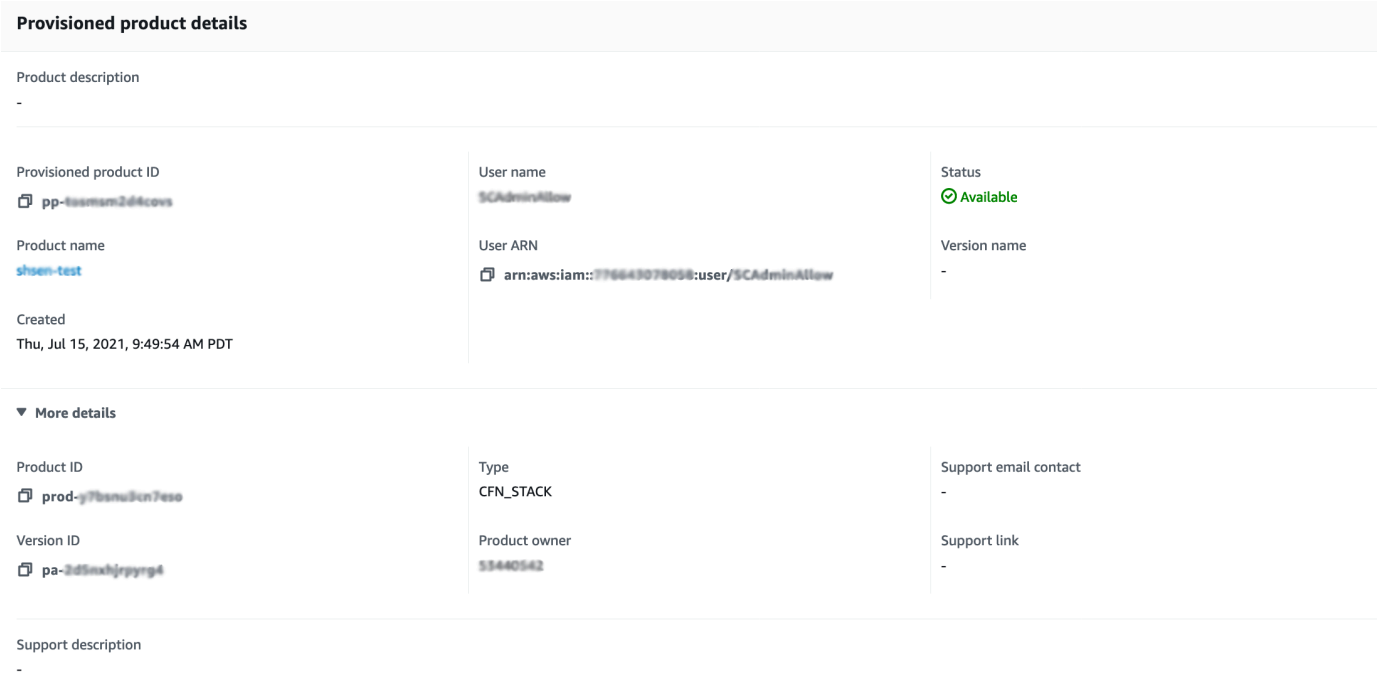
1. Abra https://console.aws.amazon.com/servicecatalog.
2. Elija Productos aprovisionados en el menú de navegación de la izquierda.
3. En el menú desplegable del Filtro de acceso, seleccione Cuenta.



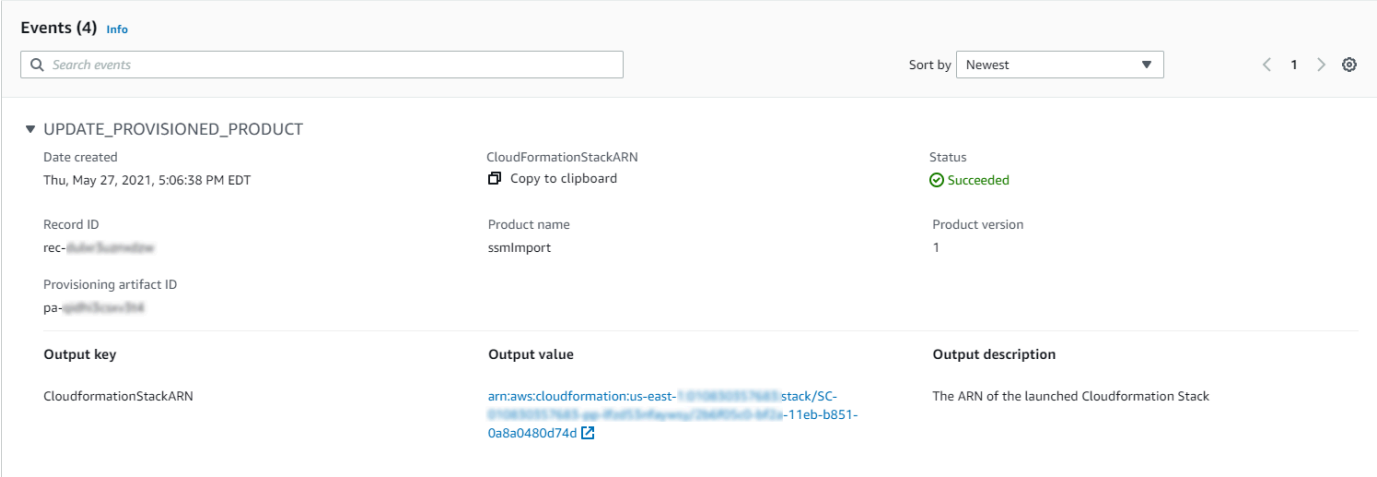
4. En la vista de la Cuenta, seleccione y abra un producto aprovisionado para ver sus detalles.



Puede ver los detalles del producto aprovisionado.



5. Desplácese hacia abajo en la sección Eventos. Tenga en cuenta los valores de `Provisioned product ID` y `CloudformationStackARN`.



6. Utilice el ID de producto aprovisionado para identificar el AWS CloudTrail registro que corresponde a este lanzamiento e identificar al usuario solicitante (normalmente, se introduce 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 `CloudformationStack`ARN valor para identificar CloudFormation los eventos y buscar información sobre los recursos creados. También puede usar la CloudFormation API para obtener esta información. Para obtener más información, consulte Referencia de la API de AWS CloudFormation.

Puede realizar los pasos 1 a 4 mediante la AWS Service Catalog API o el AWS CLI. Para obtener más información, consulte la Guía para desarrolladores de AWS Service Catalog y la Referencia de la línea de comandos de AWS Service Catalog .

Gestión de los errores de estado del producto de 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 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 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 `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 aprovisionado en los nuevos recursos en `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 aprovisionados establecidos a `TAINTED` partir de`ProvisionProduct`. Si el motor de aprovisionamiento de Terraform no devuelve un `ResourceIdentifier` grupo de recursos o AWS Service Catalog no lo crea, el producto aprovisionado se establece en ese `ERROR` estado, lo que le obliga a cancelarlo.

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 `GetStateFile` AWS Lambda plantillas de lanzamiento y a Amazon EC2. AWS Service Catalog los administradores 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, AWS Service Catalog los administradores pueden ver la lista de archivos de estado, pero no pueden leer ni escribir el contenido de los archivos. Solo el motor de aprovisionamiento de Terraform puede leer o escribir el contenido del archivo.

Administrar etiquetas en AWS Service Catalog

AWS Service Catalog proporciona etiquetas para que pueda clasificar sus recursos. Existen dos tipos de etiquetas: AutoTags y TagOptions.

AutoTags son etiquetas que identifican información sobre el origen de un recurso aprovisionado AWS Service Catalog y que se aplican automáticamente AWS Service Catalog a los recursos aprovisionados.

TagOptions son pares clave-valor gestionados y AWS Service Catalog que sirven como plantillas para crear etiquetas. AWS

Temas

AWS Service Catalog AutoTags

> **Note**
>
> AWS Service Catalog no es compatible con AutoTags los productos de código abierto de Terraform.

AutoTags son etiquetas que identifican información sobre el origen de un recurso aprovisionado AWS Service Catalog y que se aplican automáticamente AWS Service Catalog a los recursos aprovisionados.

AutoTags incluyen etiquetas para los identificadores únicos de la cartera, el producto, el usuario, la versión del producto y el producto aprovisionado. Esto proporciona un conjunto de etiquetas que reflejan la AWS Service Catalog estructura 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 no 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 CloudFormation Amazon y Amazon EC2 S3.

> **Note**
>
> AWS Service Catalog no se actualiza AutoTags después de aplicarlo a los recursos AutoTags aprovisionados. Si actualizas el producto aprovisionado a otro producto, artefacto aprovisionado o nueva ruta de lanzamiento, el producto existente AutoTags seguirá mostrando los valores originales.

AutoTag detalles

- aws:servicecatalog:portfolioArn: el ARN de la cartera desde la que se lanzó el producto aprovisionado.
- aws:servicecatalog:productArn: el ARN del producto desde el que se lanzó el producto aprovisionado.
- 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

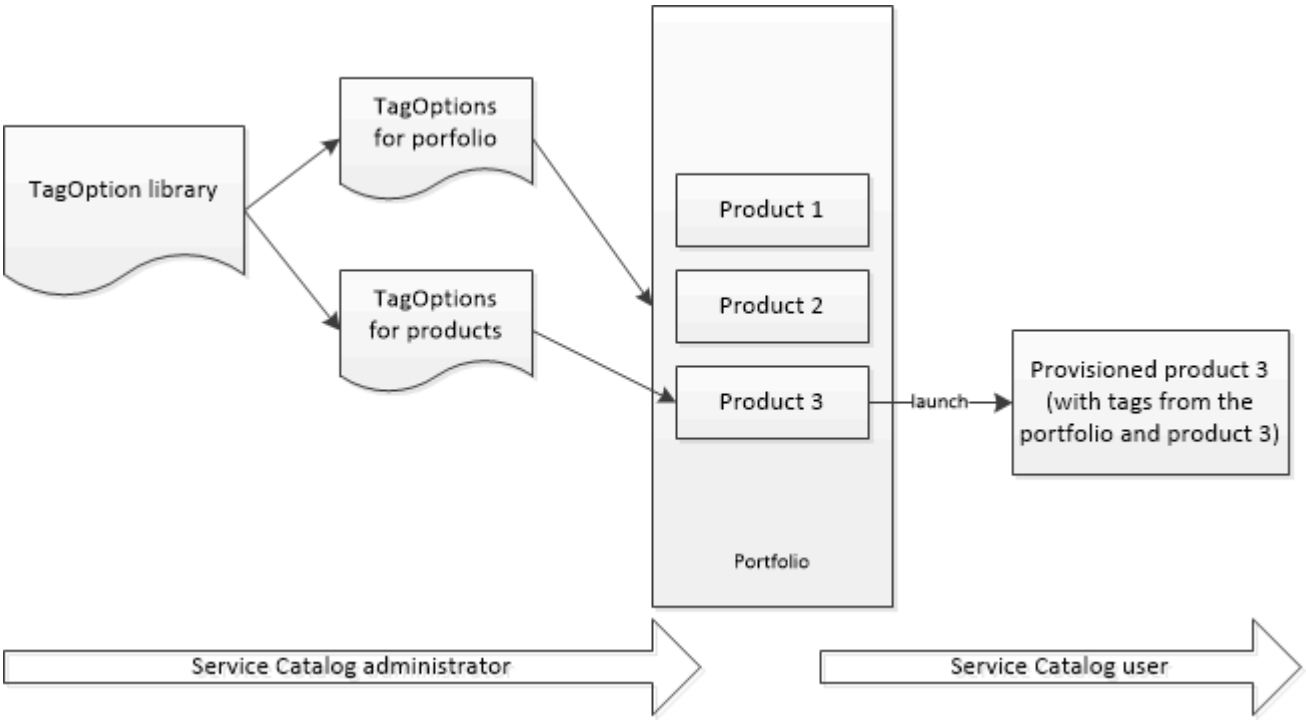
Para permitir a los administradores gestionar fácilmente las etiquetas de los productos aprovisionados, AWS Service Catalog proporciona una TagOption biblioteca. A TagOption es un par clave-valor gestionado en. AWS Service Catalog No es una AWS etiqueta, pero sirve como plantilla para crear una AWS etiqueta basada en. TagOption

AWS Service Catalog no 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
- Etiquetado adecuado de los recursos 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 Service Catalog.

Contenido

- Uso TagOptions con políticas AWS Organizations de etiquetas

Lanzamiento de un producto con TagOptions

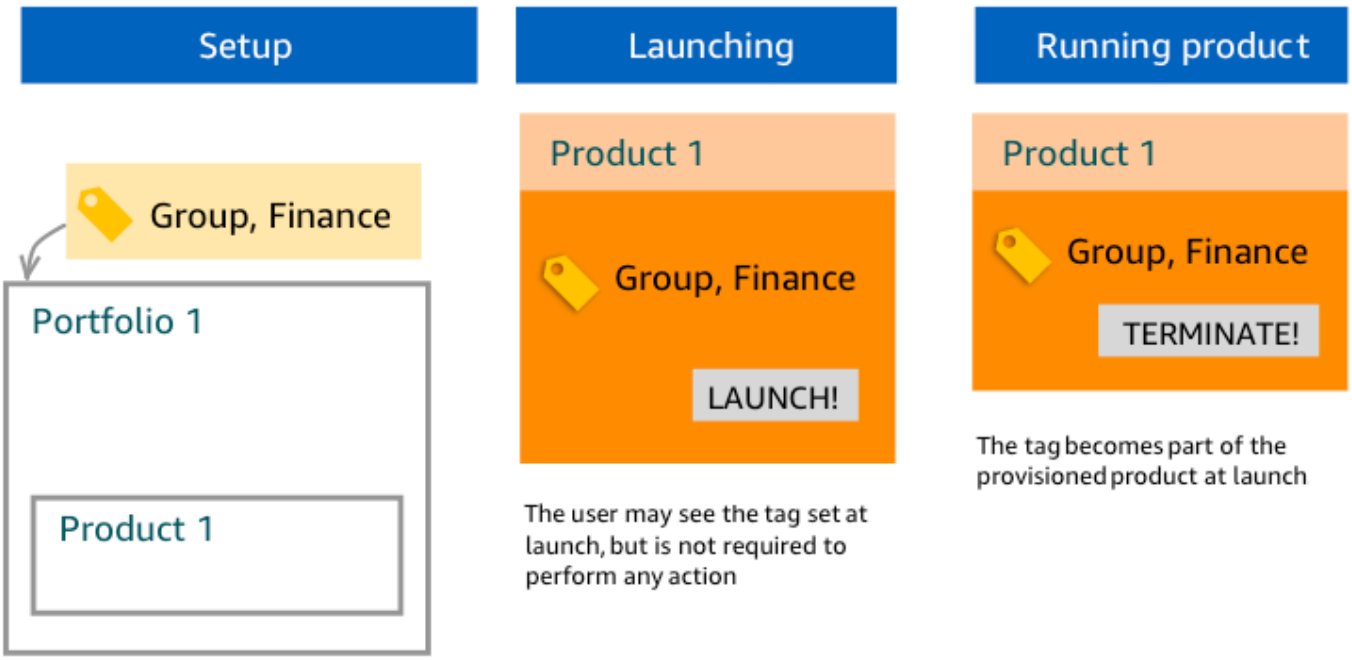
Cuando un usuario lanza un producto que lo tiene TagOptions, AWS Service Catalog realiza las siguientes acciones en tu nombre:

- 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.

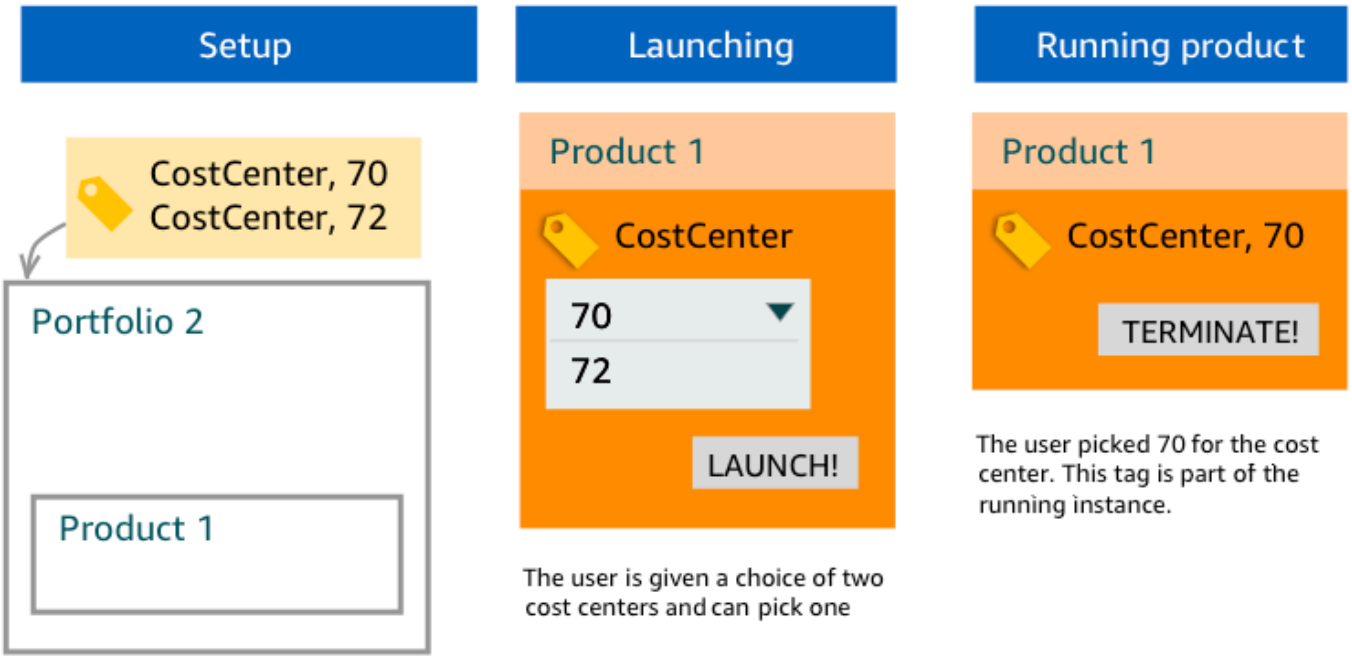
Ejemplo 1: Una TagOption clave única

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:



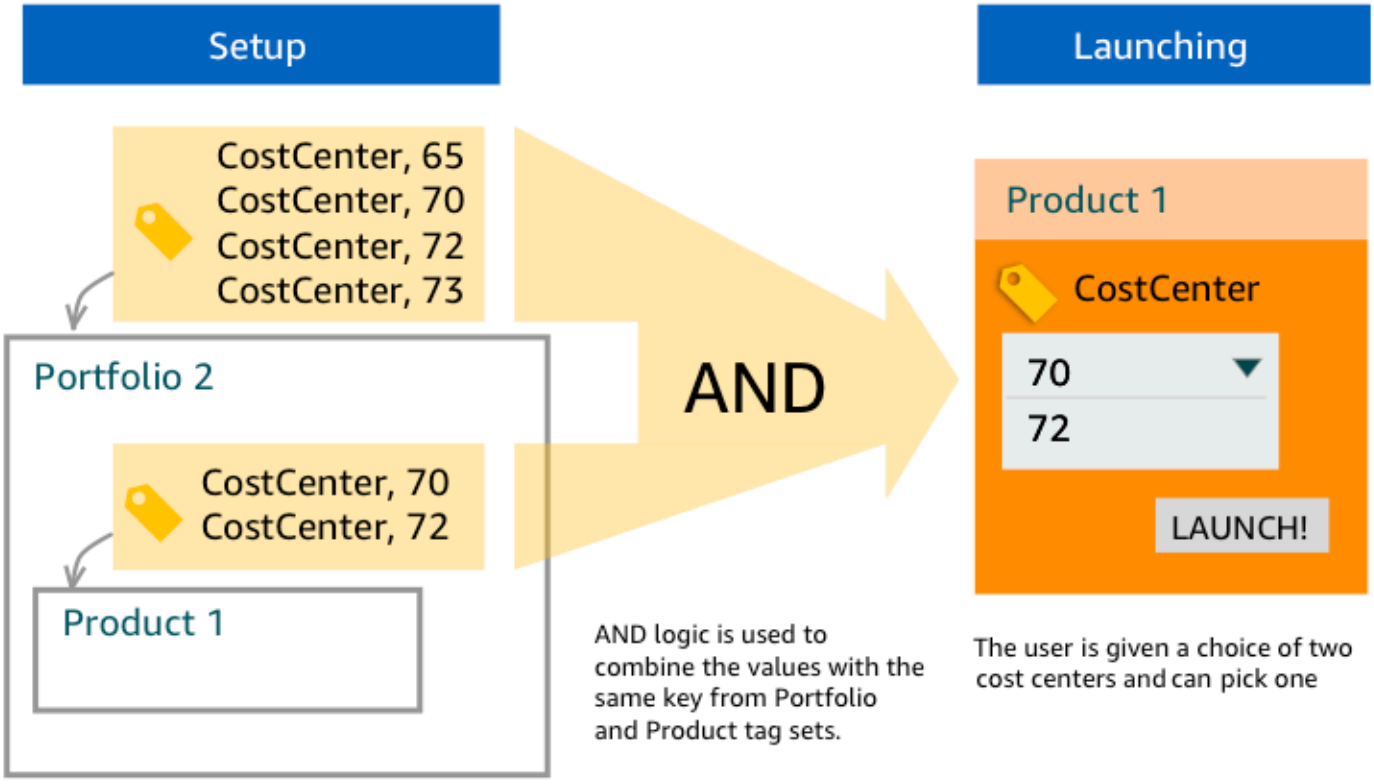
Ejemplo 2: Un conjunto de TagOptions con la misma clave en una cartera

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.



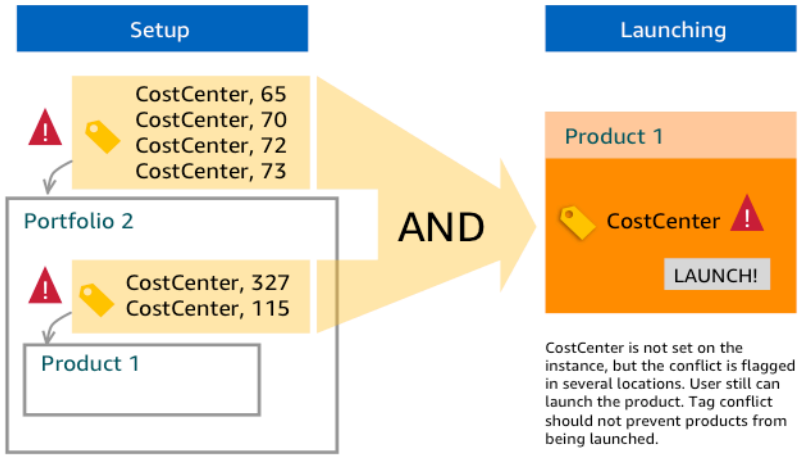
Ejemplo 3: Un conjunto TagOptions con la misma clave tanto en la cartera como en un producto de esa cartera

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 la agregación no encuentra valores para la clave, AWS Service Catalog crea una etiqueta con la misma clave y un valor `desc-tagconflict-`*`portfolioid`*`-`*`productid`*, donde *`portfolioid`* y *`productid`* son los ARNs de la cartera y el 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, elija 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, elija TagOptions biblioteca y, a continuación, 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, elija TagOptions biblioteca y, a continuación, 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 AWS Service Catalog consola 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 más TagOptions para asociarlas o desasociarlas con 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, elija 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 para AWS 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 para etiquetar AWS los recursos 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 eliges una opción de cumplimiento, las políticas de etiquetas te 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 Políticas de etiquetas en AWS Organizations.

TagOptions

TagOptions son una función de etiquetado que AWS Service Catalog se aplica a los productos aprovisionados 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 estableces 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 configuras políticas de AWS Organizations etiquetas para las cuentas de tu organización, te 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.

La siguiente tabla proporciona escenarios que describen cómo resolver los problemas de etiquetado que pueden surgir al usar políticas de etiquetas y TagOptions al mismo tiempo.

Escenario	Motivo	Solución
El producto no se puede iniciar debido a que las etiquetas no cumplen con las normas si la política de etiquetas establece su cumplimiento.	Especifica TagOptions con claves y valores lo que no has añadido a la lista permitida de etiquetas compatibles de tu política de etiquetas. Añadir etiquetas personalizadas opcionales que no se ajusten a su política de etiquetas.	Si configuras un esquema de uso de mayúsculas específico 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. 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

Escenario	Motivo	Solución
		de etiqueta y las claves de etiquetas personalizadas opcionales sean coherente s (por ejemplo, todas en minúsculas) con lo que exige su política de etiquetas.
El producto no se puede lanzar debido a que las mayúsculas de las etiquetas no están escritas correctam ente.	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.	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. Además, si no especific as el cumplimiento de las mayúsculas de las claves de etiquetas en tu política de etiquetas, asegúrate de que todas las claves de TagOption s etiquetas AWS Service Catalog estén en minúsculas para cumplir con las normas de aplicación. Si utiliza una política de etiquetas que no tiene habilitada la conformidad con el uso de mayúscula s, esa política de etiquetas solo considera que son compatibles todas las claves de etiquetas en minúscula.

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 DescribeProvisioningParameterslas operaciones AWS Service Catalog de DescribeProvisioningArtifactun 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 que se reciben UpdateProvisionedProducty TerminateProvisionedProductse gestionan de forma similar, y cada una tiene una cola y una notificación distintas: APIs

- NotifyProvisionProductEngineWorkflowResult
- NotifyUpdateProvisionedProductEngineWorkflowResult

- NotifyTerminateProvisionedProductEngineWorkflowResult.

Temas

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-spokemodelo 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, para`AWS_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 proporcio na 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 parámetro s que Service Catalog solicita al usuario final al aprovisio nar 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 por defecto 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	booleano	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 ProvisionProductoperación, 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 identifica 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.
provisionedProductName	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, para`AWS_S3`, esta es la URI de Amazon S3.
artefacto/tipo	cadena	Sí	Tipo de artefacto . Valor permitido :`AWS_S3`.
identidad	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
etiquetas	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 UpdateProvisionedProductoperación, 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 a 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 aprovisionado.
provisionedProductName	cadena	Sí	Nombre del producto aprovisionado.

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, para`AWS_S3`, esta es la URI de Amazon S3.
artefacto/tipo	cadena	Sí	Tipo de artefacto . Valor permitido :`AWS_S3`.
identidad	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.
etiquetas	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 NotifyUpdateProvisionedProductEngineWorkflowResultAPI con el objeto de respuesta especificado en la página de detalles de la API.

Terminando

Para la TerminateProvisionedProductoperación, 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 a esta operación. El token debe devolverse a Service Catalog para notificar los resultados de la ejecución.
operación	cadena	Sí	Este campo debe ser `TERMINATE_PROVISION_PRODUCT` para esta operación.
provisionedProductId	cadena	Sí	ID del producto aprovisionado.
provisionedProductName	cadena	Sí	Nombre del producto aprovisionado.
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.
identidad	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 período de dos semanas, para que puedas acceder a la información histórica y obtener una mejor perspectiva del rendimiento de tu servicio. AWS Service Catalog los datos métricos se envían automáticamente CloudWatch en períodos de 1 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.

El monitoreo es una parte importante del mantenimiento de la confiabilidad, la disponibilidad y el rendimiento de AWS Service Catalog sus AWS soluciones. Debe recopilar los datos de supervisión de todas las partes de la AWS solución para poder depurar más fácilmente una falla multipunto en caso de que se produzca. Antes de empezar a monitorizar AWS Service Catalog, debe crear un plan de monitorización 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 supervisión va a utilizar?
- ¿Quién se encargará de realizar las tareas de supervisión?
- ¿Quién debería recibir una notificación cuando surjan problemas?

Herramientas de monitorización

AWS proporciona varias herramientas que puede utilizar para supervisar 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 Amazon EC2 Auto Scaling. 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, consultaAWS 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 período de dos semanas, para que puedas acceder a la información histórica y obtener una mejor perspectiva del rendimiento de tu servicio. AWS Service Catalog los datos métricos se envían automáticamente CloudWatch en períodos de 1 minuto. Para obtener más información al respecto CloudWatch, consulta la Guía del CloudWatch usuario de Amazon.

Temas

- Habilitar CloudWatch las métricas
- Métricas y dimensiones disponibles
- Visualización de métricas 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.

AWS Service Catalog Métricas

El espacio de nombres de `AWS/ServiceCatalog` incluye las siguientes métricas.

Métrica	Description (Descripción)
`ProvisionedProductLaunch`	El número de productos aprovisionados lanzado para un producto determinado y el artefacto de aprovisionamiento en un periodo especific ado. Las dimensiones se publican como registros independientes en CloudWatch los registros. Unidades: `Count` Estadísticas válidas: `Minimum`, `Maximum`, `Sum`, `Average` Dimensiones:`State`,`PPState`,`ProductId` , `ProvisioningArtifactId`
`ProductProvisioningOperation`	El número de operaciones realizadas en el identificador del producto, `provisioningArtifactId` . Las dimensiones se publican como un registro en CloudWatch los registros. Unidades: `Count` Estadísticas válidas: `Minimum`, `Maximum`, `Sum`, `Average` Dimensiones:`State`,`PPState`,`ProductId` , `ProvisioningArtifactId`

Dimensiones de las AWS Service Catalog métricas

AWS Service Catalog envía las siguientes dimensiones a Amazon CloudWatch.

Dimensión	Description (Descripción)
`PPState`	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. Estado válido: DISPONIBLE, DAÑADO, ERROR
`ProductId`	Esta dimensión filtra únicamente los datos solicitad os para el ID de producto identificado. Esto le ayuda a seleccionar un producto exacto desde el que efectuar el lanzamiento.
`ProvisioningArtifactId`	Esta dimensión filtra únicamente los datos solicitados para el ID de artefacto de aprovisionamiento identific ado. Esto le ayuda a seleccionar una versión exacta de productos desde la que efectuar el lanzamiento.
`State`	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. Estado válido: SUCCEEDED, FAILED

Visualización de métricas 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 las métricas en Amazon CloudWatch Console

Visualización de AWS Service Catalog las 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.

Registro de llamadas a la AWS Service Catalog API 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 llamadas desde la AWS Service Catalog consola y llamadas en código a las operaciones de la AWS Service Catalog API. 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. Puedes ver, buscar y descargar los eventos recientes en tu AWS cuenta. Para obtener más información, consulta Cómo ver eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de los eventos de tu AWS cuenta, incluidos los eventos de tu cuenta AWS Service Catalog, crea una ruta. 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. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. 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
- AWS CloudTrail servicios e integraciones compatibles
- Configuración de notificaciones de Amazon SNS para AWS CloudTrail
- Recepción de archivos de AWS CloudTrail registro de varias regiones y recepción de archivos de AWS CloudTrail registro 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 le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Descripción de las entradas de los archivos de AWS Service Catalog registro

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 botocore/1.17.63",
    "requestParameters": {
        "name": "hawTestCT",
        "clientToken": "6f36d650-a086-47cf-810a-fbfab2f8ad33"
    },
    "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.

Cómo 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 Save.

Para obtener una lista de las regiones en las que se AWS Service Catalog admite la promoción de marcas de consolas, consulta la Región de AWS sección sobre compatibilidad con la marca de consolas.

Región de AWS compatibilidad con las preferencias de marca de la consola

AWS Service Catalog admite las preferencias de marca de la consola que Regiones de AWS se muestran en la tabla siguiente.

Región de AWS nombre	Región de AWS identidad	
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	
Europa (Londres)	eu-west-2	

Región de AWS nombre	Región de AWS identidad
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

AWS Service Catalog Descripción general de la API

Ventajas del uso de la API de Service Catalog

La AWS Service Catalog API proporciona un control programático sobre todas las acciones del usuario final como alternativa al uso de. Consola de administración de AWS Al utilizar la API, puede hacer lo siguiente:

- Escribe tus propias interfaces y aplicaciones personalizadas
- Obtenga un control detallado de las operaciones de aprovisionamiento de productos para los usuarios finales
- Integre el aprovisionamiento de recursos en sus procesos de organización
- Acceda a una ubicación central que aloje sus aplicaciones con sus recursos

Acceda al catálogo de servicios

Para crear aplicaciones mediante API de idiomas específicos, utilice las bibliotecas, el código de muestra, los tutoriales y otros recursos para desarrolladores de software. Estas bibliotecas proporcionan funciones básicas que automatizan tareas como la firma criptográfica de las solicitudes o el tratamiento de las respuestas de error, facilitándole así el comienzo. Para empezar, abre las Herramientas de Amazon Web Services y busca el SDK que prefieras en SDK.

Si prefiere utilizar una interfaz de línea de comandos, dispone de las siguientes opciones:

AWS Interfaz de línea de comandos (CLI)

Para empezar, consulte la AWS Command Line Interface Guía del usuario de . Para obtener más información sobre los comandos de Service Catalog, consulte servicecatalog en la AWS CLI Referencia de comandos.

AWS Herramientas para Windows PowerShell

Para empezar, consulte la Herramientas de AWS para PowerShell Guía del usuario de . Para obtener más información acerca de los cmdlets de Service Catalog, abra la referencia de Herramientas de AWS para PowerShell cmdlets y amplíe. AWS Service Catalog

La AWS Service Catalog API se puede dividir de forma lógica en las siguientes categorías.

Temas

Descubrimiento de productos

Utilice estas operaciones para descubrir u obtener información sobre los productos y sus requisitos de lanzamiento. Estas operaciones no crean ni modifican recursos.

SearchProducts

Muestra todos los productos a los que tiene acceso la persona que llama.

DescribeProduct

Obtenga información detallada sobre un producto.

DescribeProductView

Funcionalmente idéntico a`DescribeProduct`, excepto que toma el ID de una vista de producto en lugar del ID de un producto.

ListLaunchPaths

Muestra todas las formas en que el usuario tiene acceso a un producto específico, denominadas rutas al producto. El usuario debe seleccionar una ruta para aprovisionar el producto.

DescribeProvisioningParameters

Obtiene los parámetros necesarios para aprovisionar un producto específico y proporciona metadatos adicionales sobre lo que ocurrirá cuando se aprovisione el producto.

Cada uno de ellos `ProvisioningArtifactParameter` es algo que el usuario debe especificar para poder aprovisionar correctamente el producto (por ejemplo, el tamaño de una instancia EC2). Los `ConstraintSummary` objetos contienen la lista de valores permitidos y metadatos adicionales sobre los `ProvisioningArtifactParameter` objetos.

Solicitudes de aprovisionamiento

Utilice estas operaciones para solicitar, actualizar o finalizar el aprovisionamiento de un producto.

ProvisionProduct

Solicita el aprovisionamiento de un producto. Aprovisionar un producto es lanzar los recursos necesarios para ponerlo en línea para su uso real. Por ejemplo, aprovisionar un producto respaldado por una CloudFormation plantilla significa lanzar una CloudFormation pila y todos sus recursos subyacentes.

UpdateProvisionedProduct

Actualiza la configuración de un producto aprovisionado. Por ejemplo, un producto respaldado por CloudFormation actualiza su CloudFormation pila subyacente. El solicitante debe tener permisos de acceso suficientes para lo especificado ProvisionedProduct.

TerminateProvisionedProduct

Solicita la rescisión de un producto aprovisionado. Por ejemplo, en el caso de un producto respaldado por CloudFormation, esto elimina la pila subyacente CloudFormation . El solicitante debe tener suficientes permisos de acceso al producto aprovisionado especificado.

Productos aprovisionados

Utilice estas operaciones para obtener información sobre los productos aprovisionados. Estas operaciones no crean ni modifican recursos.

ListRecordHistory

Muestra todas las solicitudes realizadas, incluso las de los productos aprovisionados cancelados.

DescribeRecord

Obtiene información sobre una solicitud. Utilice esta operación después de la operación de solicitud para obtener la `RecordDetail` información actual.

SearchProvisionedProducts

Obtiene información sobre los productos aprovisionados que cumplen los criterios especificados.

ScanProvisionedProducts

Muestra los productos aprovisionados que no están terminados.

DescribeProvisionedProduct

Obtiene información sobre un producto aprovisionado.

ImportAsProvisionedProduct

Solicita la importación de un recurso como un producto aprovisionado de Service Catalog que está asociado a un producto de Service Catalog y a un artefacto de aprovisionamiento. Una vez importadas, todas las acciones de gobierno de Service Catalog compatibles se admiten en el producto aprovisionado.

UpdateProvisionedProductProperties

Solicita actualizaciones de las propiedades del producto aprovisionado especificado.

Planes de productos aprovisionados

Utilice estas operaciones para gestionar los planes de productos aprovisionados. Un plan incluye la lista de recursos que se pueden crear o modificar al ejecutar el plan.

CreateProvisionedProductPlan

Crea un plan.

DescribeProvisionedProductPlan

Obtiene información sobre los cambios en los recursos de un plan.

ExecuteProvisionedProductPlan

Aprovisiona o modifica un producto en función de un plan.

ListProvisionedProductPlans

Muestra los planes de un producto aprovisionado.

DeleteProvisionedProductPlan

Elimina un plan.

Carteras

Los administradores del catálogo utilizan estas operaciones para proporcionar todas las operaciones necesarias para la administración de la cartera.

CreatePortfolio

Crea una cartera.

DeletePortfolio

Elimina una cartera.

DescribePortfolio

Obtiene información detallada sobre una cartera.

DescribePortfolioShares

Devuelve un resumen de cada una de las acciones de la cartera que se crearon para la cartera especificada.

ListPortfolios

Muestra todas las carteras del catálogo.

ListPortfoliosForProduct

Muestra todas las carteras a las que está asociado un producto.

UpdatePortfolio

Actualiza una cartera.

UpdatePortfolioShare

Actualiza una cuota de cartera.

CreatePortfolioShare

Comparte una cartera con una AWS cuenta.

DeletePortfolioShare

Deja de compartir una cartera.

AcceptPortfolioShare

Acepta una oferta para compartir una cartera.

RejectPortfolioShare

Rechaza una oferta de compartir una cartera.

ListAcceptedPortfolioShares

Muestra los detalles de todas las carteras que esta cuenta ha aceptado compartir.

ListPortfolioAccess

Muestra los ID de cuenta que tienen acceso a una cartera.

Asociación principal

Los administradores del catálogo utilizan estas operaciones para realizar todas las operaciones necesarias para la asociación principal.

AssociatePrincipalWithPortfolio

Asocia un ARN principal a una cartera.

DisassociatePrincipalFromPortfolio

Disocia un ARN principal de una cartera.

ListPrincipalsForPortfolio

Muestra todos los ARN principales asociados a una cartera.

Productos

Los administradores del catálogo utilizan estas operaciones para proporcionar todas las operaciones necesarias para la administración del producto.

SearchProductsAsAdmin

Obtiene información resumida y de estado de los productos.

DescribeProductAsAdmin

Obtiene información sobre un producto.

CreateProduct

Crea un producto.

CopyProduct

Copia un producto.

DescribeCopyProductStatus

Obtiene el estado de una operación de copia de un producto.

UpdateProduct

Actualiza un producto.

DeleteProduct

Elimina un producto.

AssociateProductWithPortfolio

Asocia un producto a una cartera.

DisassociateProductFromPortfolio

Disocia un producto de una cartera.

Aprovisionamiento de artefactos

Los administradores del catálogo utilizan estas operaciones para administrar los artefactos de aprovisionamiento (también conocidos como versiones de productos).

DescribeProvisioningArtifact

Obtiene información sobre un artefacto de aprovisionamiento.

CreateProvisioningArtifact

Crea un artefacto de aprovisionamiento para un producto.

DeleteProvisioningArtifact

Elimina un artefacto de aprovisionamiento.

ListProvisioningArtifacts

Muestra todos los artefactos de aprovisionamiento asociados a un producto.

UpdateProvisioningArtifact

Actualiza un artefacto de aprovisionamiento.

Restricciones

El administrador del catálogo utiliza estas operaciones para gestionar las restricciones.

CreateConstraint

Crea una restricción.

DeleteConstraint

Elimina una restricción.

DescribeConstraint

Obtiene información sobre una restricción.

UpdateConstraint

Actualiza una restricción.

ListConstraintsForPortfolio

Obtiene información sobre las restricciones de una cartera y un producto.

Acciones de servicio

Los administradores del catálogo utilizan estas operaciones para gestionar las acciones de servicio.

AssociateServiceActionWithProvisioningArtifact

Asocia una acción de autoservicio a un artefacto de aprovisionamiento.

CreateServiceAction

Crea una acción de autoservicio.

DeleteServiceAction

Elimina una acción de autoservicio.

DescribeServiceAction

Describe una acción de autoservicio.

DescribeServiceActionExecutionParameters

Busca los parámetros predeterminados de una acción de autoservicio específica en un producto aprovisionado específico y devuelve un mapa de los resultados al usuario.

ExecuteProvisionedProductServiceAction

Ejecuta una acción de autoservicio contra un producto aprovisionado.

UpdateServiceAction

Actualiza una acción de autoservicio.

TagOptions

Los administradores del catálogo utilizan estas operaciones para administrar. TagOptions

CreateTagOption

Crea un TagOption.

ListTagOptions

Enumera tus TagOptions.

DescribeTagOption

Describe un TagOption.

UpdateTagOption

Actualiza un TagOption.

AssociateTagOptionWithResource

Asocia a TagOption a un recurso.

DisassociateTagOptionFromResource

Disocia a TagOption de un recurso.

ListResourcesForTagOption

Muestra los recursos de un TagOption.

DeleteTagOption

Elimina un TagOption.

AppRegistry

Sirve como repositorio para sus aplicaciones, sus recursos y los metadatos de las aplicaciones que utiliza en su empresa.

AssociateAttributeGroup

Asocia un grupo de atributos a una aplicación para aumentar los metadatos de la aplicación con los atributos del grupo.

AssociateResource

Asocia un recurso a una aplicación.

CreateApplication

Crea una nueva aplicación que es el nodo de nivel superior de una jerarquía de abstracciones de recursos de nube relacionados.

CreateAttributeGroup

Crea un nuevo grupo de atributos como contenedor para atributos definidos por el usuario.

DeleteApplication

Elimina una aplicación que se especifica por su nombre o ID de aplicación.

DeleteAttributeGroup

Elimina un grupo de atributos, especificado por su ID o nombre del grupo de atributos.

DisassociateAttributeGroup

Disocia un grupo de atributos de una aplicación para eliminar los atributos adicionales contenidos en el grupo de atributos de los metadatos de la aplicación.

DisassociateResource

Disocia un recurso de la aplicación.

GetApplication

Recupera información de metadatos sobre una de sus aplicaciones.

GetAssociatedResource

Obtiene el recurso asociado a la aplicación.

GetAttributeGroup

Recupera un grupo de atributos, ya sea por su nombre o por su identificador.

ListApplications

Muestra todos los grupos de atributos que están asociados a la aplicación especificada.

ListAssociatedAttributeGroups

Muestra todos los grupos de atributos que están asociados a la aplicación especificada.

ListAssociatedResources

Muestra todos los recursos asociados a la aplicación especificada.

ListAttributeGroups

Muestra todos los grupos de atributos a los que tiene acceso.

ListAttributeGroupsForApplication

Muestra los detalles de todos los grupos de atributos asociados a una aplicación específica.

ListTagsForResource

Muestra todas las etiquetas del recurso.

TagResource

Asigna una o más etiquetas (pares clave-valor) al recurso especificado.

SyncResource

Sincroniza el recurso con lo que está registrado actualmente. AppRegistry

UntagResource

Elimina etiquetas de un recurso.

UpdateApplication

Actualiza una aplicación existente con nuevos atributos.

UpdateAttributeGroup

Actualiza un grupo de atributos existente con nuevos detalles.

Ejemplo de flujo de trabajo

En este escenario, el administrador crea recursos utilizando los productos disponibles AWS Service Catalog y un usuario final los encuentra y los aprovisiona. Este es un ejemplo de flujo de trabajo; no es la única forma de utilizar la AWS Service Catalog API.

Tareas de administrador

- Cree carteras, vistas de productos, productos, versiones de productos y restricciones.
- Asigne usuarios de IAM a los productos, lo que les da acceso.

Tareas del usuario final

1. El usuario llama SearchProductssin argumentos. Esto devuelve la lista de productos a los que tiene acceso el usuario, así como un «SearchDomain» que se puede utilizar para analizar los resultados.
2. El usuario sigue llamando SearchProductscon filtros de búsqueda adicionales hasta encontrar el producto deseado.
3. El usuario llama DescribeProductViewpara buscar la lista de dispositivos de aprovisionamiento (también conocidos como versiones) de este producto. Esto determina lo que realmente aprovisiona el usuario.
4. El usuario llama ListLaunchPathspara buscar la lista de rutas de este producto, junto con las restricciones de cada ruta. Esto determina qué conjunto de restricciones se aplica al producto aprovisionado.
5. Tras elegir un artefacto de aprovisionamiento y una ruta, el usuario llama. DescribeProvisioningParameters Esto devuelve la lista de parámetros que el usuario debe proporcionar antes de aprovisionar un producto mediante el artefacto y la ruta de aprovisionamiento, junto con las instrucciones de uso adicionales que el administrador haya decidido proporcionar.

6. El usuario llama y especifica el producto ProvisionProduct, aprovisiona el artefacto, la ruta y los parámetros de entrada. Los parámetros de entrada son una lista de pares clave-valor, donde las claves se obtienen utilizando DescribeProvisioningParametersy los valores los proporciona el usuario (por ejemplo,). `{ParameterKey:"dbpassword", ParameterValue:"mycoolpassword"}` Esto inicia un flujo de trabajo para crear los recursos especificados. AWS También crea un detalle de registro que rastrea la solicitud de aprovisionamiento y un objeto de producto aprovisionado que representa los recursos subyacentes AWS .
7. El usuario sondea DescribeRecordpara ver cuándo el estado de los detalles del registro cambia de `IN_PROGRESS` estado a estado completo (`SUCCEEDED`o `ERROR` completo).
8. Cuando el detalle del registro de la solicitud está completado, el usuario DescribeRecordvuelve a llamar. Los resultados identifican los recursos creados.
9. El usuario llama UpdateProvisionedProductpara actualizar los recursos subyacentes existentes. En función de las actualizaciones específicas solicitadas, esta operación puede actualizarse sin interrupción, con alguna interrupción o sustituir por completo el producto aprovisionado.
10. Por último, el usuario llama TerminateProvisionedProductpara cancelar el producto aprovisionado.

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
Motores externos para AWS Service Catalog	AWS Service Catalog añade nueva documentación para motores externos. Los motores externos se represent an 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 informaci ón, consulte Motores externos para. AWS Service Catalog	16 de mayo de 2024
Actualización de seguridad de IAM	AWS Service Catalog actualiza la `AWSServic eCatalogSyncServic eRolePolicy` política	7 de mayo de 2024

	para cambiarla `codestar-connections` `acodeconnections` . 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	Description (Descripción)	Fecha de lanzamiento de la nueva versión
AWS Service Catalog	Para obtener más informaci ón sobre los cambios de Hashicorp en las licencias de Terraform y la actualiza ción al tipo de producto externo, consulte Actualizar los productos existentes de Terraform Open Source y los productos aprovisionados al tipo de producto externo.	20 de octubre de 2023
AWS Service Catalog	Para obtener información sobre cómo compartir una cartera AWS Organizations y AWS Service Catalog permitir su sincronización AWS Organizations, consulta la AWSServiceCatalogO rgsDataSyncService RolePolicypolítica y la función	14 de abril de 2023

Característica	Description (Descripción)	Fecha de lanzamiento de la nueva versión
	AWSServiceRoleForServiceCatalogOrgsDataSyncvinculada al servicio.	
AWS Service Catalog	Para obtener información sobre cómo administrar los productos conectados AWS Service Catalog a git y permitir la sincronización de las plantillas de un repositorio externo con tus AWS Service Catalog productos, consulta la función vinculada a la AWSServiceCatalogSyncServiceRolePolicypolítica y al servicio. AWSServiceRoleForServiceCatalogSync	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. AWS Service Catalog AppRegistry	15 de junio de 2022
AWS Service Management Connector	Para obtener más información sobre Connectors for Jira Service Management ServiceNow, consulte AWS Service Management Connector.	9 de junio de 2022

Característica	Description (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 conector de administración de servicios de AWS para Jira Service Management.	25 de mayo de 2021
Conector para ServiceNow	Para obtener más información sobre las actualizaciones del conector ServiceNow, consulte AWS Service Management Connector for ServiceNow.	7 de abril de 2021
Conector para ServiceNow	Para obtener más información sobre las actualizaciones del conector ServiceNow, consulte AWS Service Management Connector for ServiceNow.	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 servicio AWS Service Catalog predeterminadas.	24 de marzo de 2020

Característica	Description (Descripción)	Fecha de lanzamiento de la nueva versión
Biblioteca de introducción	Para obtener más informaci ón sobre la biblioteca de plantillas de productos bien diseñadas que ofrece, consulte AWS Service CatalogBiblioteca de introducción	10 de marzo de 2020
Guía de versión	Para obtener más información acerca de la guía de versión del producto, consulte Guía de la versión.	17 de diciembre de 2019
Conector para Jira Service Desk	Para empezar a usar el conector para Jira Service Desk, consulte el conector de administración de servicios de AWS para Jira Service Desk.	21 de noviembre de 2019
Conector para ServiceNow	Para obtener más informaci ón sobre las actualizaciones del conector ServiceNo w, consulte AWS Service Management Connector for ServiceNow.	18 de noviembre de 2019
Nuevo capítulo de seguridad	Para obtener más información sobre la seguridad en AWS Service Catalog, consulte Seguridad en AWS Service Catalog.	31 de octubre de 2019

Característica	Description (Descripción)	Fecha de lanzamiento de la nueva versión
Cambio del propietario del producto aprovisionado	Para obtener informaci ón sobre cómo cambiar el propietario de los productos aprovisionados, consulte Cambio del propietario del producto aprovisionado.	31 de octubre de 2019
Nueva restricción de actualiza ción de recursos	Para obtener más informaci ón acerca de cómo utilizar la restricción RESOURCE_ UPDATE para actualizar las etiquetas en los productos aprovisionados, consulte Restricciones de actualización de etiquetas de AWS Service Catalog.	17 de abril de 2019
Conector para ServiceNow	Para empezar a utilizar el conector para ServiceNo w, consulte el conector de administración de AWS servi cios para ServiceNow.	19 de marzo de 2019
Support para AWS CloudFormation StackSets	Para empezar a usarlo AWS CloudFormation StackSets, consulte Uso AWS CloudFormation StackSets.	14 de noviembre de 2018
Acciones de autoservicio	Para comenzar a utilizar acciones de autoservicio, consulte Acciones de servicio de AWS CloudFormation .	17 de octubre de 2018

Característica	Description (Descripción)	Fecha de lanzamiento de la nueva versión
CloudWatch Métricas de Amazon	Para obtener más informaci ón sobre CloudWatch las métricas de Amazon, consulta AWS Service CatalogAmazon CloudWatch.	26 de septiembre de 2018
Support para TagOptions	Para administrar etiquetas , consulte AWS Service Catalog TagOptionBiblioteca.	28 de junio de 2017
Importación de una cartera	Para importar una cartera compartida desde otra AWS cuenta, consulta Importación de una cartera.	16 de febrero de 2016
Actualización de la informaci ón de permisos	Para conceder acceso a la vista de la consola de usuario final, consulte Acceso a la consola para usuarios finales.	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.