Guia do administrador

AWS Service Catalog

AWS Service Catalog: Guia do administrador

Table of Contents

O que é Service Catalog?

O Service Catalog permite que organizações criem e gerenciem os catálogos de serviços de TI aprovados para uso na AWS. Esses serviços de TI podem incluir tudo, de imagens de máquinas virtuais, servidores, software e bancos de dados e mais para concluir arquiteturas de aplicativos multicamada.

O Service Catalog permite que as organizações gerenciem de maneira centralizada os serviços de TI comumente implantados, além de ajudá-las a atingir uma governança consistente e atender aos requisitos de conformidade. Os usuários finais podem implantar rapidamente somente os serviços de TI aprovados de que precisam, seguindo as restrições definidas pela organização.

O Service Catalog oferece os seguintes benefícios:

- Padronização

  Administre e gerencie ativos aprovados, restringindo onde o produto pode ser lançado, o tipo de instância que pode ser usada, e muitas outras opções de configuração. O resultado é um cenário padronizado para o provisionamento de produtos para toda a organização.

- Descoberta e lançamento por autoatendimento

  Os usuários procuram listas de produtos (serviços ou aplicativos) às quais têm acesso, localizam o produto que desejam usar e o lançam por conta própria como um produto provisionado.

- Controle de acesso detalhado

  Os administradores criam portfólios de produtos de seu catálogo, adicionam restrições e tags de recursos a serem usadas no provisionamento, depois concedem acesso ao portfólio por meio de usuários (IAM) e grupos AWS Identity and Access Management.

- Extensibilidade e controle de versão

  Os administradores podem adicionar um produto a quantos portfólios quiserem e restringi-lo sem criar outra cópia. Atualizar o produto para uma nova versão propaga a atualização para todos os produtos em todos os portfólios que fazem referência a ele.

Para obter mais informações, consulte a página de detalhes do Service Catalog.

A API do Service Catalog fornece controle programático de todas as ações do usuário final como alternativa ao uso do AWS Management Console. Para obter mais informações, consulte o Guia do Desenvolvedor do Service Catalog.

Vídeo: Introdução ao AWS Service Catalog

Este vídeo (7:27) descreve como criar, organizar e controlar um catálogo de produtos da AWS com curadoria e compartilhar produtos com nível de permissões. Como resultado, os usuários finais podem provisionar rapidamente os recursos de TI aprovados sem acesso direto aos serviços da AWS subjacentes.

Introdução à AWS Service Catalog

Visão geral do Service Catalog

Quando você começar a usar o Service Catalog, poderá tirar proveito do conhecimento sobre seus componentes e os fluxos de trabalho iniciais para administradores e usuários finais.

Usuários

O Service Catalog comporta os seguintes tipos de usuário:

- Administradores de catálogo (administradores) - gerenciam um catálogo de produtos (aplicativos e serviços), organizando-os em portfólios e concedendo acesso a usuários finais. Os administradores de catálogo preparam modelos do AWS CloudFormation, configuram restrições e gerenciam os perfis do IAM que são atribuídos a produtos para oferecer um gerenciamento avançado de recursos.
- Usuários finais - recebem as credenciais da AWS do departamento de TI ou do gerente e usam o AWS Management Console para lançar os produtos para os quais receberam acesso. Às vezes chamados simplesmente de usuários, os usuários finais podem receber permissões diferentes de acordo com suas necessidade operacionais. Por exemplo, um usuário pode ter o nível de permissão máximo (para lançar e gerenciar todos os recursos necessários pelos produtos que usa) ou permissão somente para usar recursos de serviços específicos.

Produtos

Um produto é um serviço de TI que você deseja disponibilizar para implantação na AWS. Um produto consiste em um ou mais recursos da AWS, como instâncias do EC2, volumes de armazenamento,

bancos de dados, configurações de monitoramento e componentes de rede ou pacotes de produtos da AWS Marketplace. Um produto pode ser uma única instância de computação em execução no AWS Linux, um aplicativo web multicamada totalmente configurado em execução em seu próprio ambiente ou uma opção intermediária.

Para criar um produto, é necessário importar um modelo do AWS CloudFormation. Os modelos do AWS CloudFormation definem os recursos da AWS necessários para o produto, os relacionamentos entre os recursos e os parâmetros que os usuários finais podem conectar ao lançar o produto para configurar grupos de segurança, criar pares de chaves e realizar outras personalizações.

HashiCorp Suporte ao Terraform Open Source e ao Terraform Cloud

AWS Service Catalogpermite o provisionamento rápido e de autoatendimento com governança para suas configurações internas do HashiCorp Terraform Open Source e do Terraform Cloud. AWS Você pode usar o Service Catalog como uma única ferramenta para organizar, controlar e distribuir suas configurações do Terraform em grande escala na AWS. Você pode acessar os principais recursos do Service Catalog, incluindo catalogação de modelos padronizados e pré-aprovados do Terraform, controle de acesso, provisionamento de privilégios mínimos, controle de versão, marcação e compartilhamento com milhares de contas da AWS. Seus usuários finais veem uma lista simples de produtos e versões aos quais têm acesso e, em seguida, podem implantar esses produtos em uma única ação.

Para saber mais e concluir um tutorial do produto Terraform, consulte Conceitos básicos de um produto Terraform.

Produtos provisionados

As pilhas do AWS CloudFormation facilitam o gerenciamento do ciclo de vida do seu produto permitindo que você provisione, marque, atualize e elimine a instância do produto como uma única unidade. Uma pilha do AWS CloudFormation inclui um modelo do AWS CloudFormation, escrito em formato JSON ou YAML, e o conjunto de recursos correspondente. Um produto provisionado é uma pilha. Quando um usuário final lança um produto, a instância do produto provisionada pelo Service Catalog é uma pilha com os recursos necessários para executar o produto. Para obter mais informações, consulte o Guia do usuário do AWS CloudFormation.

Portfólios

Um portfólio é uma coleção de produtos junto com informações de configuração. Os portfólios ajudam a gerenciar quem pode usar produtos específicos e como podem usá-los. Com o Service

Catalog, você pode criar um portfólio personalizado para cada tipo de usuário em sua organização e conceder acesso de modo seletivo ao portfólio adequado. Quando você adiciona uma nova versão de um produto a um portfólio, essa versão é disponibilizada automaticamente para todos os usuários atuais.

Você também pode compartilhar portfólios com outras contas da AWS e permitir que o administrador dessas contas distribua seus portfólios com restrições adicionais, como limitar quais instâncias do EC2 um usuário pode criar. Com o uso de portfólios, permissões, compartilhamento e restrições, você pode garantir que os usuários estejam lançando produtos configurados corretamente de acordo com as necessidades e os padrões da organização.

Versionamento

O Service Catalog permite que você gerencie várias versões dos produtos no catálogo. Isso permite que você adicione novas versões de modelos e recursos associados com base em atualizações de software ou em alterações da configuração.

Quando você cria uma nova versão de um produto, a atualização é distribuída automaticamente a todos os usuários que têm acesso ao produto, permitindo que o usuário selecione qual versão do produto usar. Os usuários podem atualizar instâncias do produto em execução para a nova versão de maneira rápida e fácil.

Permissões

A concessão de acesso a um portfólio a um usuário permite que esse usuário navegue pelo portfólio e lance os produtos contidos nele. Você aplica permissões do AWS Identity and Access Management (IAM) para controlar quem pode visualizar e modificar seu catálogo. As permissões do IAM podem ser atribuídas a usuários IAM, grupos e perfis.

Quando um usuário lança um produto que tem um perfil do IAM atribuído a ele, o Service Catalog usa o perfil para lançar os recursos em nuvem do produto usando o AWS CloudFormation. Ao atribuir um perfil do IAM a cada produto, você pode evitar conceder permissões aos usuários para execução de operações não aprovadas e permitir que eles provisionem recursos usando o catálogo.

Restrições

As restrições controlam a maneira como você pode implantar recursos da AWS específicos para um produto. Você pode usá-las para aplicar limites aos produtos para realizar a governança e o controle

de custos. O AWS Service Catalog tem diferentes tipos de restrição: restrições de lançamento, restrições de notificação e restrições de modelo.

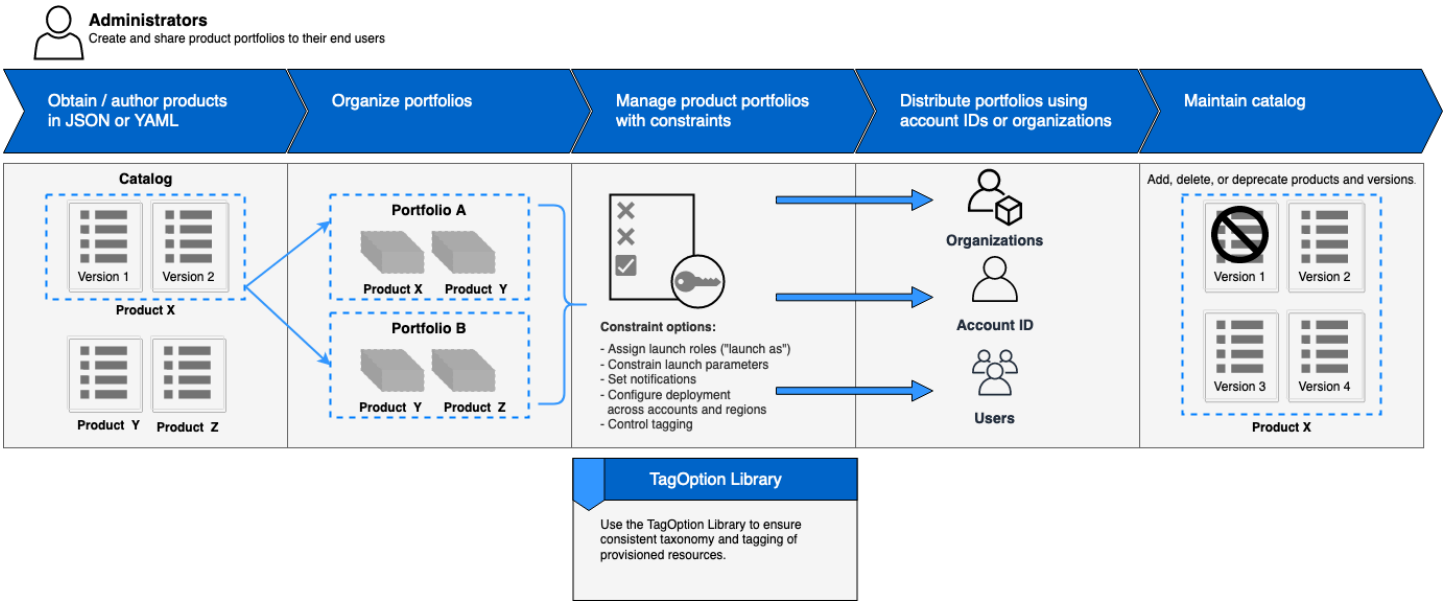
Com as restrições de lançamento, você especifica uma função para um produto em um portfólio. Use esta função para provisionar os recursos no lançamento, dessa forma você pode restringir as permissões de usuários sem prejudicar a capacidade dos usuários de provisionarem produtos do catálogo.

As restrições de notificação permitem que você receba notificações sobre eventos de pilha usando um tópico do Amazon SNS.

As restrições de modelos limitam os parâmetros de configuração disponíveis para o usuário durante o lançamento do produto (por exemplo, tipos de instância do EC2 ou intervalos de endereços IP). Com restrições de modelos, você reutiliza modelos do AWS CloudFormation para produtos e aplica restrições aos modelos com base em produto ou em portfólio.

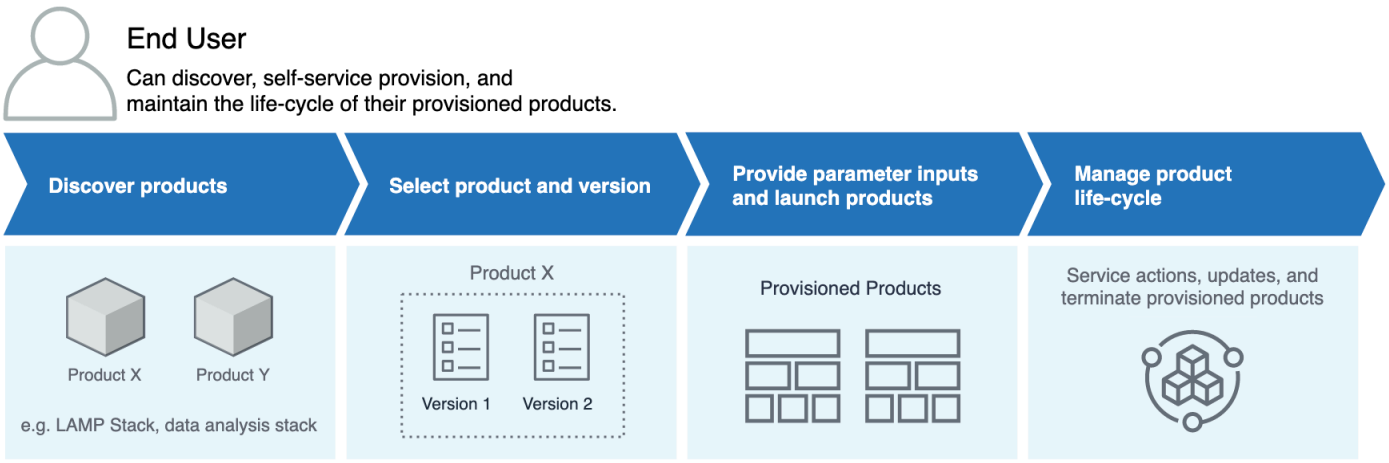
Fluxo de trabalho inicial de administrador

O diagrama mostra o fluxo de trabalho inicial para um administrador para criar um catálogo.



Fluxo de trabalho inicial de usuário final

Este diagrama mostra o fluxo de trabalho inicial para um usuário final.



Cotas de serviço padrão do AWS Service Catalog

Sua AWS conta tem as seguintes cotas padrão para restriçãoAWS Organizations, portfólio, produto, produto provisionado, regional, ação de serviço e. TagOptions

É possível usar Service Quotas para gerenciar as cotas ou solicitar um aumento de cota. Para obter mais informações sobre o Service Quotas, consulte O que é Service Quotas? no Guia do usuário do Service Quotas. Para solicitar um aumento de cota, consulte Solicitar um aumento de cota.

AWS Organizations

- Administradores delegados do AWS Service Catalog por organização: 50

Cotas de restrição

- Restrições por produto por portfólio: 100

Cotas de portfólio

- Usuários, grupos e funções por portfólio: 100
- Produtos por portfólio: 150
- Tags por portfólio: 20
- Contas compartilhadas por portfólio: 5.000
- Valores de tag por chave de tag: 25

Cotas de produtos

- Usuários, grupos e funções por produto: 200
- Versões de produtos por produto: 100
- Tags por produto: 20
- Valores de tag por chave de tag: 25

Cotas de produtos provisionados

- Tags por produto provisionado: 50

Cotas regionais

- Portfólios: 100
- Produtos: 350

Cotas de ação de serviço

- Ações de serviço por região: 200
- Associações de ação de serviço por versão do produto: 25

TagOptions cotas

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

Configuração AWS Service Catalog

Antes de começar AWS Service Catalog, conclua as tarefas a seguir.

Tópicos

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga as instruções on-line.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e digitar um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário-raiz tem acesso a todos os Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, é possível visualizar as atividades da conta atual e gerenciar sua conta acessando https://aws.amazon.com/ e selecionando Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS AWS IAM Identity Center, habilite e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login AWS Management Consolecomo proprietário da conta escolhendo Usuário raiz e inserindo seu endereço de Conta da AWS e-mail. Na próxima página, digite sua senha.

   Para obter ajuda ao fazer login usando o usuário-raiz, consulte Signing in as the root user (Fazer login como usuário-raiz) no Guia do usuário do Início de Sessão da AWS .
2. Habilite a autenticação multifator (MFA) para o usuário-raiz.

   Para obter instruções, consulte Habilitar um dispositivo de MFA virtual para seu usuário Conta da AWS raiz (console) no Guia do usuário do IAM.

Criar um usuário com acesso administrativo

1. Habilitar o IAM Identity Center.

   Para obter instruções, consulte Habilitar AWS IAM Identity Center no Guia do usuário do AWS IAM Identity Center .
2. No Centro de Identidade do IAM, conceda o acesso administrativo para um usuário.

   Para ver um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no Guia AWS IAM Identity Center do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para fazer login com seu usuário do Centro de Identidade do IAM, use a URL de login que foi enviada ao seu endereço de e-mail quando você criou o usuário do Centro do Usuário do IAM.

  Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no portal de AWS acesso no Guia Início de Sessão da AWS do usuário.

Atribuir acesso a usuários adicionais

1. No Centro de Identidade do IAM, crie um conjunto de permissões que siga as práticas recomendadas de aplicação de permissões com privilégio mínimo.

Para obter instruções, consulte Create a permission set no Guia do usuário do AWS IAM Identity Center .

2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Add groups no Guia do usuário do AWS IAM Identity Center .

Para conceder acesso, adicione as permissões aos seus usuários, grupos ou perfis:

- Usuários e grupos em AWS IAM Identity Center:

  Crie um conjunto de permissões. Siga as instruções em Criação de um conjunto de permissões no Guia do usuário do AWS IAM Identity Center .
- Usuários gerenciados no IAM com provedor de identidades:

  Crie um perfil para a federação de identidades. Siga as instruções em Criar um perfil para um provedor de identidades de terceiros (federação) no Guia do usuário do IAM.
- Usuários do IAM:
  - Crie um perfil que seu usuário possa assumir. Siga as instruções em Criação de um perfil para um usuário do IAM no Guia do usuário do IAM.
  - (Não recomendado) Vincule uma política diretamente a um usuário ou adicione um usuário a um grupo de usuários. Siga as instruções em Adição de permissões a um usuário (console) no Guia do usuário do IAM.

Conceder permissões a administradores do AWS Service Catalog

Como administrador do catálogo, você precisa de acesso à visualização do console do administrador do AWS Service Catalog e permissões do IAM que permitam executar tarefas como as seguintes:

- Criar e gerenciar portfólios
- Criar e gerenciar produtos
- Adicionar restrições de modelos para controlar as opções disponíveis para os usuários finais ao lançar um produto
- Adicionar restrições de lançamento para definir os perfis do IAM que o AWS Service Catalog assume quando os usuários finais lançam produtos
- Conceder acesso a seus produtos aos usuários finais

Você ou um administrador que gerencia suas permissões do IAM deve anexar políticas a seu usuário, grupo ou perfil do IAM que são necessárias para concluir este tutorial.

Para conceder permissões a um administrador de catálogo

1. Abra o console IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, expanda Gerenciamento de acesso e escolha Usuários. Se você já tiver criado um usuário do IAM que você gostaria de usar como o administrador do catálogo, escolha o nome do usuário e, em seguida, Adicionar permissões. Do contrário, crie um usuário da seguinte forma:
   a. Escolha Adicionar usuário.
   b. Para User name, digite **`ServiceCatalogAdmin`**.
   c. Selecione Acesso programático e AWS Management Console acesso.
   d. Escolha Próximo: permissões.
3. Escolha Anexar políticas existentes diretamente.
4. Escolha Criar política e proceda da seguinte maneira:
   a. Selecione a guia JSON.
   b. Copie e cole a política de exemplo a seguir em Documento da 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. Escolha Próximo: etiquetas.

d. (Opcional) Selecione Adicionar tag para associar um par de chave-valor ao recurso. É possível adicionar um máximo de 50 tags.

> **Note**
>
> As tags são pares de chave-valor que você pode adicionar aos recursos. Isso ajuda a identificar, organizar e pesquisar recursos. Para obter mais informações, consulte Marcar recursos da AWS no Guia de Referência da Referência geral da AWS.

e. Escolha Próximo: revisar.

f. Para Policy Name, digite **`ServiceCatalogAdmin-AdditionalPermissions`**.

> **Important**
>
> Você deve conceder aos administradores permissões do Amazon S3 para acessar modelos que o AWS Service Catalog armazena no Amazon S3. Para obter mais informações, consulte Exemplos de política do usuário no Guia do Usuário do Amazon Simple Storage Service.

g. Escolha Create Policy.

5. Retorne para a janela do navegador com a página de permissões e escolha Refresh.
6. No campo de pesquisa, digite **`ServiceCatalog`** para filtrar a lista de políticas.
7. Selecione a caixa de seleção ao lado da política **`AWSServiceCatalogAdminFullAccess`** e **`ServiceCatalogAdmin-AdditionalPermissions`** e selecione Próximo: Revisar.
8. Se estiver atualizando um usuário, escolha Add permissions.

   Se você estiver criando um usuário, escolha Create user. Você pode fazer download ou copiar as credenciais e escolher Close.

9. Para fazer login como o administrador do catálogo, use a URL específica à conta. Para localizar essa URL, escolha Dashboard no painel de navegação e escolha Copy Link. Cole o link em seu navegador e use o nome e a senha do usuário do IAM criado ou atualizado neste procedimento.

Conceder permissões a usuários finais do AWS Service Catalog

Para que o usuário final possa usar o AWS Service Catalog, você deve conceder acesso à visualização do console de usuário final do AWS Service Catalog. Para conceder acesso, anexe políticas ao usuário, grupo ou função do IAM que é usada pelo usuário final. No procedimento a seguir, anexamos a política **`AWSServiceCatalogEndUserFullAccess`** a um grupo do IAM.

Como conceder permissões a um usuário final

1. Abra o console IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, selecione User groups (Grupos de usuários).
3. Escolha Criar grupo e faça o seguinte:
   a. Em Nome do grupo do usuário, digite **`Endusers`**.
   b. No campo de pesquisa, digite **`AWSServiceCatalog`** para filtrar a lista de políticas.
   c. Marque a caixa de seleção da política **`AWSServiceCatalogEndUserFullAccess`**. Você também pode escolher **`AWSServiceCatalogEndUserReadOnlyAccess`**.
   d. Selecione Create Group.
4. No painel de navegação, escolha Users.
5. Escolha Adicionar usuários e faça o seguinte:
   a. Em Nome de usuário, digite um nome para o usuário.
   b. Selecione Senha – acesso ao Console de Gerenciamento da AWS.
   c. Escolha Próximo: permissões.
   d. Escolha Add user to group.
   e. Marque a caixa de seleção para o grupo Endusers (Usuários finais) e selecione Next: Tags (Próximo: tags) e Next: Review (Próximo: revisar).
   f. Na página Review (Revisar), selecione Create user (Criar usuário). Baixe ou copie as credenciais e selecione Fechar.

Instale e configure o mecanismo de provisionamento do Terraform

Para usar com sucesso os produtos Terraform com AWS Service Catalog, você deve instalar e configurar um mecanismo de provisionamento do Terraform na mesma conta em que administrará os produtos Terraform. Para começar, você pode usar o mecanismo de provisionamento do Terraform fornecido pela AWS, que instala e configura o código e a infraestrutura necessários para o mecanismo de provisionamento do Terraform funcionar com AWS Service Catalog. Essa configuração única leva aproximadamente 30 minutos. AWS Service Catalogfornece um GitHub repositório com instruções sobre como instalar e configurar o mecanismo de provisionamento do Terraform.

Determinação da fila

Quando você chama uma operação de provisionamento, AWS Service Catalog prepara uma mensagem de carga útil para enviar à fila relevante no mecanismo de provisionamento. Para criar o ARN para a fila, AWS Service Catalog faz as seguintes suposições:

- O mecanismo de provisionamento está localizado na conta do proprietário do produto
- O mecanismo de provisionamento está localizado na mesma região em que a chamada para AWS Service Catalog foi feita
- As filas do mecanismo de provisionamento seguem o esquema de nomenclatura documentado, detalhado abaixo.

Por exemplo, se ProvisionProduct for chamado `us-east-1` da conta 1111111111 usando um produto criado pela conta 0000000000000, presume-se AWS Service Catalog que o ARN correto do SQS seja. `arn:aws:sqs:us-east-1:0000000000000:ServiceCatalogTerraformOSProvisionOperationQueue`

A mesma lógica se aplica à função do Lambda chamada por `DescribeProvisioningParameters`.

Adicionar Confused Deputy ao seu mecanismo de provisionamento do Terraform

Chaves de contexto Confused Deputy nos endpoints para restringir o acesso às operações **`lambda:Invoke`**

A função do Lambda do analisador de parâmetros criada por mecanismos fornecidos por AWS Service Catalog tem uma política de acesso que concede permissão `lambda:Invoke` entre contas somente à entidade principal do serviço do AWS Service Catalog:

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

Essa deve ser a única permissão necessária para que a integração com AWS Service Catalog funcione corretamente. No entanto, você pode restringir isso ainda mais usando a chave de contexto `aws:SourceAccount` Confused Deputy. Ao enviar mensagens AWS Service Catalog para essas filas, AWS Service Catalog preenche a chave com o ID da conta de aprovisionamento. Isso é útil quando você pretende distribuir produtos por meio do compartilhamento de portfólio e quer garantir que somente contas específicas estejam usando seu mecanismo.

Por exemplo, você pode restringir seu mecanismo para permitir somente solicitações originadas de 000000000000 e 111111111111 usando a condição mostrada abaixo:

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

```
          "Principal": {
            "Service": "servicecatalog.amazonaws.com"
          },
          "Action": "lambda:InvokeFunction",
          "Resource": "arn:aws:lambda:us-
east-1:account_id:function:ServiceCatalogTerraformOSParameterParser",
          "Condition": {
            "StringLike": {
              "aws:SourceAccount": ["000000000000", "111111111111"]
        }
      }
    }
  ]
}
```

Chaves de contexto Confused Deputy nos endpoints para restringir o acesso às operações **`sqs:SendMessage`**

As filas de entrada da operação de provisionamento do Amazon SQS criadas por mecanismos fornecidos por AWS Service Catalog têm uma política de acesso que concede permissões `sqs:SendMessage` entre contas (e KMS associadas) somente à entidade principal do serviço AWS Service Catalog:

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

```
          "Principal": {
            "Service": "servicecatalog.amazonaws.com"
          },
          "Action": [
            "kms:DescribeKey",
            "kms:Decrypt",
            "kms:ReEncrypt",
            "kms:GenerateDataKey"
          ],
          "Resource": "arn:aws:kms:us-east-1:account_id:key/key_id"
    }
  ]
}
```

Essa deve ser a única permissão necessária para que a integração com AWS Service Catalog funcione corretamente. No entanto, você pode restringir isso ainda mais usando a chave de contexto `aws:SourceAccount` Confused Deputy. Ao AWS Service Catalog enviar mensagens para essas filas, AWS Service Catalog preenche as chaves com a ID da conta de aprovisionamento. Isso é útil quando você pretende distribuir produtos por meio do compartilhamento de portfólio e quer garantir que somente contas específicas estejam usando seu mecanismo.

Por exemplo, você pode restringir seu mecanismo para permitir somente solicitações originadas de 000000000000 e 111111111111 usando a condição mostrada abaixo:

```
{
      "Version": "2008-10-17",
      "Statement": [
      {
        "Sid": "Enable AWS Service Catalog to send messages to the queue",
        "Effect": "Allow",
        "Principal": {
          "Service": "servicecatalog.amazonaws.com"
        },
        "Action": "sqs:SendMessage",
        "Resource": [
          "arn:aws:sqs:us-
east-1:account_id:ServiceCatalogTerraformOSProvisionOperationQueue"
        ],
        "Condition": {
          "StringLike": {
            "aws:SourceAccount": ["000000000000", "111111111111"]
          }
```

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

Conceitos básicos

Você pode começar com AWS Service Catalog usando um dos modelos de produto bem arquitetados na Biblioteca de Fundamentos básicos ou seguindo as etapas em um dos tutoriais de introdução.

No tutorial, você executa tarefas como administrador do catálogo e usuário final. Como administrador do catálogo, você cria um portfólio e depois um produto. Como usuário final, você verifica se pode acessar o console do usuário final e lançar o produto. O produto é um dos seguintes:

- Um ambiente de desenvolvimento em nuvem executado no Amazon Linux e baseado em um modelo AWS CloudFormation que define os recursos da AWS que o produto pode usar.
- Um ambiente de código aberto executado em um mecanismo de provisionamento do Terraform e baseado em um arquivo de configuração tar.gz que define os recursos da AWS que o produto pode usar.

> **Note**
>
> Antes de começar, conclua os itens de ação em Configuração AWS Service Catalog.

Tópicos

Biblioteca de conceitos básicos

O AWS Service Catalog oferece uma biblioteca de conceitos básicos de modelos de produtos well-architected para você começar rapidamente. É possível copiar todos os produtos da biblioteca de conceitos básicos para a sua conta e depois personalizá-los de acordo com as suas necessidades.

Tópicos

Pré-requisitos

Antes de usar os modelos em nossa biblioteca de conceitos básicos, certifique-se de que você tem:

- As permissões necessárias para usar modelos do AWS CloudFormation. Para obter mais informações, consulte Controlar o acesso com o AWS Identity and Access Management.
- As permissões de administrador necessárias para gerenciar o AWS Service Catalog. Para ter mais informações, consulte the section called “Identity and Access Management”.

Saiba mais

Para obter mais informações sobre a estrutura bem arquitetada, consulte AWS bem arquitetada.

Conceitos básicos de um produto AWS CloudFormation

Você pode começar com AWS Service Catalog usando um dos modelos de produto bem arquitetados na Biblioteca de Fundamentos básicos ou seguindo as etapas em um dos tutoriais de introdução.

No tutorial, você executa tarefas como administrador do catálogo e usuário final. Como administrador do catálogo, você cria um portfólio e depois um produto. Como usuário final, você verifica se pode acessar o console do usuário final e lançar o produto. O produto é um ambiente de desenvolvimento em nuvem executado no Amazon Linux e é baseado em um modelo AWS CloudFormation que define os recursos AWS que o produto pode usar.

> **Note**
>
> Antes de começar, conclua os itens de ação em Configuração AWS Service Catalog.

Tópicos

- Etapa 7: Conceder acesso ao portfólio a usuários finais
- Etapa 8: Testar a experiência do usuário final

Etapa 1: Fazer download do modelo do AWS CloudFormation

Você pode usar modelos do AWS CloudFormation para configurar e provisionar portfólios e produtos. Modelos são arquivos de texto sem o formato JSON ou YAML que descrevem os recursos que você deseja provisionar. Para obter mais informações, consulte Formatos de modelos no Guia do usuário do AWS CloudFormation. Você pode usar o editor do AWS CloudFormation ou qualquer editor de texto para criar e salvar modelos. Para este tutorial, fornecemos um modelo simples para você começar. Esse modelo lança uma única instância do Linux configurada para acesso SSH.

> **Note**
>
> O uso de modelos do AWS CloudFormation requer permissões especiais. Antes de começar, verifique se você tem as seguintes permissões: Para obter mais informações, consulte pré-requisitos em Biblioteca de conceitos básicos.

Download do modelo

O modelo de amostra fornecido para este tutorial, `development-environment.template`, está disponível em https://awsdocs.s3.amazonaws.com/servicecatalog/development-environment.template.

Visão geral do modelo

O texto do modelo de exemplo é:

```
{
  "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 do modelo

O modelo declara os recursos a serem criados quando o produto for lançado. Consiste nas seguintes seções:

- AWSTemplateFormatVersion(opcional) — A versão do formato de AWS modelo usada para criar esse modelo. A versão do modelo mais recente é 2010-09-09 é o único valor válido no momento.
- Descrição (opcional) — uma descrição do modelo.
- Parâmetros (opcional) — os parâmetros que o usuário deve especificar para lançar o produto. Para cada parâmetro, o modelo inclui uma descrição e as restrições que devem ser atendidas pelo valor digitado. Para obter mais informações sobre restrições, consulte Uso de restrições do AWS Service Catalog.

  O parâmetro `KeyName` permite que você especifique um nome de par de chaves do Amazon Elastic Compute Cloud (Amazon EC2) que os usuários finais devem fornecer ao usar o AWS Service Catalog para lançar seu produto. Você criará o par de chaves na próxima etapa.
- Metadados (opcional) - os objetos que fornecem informações adicionais sobre o modelo. A chave AWS::CloudFormation: :Interface define como a visualização do console do usuário final exibe os parâmetros. A propriedade `ParameterGroups` define como os parâmetros são agrupados e os títulos desses grupos. A propriedade `ParameterLabels` define nomes de parâmetros amigáveis. Quando um usuário especifica parâmetros para lançar um produto baseado nesse modelo, a visualização do console do usuário final exibe o parâmetro rotulado `Server size:` sob o título `Instance configuratione` exibe os parâmetros rotulados `Key pair:` e `CIDR range:` sob o título `Security configuration`.
- Mapeamentos (opcional) - um mapeamento de chaves e valores associados que você pode usar para especificar valores de parâmetros condicionais, semelhante a uma tabela de pesquisa. Você pode associar uma chave a um valor correspondente usando a função FindInMap intrínseca Fn::

nas seções Recursos e Saídas. O modelo acima inclui uma lista de regiões da AWS a Imagem de máquina da Amazon (AMI) que corresponde a cada uma delas. O AWS Service Catalog usa o mapeamento para determinar qual AMI usar com base na região da AWS que o usuário seleciona no AWS Management Console.

- Recursos (obrigatório) — acumula recursos e suas propriedades. Você pode fazer referência a recursos nas seções Recursos e Saídas do modelo. No modelo acima, especificamos uma instância do EC2 executando o Amazon Linux e um grupo de segurança que permite acesso SSH à instância. A seção Propriedades do recurso da instância do EC2 usa as informações que o usuário digita para configurar o tipo de instância e um nome de chave para acesso ao SSH.

  O AWS CloudFormation usa a região da AWS atual para selecionar a ID da AMI nos mapeamentos definidos anteriormente e atribui um grupo de segurança a ele. O grupo de segurança é configurado para permitir acesso de entrada na porta 22 no intervalo de endereços IP do CIDR especificado pelo usuário.
- Saídas (opcional) - texto que informa ao usuário quando o lançamento do produto está concluído. O modelo fornecido obtém o nome DNS público da instância executada e o exibe para o usuário. O usuário precisa do nome DNS para conectar-se à instância usando SSH.

  Para obter mais informações sobre a página de anatomia do modelo, consulte Anatomia do modelo no Guia do usuário do AWS CloudFormation.

Etapa 2: criar um par de chaves

Para habilitar seus usuários finais a lançar o produto baseado no modelo de amostra para este tutorial, você deve criar um par de chaves do Amazon EC2. Um par de chaves é uma combinação de uma chave pública que é usada para criptografar dados e de uma chave privada que é usada para descriptografar dados. Para obter mais informações sobre pares de chaves, verifique se você está conectado ao AWS console e, em seguida, revise os pares de chaves do Amazon EC2 no Guia do usuário do Amazon EC2.

O AWS CloudFormation modelo deste tutorial,`development-environment.template`, inclui o `KeyName` parâmetro:

```
. . .
  "Parameters" : {
    "KeyName": {
```

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

Os usuários finais devem especificar o nome de um key pair AWS Service Catalog ao lançarem o produto baseado no modelo.

Se já tiver um par de chaves em sua conta que prefira usar, você poderá ir direto para Etapa 3: Criar um portfólio. Caso contrário, execute as etapas a seguir.

Para criar um par de chaves

1. Abra o console do Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, em Rede e segurança, selecione Pares de chaves.
3. Na página Key Pairs (Pares de chave), escolha Create Key Pair (Criar par de chave).
4. Em Key pair name (nome do par de chave), digite um nome que seja fácil de lembrar e, em seguida, escolha Create (Criar).
5. Quando o console solicitar que você salve o arquivo de chave privada, salve-o em um local seguro.

> **Important**
>
> Esta é a única chance de você salvar o arquivo de chave privada.

Etapa 3: Criar um portfólio

Para fornecer produtos aos usuários, comece criando um portfólio para esses produtos.

Para criar um portfólio

1. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/.
2. No painel de navegação à esquerda, escolha Portfólios e Criar portfólio.
3. Digite os seguintes valores:
   - Portfolio name – **`Engineering Tools`**

- Descrição do portfólio — **`Sample portfolio that contains a single product.`**
- Proprietário — **`IT (it@example.com)`**

4. Escolha Create (Criar).

Etapa 4: Criar um novo produto no portfólio

Depois de criar um portfólio, você estará pronto para criar um produto dentro do portfólio. Para este tutorial, você criará um produto chamado Linux Desktop, um ambiente de desenvolvimento na nuvem que é executado no Amazon Linux, dentro do portfólio Ferramenta de Engenharia.

Para criar um produto dentro de um portfólio

1. Se você acabou de concluir a etapa anterior, a página Portfolios já estará exibida. Caso contrário, abra https://console.aws.amazon.com/servicecatalog/.
2. Escolha e abra o portfólio da Ferramenta de Engenharia que você criou na Etapa 2.
3. Escolha Fazer upload de novo produto.
4. Na página Criar produto, na seção Detalhes do produto, insira o seguinte:
   - Nome do produto – **`Linux Desktop`**
   - Descrição do produto - **`Cloud development environment configured for engineering staff. Runs AWS Linux.`**
   - Proprietário - **`IT`**
   - Distribuidor — (em branco)
5. Na página Detalhes da versão, escolha Usar um CloudFormation modelo. Em seguida, escolha Especificar uma URL de modelo do Amazon S3 e insira o seguinte:
   - Select template - **`https://awsdocs.s3.amazonaws.com/servicecatalog/development-environment.template`**
   - Título da versão - **`v1.0`**
   - Description (Descrição): **`Base Version`**
6. Na seção Detalhes de suporte, insira o seguinte:
   - Contato de e-mail - **`ITSupport@example.com`**
   - Link de suporte — **`https://wiki.example.com/IT/support`**

- Descrição do suporte - **`Contact the IT department for issues deploying or connecting to this product.`**

7. Escolha Criar produto.

Etapa 5: Adicionar uma restrição de modelo para limitar o tamanho da instância

As restrições adicionam outra camada de controle sobre os produtos no portfólio. As restrições podem controlar o contexto de lançamento de um produto (restrições de lançamento) ou adicionar regras ao modelo do AWS CloudFormation (restrições de modelo). Para ter mais informações, consulte Uso de restrições do AWS Service Catalog.

Adicione uma restrição de modelo ao produto Linux Desktop que impede que os usuários selecionem tipos de instâncias grandes no momento do lançamento. O modelo do ambiente de desenvolvimento permite que o usuário selecione seis tipos de instância; esta restrição limita os tipos de instância válidos a dois tipos menores: `t2.micro` e `t2.small`. Para obter mais informações, consulte Instâncias T2 no Guia do usuário do Amazon EC2.

Adicionar uma restrição de modelo ao produto Linux Desktop

1. Na página Detalhes do portfólio, escolha a guia Restrições e escolha Criar restrição.
2. Na página Criar restrição, em Produto, escolha Linux Desktop. Em seguida, para Tipo de restrição, escolha Modelo.
3. Na seção Restrição de modelo, escolha Editor de texto.
4. Cole o seguinte conteúdo no editor:

```
{
  "Rules": {
    "Rule1": {
      "Assertions": [
        {
          "Assert" : {"Fn::Contains": [["t2.micro", "t2.small"], {"Ref":
 "InstanceType"}]},
          "AssertDescription": "Instance type should be t2.micro or t2.small"
        }
      ]
    }
  }
```

```
}
```

5. Em Descrição da restrição, insira **`Small instance sizes`**.
6. Escolha Create (Criar).

Etapa 6: Adicionar uma restrição de lançamento para atribuir um perfil do IAM

Uma restrição de lançamento designa um perfil do IAM que o AWS Service Catalog assume quando um usuário final lança um produto.

Para essa etapa, você adicionará uma restrição de lançamento ao produto Linux Desktop para que o AWS Service Catalog use os recursos do IAM que fazem parte do modelo do AWS CloudFormation do produto.

O perfil do IAM que você atribui a um produto como restrição de lançamento deve ter as seguintes permissões:

1. AWS CloudFormation
2. Os serviços usados no modelo do AWS CloudFormation para o produto
3. Leia o acesso ao modelo AWS CloudFormation em um bucket Amazon S3 de propriedade do serviço.

Esta restrição de lançamento permitirá que o usuário final lance o produto e, depois, gerencie-o como um produto provisionado. Para ver mais informações, consulte Restrições de lançamento do AWS Service Catalog.

Sem uma restrição de lançamento, seria necessário conceder permissões adicionais do IAM aos usuários finais para que pudessem usar o produto Linux Desktop. Por exemplo, a política `ServiceCatalogEndUserAccess` concede as permissões mínimas do IAM necessárias para acessar a visualização de console do usuário final do AWS Service Catalog.

Usar uma restrição de lançamento permite que você siga as melhores práticas do IAM de manter as permissões do IAM do usuário final no mínimo. Para obter mais informações, consulte Conceder privilégio mínimo no Guia do usuário do IAM.

Para adicionar uma restrição de lançamento

1. Siga as instruções para Criar novas políticas na guia JSON no Guia do Usuário do IAM.
2. Cole o seguinte documento da política JSON:

   - `cloudformation` — concede ao AWS Service Catalog permissões completas para criar, ler, atualizar, excluir, listar e marcar pilhas AWS CloudFormation.
   - `ec2` — concede ao AWS Service Catalog permissões completas para listar, ler, gravar, provisionar e marcar recursos do Amazon Elastic Compute Cloud (Amazon EC2) que fazem parte do produto AWS Service Catalog. Dependendo do recurso da AWS que você deseja implantar, essa permissão pode mudar.
   - `ec2` — cria uma nova política gerenciada para sua conta da AWS e anexa a política gerenciada especificada ao perfil do IAM especificado.
   - `s3` — permite acesso aos buckets do Amazon S3 de propriedade do AWS Service Catalog. Para implantar o produto, AWS Service Catalog é necessário acesso aos artefatos de provisionamento.
   - `servicecatalog` — concede ao AWS Service Catalog permissões para listar, ler, gravar, marcar e iniciar recursos em nome do usuário final.
   - `sns` — concede ao AWS Service Catalog permissões para listar, ler, escrever e marcar tópicos do Amazon SNS para a restrição de lançamento.

> **Note**
>
> Dependendo dos recursos subjacentes que você deseja implantar, talvez seja necessário modificar o exemplo de política 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. Escolha Próximo, Tags.
4. Escolha Próximo, Revisar.
5. Na página Revisar política, para o Nome , insira**`linuxDesktopPolicy`** .
6. Escolha Criar política.
7. No painel de navegação, escolha Perfis. Então escolha Criar perfil e faça o seguinte:
   a. Em Selecionar entidade confiável, escolha AWSserviço e, em Caso de uso para outros serviços da AWS, escolha Service Catalog. Selecione o caso de uso Service Catalog e depois escolha Próximo.
   b. Pesquise a linuxDesktopPolicypolítica e marque a caixa de seleção.
   c. Escolha Próximo.
   d. Em Role name, insira **`linuxDesktopLaunchRole`**.
   e. Selecione Criar perfil.
8. Abra o AWS Service Catalog console em https://console.aws.amazon.com/servicecatalog.

9. Escolha o portfólio Engineering Tools.
10. Na página Detalhes do portfólio, escolha a guia Restrições e escolha Criar restrição.
11. Em Produto, escolha Linux Desktop, e escolha Lançamento como Tipo de restrição.
12. Escolha Selecionar perfil do IAM. Em seguida, escolha linuxDesktopLaunchFunção e, em seguida, escolha Criar.

Etapa 7: Conceder acesso ao portfólio a usuários finais

Agora que você criou um portfólio e adicionou um produto, já está pronto para conceder acesso aos usuários finais.

Pré-requisitos

Se você não tiver criado um grupo do IAM para os usuários finais, consulte Conceder permissões a usuários finais do AWS Service Catalog.

Para dar acesso ao portfólio

1. Na página de detalhes do portfólio, escolha a guia Acesso.
2. Escolha Conceder acesso.
3. Na guia Grupos, marque a caixa de seleção referente ao grupo IAM para os usuários finais.
4. Escolha Adicionar acesso.

Etapa 8: Testar a experiência do usuário final

Para verificar se o usuário final pode acessar a visualização do console do usuário final e lançar seu produto com êxito, faça login na AWS como o usuário final e execute estas tarefas.

Para verificar se o usuário final pode acessar o console de usuário final

1. Siga as instruções para Fazer login como usuário IAM no Guia do usuário do IAM.
2. Na barra de menus, escolha a região da AWS em que você criou o portfólio `Engineering Tools`. Para este tutorial, escolha us-east-1 region.
3. Abra o console do AWS Service Catalog em https://console.aws.amazon.com/servicecatalog/ para ver:

   - Products – os produtos que o usuário pode usar.

- Provisioned products – os produtos provisionados que o usuário lançou.

Para verificar se o usuário final pode lançar o produto Linux Desktop

Para este tutorial, escolha us-east-1 region.

1. Na seção Produtos do console, escolha Linux Desktop.
2. Escolha Lançar produto para iniciar o assistente que configura seu produto.
3. Na página Lançar: Linux Desktop, insira **`Linux-Desktop`** para o nome do produto provisionado.
4. Na página Parâmetros, insira o seguinte e escolha Próximo:
   - Tamanho do servidor - escolha **`t2.micro`**.
   - Key pair – selecione o par de chaves que você criou em Etapa 2: criar um par de chaves.
   - CIDR range – digite um intervalo CIDR válido para o endereço IP do qual você se conectará à instância. Pode ser o valor padrão (0.0.0.0/0) para permitir acesso por meio de qualquer endereço IP, seu endereço IP seguido de **`/32`** para restringir o acesso a seu endereço IP apenas ou algo entre essas duas opções.
5. Escolha Lançar produto para lançar a pilha. O console exibe a página de detalhes da pilha do Linux-Desktop. O status inicial do produto é Em alteração. O AWS Service Catalog demora vários minutos para lançar o produto. Para ver o status atual, atualize o navegador. Depois que o produto for lançado, o status será Disponível.

Conceitos básicos de um produto Terraform

AWS Service Catalogpermite o provisionamento rápido e de autoatendimento com governança para suas configurações internas do HashiCorp Terraform. AWS Você pode usar o AWS Service Catalog como uma ferramenta única para organizar, controlar e distribuir suas configurações do Terraform em escala dentro do AWS. O AWS Service Catalog oferece suporte ao Terraform em vários recursos principais, incluindo catalogação de modelos Terraform padronizados e pré-aprovados, controle de acesso, controle de versão, marcação e compartilhando com outras contas do AWS. Em AWS Service Catalog, seus usuários finais veem uma lista simples de produtos e versões aos quais têm acesso e, em seguida, podem implantar esses produtos em uma única ação.

> **Note**
>
> Para continuar com o suporte às HashiCorp tecnologias, como resultado das recentes mudanças de licenciamento no Terraform, AWS Service Catalog alterei todas as referências anteriores do Terraform Open Source para External. O tipo de produto External inclui suporte para Terraform Community Edition, anteriormente conhecido como Terraform Open Source. Para obter mais informações e instruções sobre como migrar seus produtos existentes do Terraform Open Source e produtos provisionados para o tipo de produto externo, revise Atualizar os produtos existentes do Terraform Open Source e dos produtos provisionados para o tipo de produto External.

As etapas do tutorial a seguir ajudarão você a começar a usar um produto Terraform em AWS Service Catalog.

Como administrador do catálogo, você trabalha em uma conta de administrador central (conta hub). Os produtos Terrafrm Community Edition e Terraform Cloud requerem um mecanismo de provisionamento Terraform, sobre o qual você pode aprender mais em Mecanismo de provisionamento para Terraform Community Edition (tipo de produto External) e Mecanismo de provisionamento para Terraform Cloud .

Durante o tutorial, execute as seguintes tarefas na conta do administrador:

- Crie um produto Terraform usando o tipo de produto Terraform Cloud ou External. O Service Catalog usa o tipo de produto External para oferecer suporte aos produtos Terraform Community Edition.
- Associar um produto a um portfólio
- Crie uma restrição de lançamento para permitir que seus usuários finais provisionem o produto
- Etiquetar o produto
- Compartilhe o portfólio e o produto Terraform com a conta do usuário final (conta spoke)

Neste tutorial, você compartilha um portfólio usando a opção de compartilhamento da organização a partir da conta de administrador (conta hub), que também é a conta de gerenciamento da organização. Para mais informações sobre o compartilhamento organizacional, consulte Compartilhar um portfólio.

O recurso AWS contido no produto Terraform que você cria no tutorial é um bucket simples do Amazon S3.

> **Note**
>
> Antes de começar, conclua os itens de ação em Configuração AWS Service Catalog.

Tópicos

Atualizar os produtos existentes do Terraform Open Source e dos produtos provisionados para o tipo de produto External

Para continuar com o suporte às HashiCorp tecnologias, como resultado das recentes mudanças de licenciamento no Terraform, AWS Service Catalog alterei todas as referências anteriores do Terraform Open Source para External. O tipo de produto External inclui suporte para Terraform Community Edition, anteriormente conhecido como Terraform Open Source. AWS Service Catalog não oferece mais suporte ao Terraform Open Source como um tipo de produto válido para novos produtos ou produtos provisionados. Você só pode atualizar ou encerrar recursos existentes do Terraform Open Source, incluindo versões de produtos e produtos provisionados.

Se ainda não tiver feito isso, você deverá fazer a transição de todos os produtos Terraform Open Source existentes e produtos provisionados para produtos External, seguindo as instruções nesta seção.

1. Atualize seu Terraform Reference Engine existente AWS Service Catalog para incluir suporte para os tipos de produtos External e Terraform Open Source. Para obter instruções sobre como atualizar seu Terraform Reference Engine, consulte nosso GitHub Repositório.
2. Recrie qualquer produto Terraform Open Source existente usando o novo tipo de produto Externo.
3. Exclua todos os produtos existentes que usam o tipo de produto Terraform Open Source.
4. Reprovisione esses recursos usando o novo tipo de produto External.
5. Exclua todos os produtos existentes que usam o tipo de produto Terraform Open Source.

Após fazer a transição dos produtos existentes, use o tipo de produto External para quaisquer novos produtos que usem um arquivo de configuração tar.gz.

A AWS Service Catalog apoiará os clientes nessa mudança, conforme necessário. Se essas alterações exigirem um grande esforço para sua conta ou impactarem workloads críticas do produto, entre em contato com o representante da sua conta para solicitar assistência.

Pré-requisito: Configurar seu mecanismo de provisionamento do Terraform

Como pré-requisito para criar produtos Terraform no AWS Service Catalog, você deve instalar e configurar um mecanismo de provisionamento em sua conta de administrador do Service Catalog (conta hub). O mecanismo de provisionamento é necessário para produtos Terraform Community Edition (usando o tipo de produto External) e produtos Terraform Cloud (usando o tipo de produto Terraform Cloud).

> **Note**
>
> A configuração do mecanismo é uma configuração única que leva aproximadamente 30 minutos.

Mecanismo de provisionamento para Terraform Community Edition (tipo de produto External)

O AWS Service Catalog usa o tipo de produto External para oferecer suporte a produtos Terraform Community Edition. O tipo de produto External também oferece suporte a outras ferramentas de provisionamento, incluindo Pulumi, Ansible, Chef e outras, com base na configuração do mecanismo de provisionamento.

Para AWS Service Catalog produtos que usam o tipo de produto externo com HashiCorp o Terraform Community Edition, você deve instalar e configurar um mecanismo de provisionamento do Terraform em sua conta de AWS Service Catalog administrador (conta hub). AWSgerencia esse mecanismo e seus recursos.

AWS Service Catalogfornece um GitHub repositório com instruções sobre como instalar e configurar o mecanismo de provisionamento Terraform AWS fornecido. O repositório inclui as seguintes informações:

- Ferramentas de instalação necessárias
- Criação do código
- Implantação em uma conta da AWS
- Informações adicionais sobre fluxos de trabalho de provisionamento, garantia de qualidade e limitações

Mecanismo de provisionamento para Terraform Cloud

Para AWS Service Catalog produtos que usam o tipo de produto Terraform Cloud com HashiCorp o Terraform Cloud, você deve instalar e configurar um mecanismo de provisionamento do Terraform em sua conta de AWS Service Catalog administrador (conta hub). HashiCorp gerencia esse mecanismo em um ambiente remoto.

HashiCorp fornece um GitHub repositório com instruções sobre como configurar o mecanismo Terraform Cloud para. AWS Service Catalog O repositório inclui as seguintes informações:

- Ferramentas de instalação necessárias
- Criação do código
- Implantação em uma conta da AWS

- Informações adicionais sobre fluxos de trabalho de provisionamento, garantia de qualidade e limitações

Etapa 1: Baixar o arquivo de configuração do Terraform

Você pode usar um arquivo de configuração do Terraform para criar e provisionar produtos do HashiCorp Terraform. Essas configurações são arquivos de texto sem formatação e descrevem os recursos que você deseja provisionar. Você pode usar o editor de texto de sua preferência para criar, atualizar e salvar configurações. Para a criação do produto, você deve carregar as configurações do Terraform como um arquivo tar.gz. Neste tutorial, AWS Service Catalog fornece um arquivo de configuração simples para que você possa começar. A configuração cria um bucket do Amazon S3.

Baixar o arquivo de configuração

AWS Service Catalog fornece um exemplo `simple-s3-bucket.tar.gz` de arquivo de configuração para você usar neste tutorial.

Visão geral do arquivo de configuração

O texto do arquivo de configuração de amostra é o seguinte:

```
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
}
```

Recursos de configuração

O arquivo de configuração declara os recursos a serem criados quando o AWS Service Catalog provisionar o produto. Consiste nas seguintes seções:

- Variável (opcional) - as definições de valor que um usuário administrador (administrador da conta do hub) pode atribuir para personalizar a configuração. As variáveis fornecem uma interface consistente para alterar o comportamento de uma determinada configuração. O rótulo após a palavra-chave variável é um nome para a variável, que deve ser exclusiva entre todas as variáveis no mesmo módulo. Esse nome é usado para atribuir um valor externo à variável e para referenciar o valor da variável de dentro do módulo.
- Provedor (opcional) - o provedor de serviços em nuvem para provisionamento de recursos, que é `AWS`. AWS Service Catalog só oferece suporte da `AWS` como provedor. Como resultado, o mecanismo de provisionamento do Terraform substitui qualquer outro provedor listado da `AWS`.
- Recurso (obrigatório) - o recurso de infraestrutura da AWS para provisionamento. Para este tutorial, o arquivo de configuração do Terraform especifica o Amazon S3.
- Saída (opcional) - as informações ou valores retornados, semelhantes aos valores retornados em uma linguagem de programação. Você pode usar dados de saída para configurar o fluxo de trabalho da infraestrutura com ferramentas de automação.

Etapa 2: Crie um produto do Terraform

Depois de instalar o mecanismo de provisionamento do Terraform, você está pronto para criar um produto HashiCorp Terraform no. AWS Service Catalog Neste tutorial, você criará um produto do Terraform contendo um bucket do Amazon S3 simples.

Para criar um novo produto do Terraform.

1. Abra o console do AWS Service Catalog em https://console.aws.amazon.com/servicecatalog/ e faça login como usuário administrador.
2. Navegue até a seção Administração e escolha Lista de produtos.
3. Escolha Criar produto.
4. Na página Criar produto, na seção Detalhes do produto, escolha o tipo de produto External ou Terraform Cloud. O Service Catalog usa o tipo de produto External para oferecer suporte aos produtos Terraform Community Edition.
5. Insira os seguintes detalhes do produto:
   - Nome do produto – **`Simple S3 bucket`**
   - Descrição do produto — Produto do Terraform contendo um bucket Amazon S3.
   - Proprietário - **`IT`**

- Distribuidor — (em branco)

6. No painel Detalhes da versão, escolha Fazer upload um arquivo de modelo, escolha Selecionar arquivo. Selecione o arquivo que você baixou em Etapa 1: Baixar o arquivo de configuração do Terraform.
7. Insira o seguinte:
   - Nome da versão — **`v1.0`**
   - Descrição da versão — **`Base Version`**
8. Na seção Detalhes do suporte, insira o seguinte e escolha Criar produto.
   - Contato de e-mail — **`ITSupport@example.com`**
   - Link de suporte — **`https://wiki.example.com/IT/support`**
   - Descrição do suporte - **`Contact the IT department for issues deploying or connecting to this product.`**
9. Escolha Criar produto.

Depois de criar o produto com sucesso, AWS Service Catalog exibe um banner de confirmação na página do produto.

Etapa 3: Criar um portfólio do AWS Service Catalog

Você pode criar um portfólio em sua conta de administrador de AWS Service Catalog (conta hub) para facilitar a organização e distribuição do produto para contas de usuários finais (contas spoke).

Para criar um portfólio

1. Abra o console do AWS Service Catalog em https://console.aws.amazon.com/servicecatalog/ e faça login como administrador.
2. No painel de navegação à esquerda, escolha Portfólios e Criar portfólio.
3. Insira os seguintes valores:
   - Portfolio name – **`S3 bucket`**
   - Descrição do portfólio — **`Sample portfolio for Terraform configurations.`**
   - Proprietário — **`IT (it@example.com)`**
4. Escolha Create (Criar).

Etapa 4: Adicionar produto ao portfólio

Depois de criar um portfólio, você pode adicionar o produto HashiCorp Terraform que você criou na Etapa 2.

Para adicionar um produto a um portfólio

1. Navegue até a página Lista de produtos.
2. Selecione o produto Terraform do bucket S3 simples que você criou na Etapa 2 e escolha Ações. No menu suspenso, escolha Adicionar produto ao portfólio. AWS Service Catalog exibe o painel Adicionar bucket S3 simples ao portfólio.
3. Selecione o portfólio de buckets S3 e, em seguida, desative Criar restrição de lançamento. Você criará a restrição de lançamento posteriormente no tutorial.
4. Escolha Adicionar produto ao portfólio.

Depois de criar o produto ao portfólio com sucesso, AWS Service Catalog exibe um banner de confirmação na página de Lista do produto.

Etapa 5: Criar funções de lançamento

Nesta etapa, você criará uma função do IAM (função de lançamento) especificando as permissões que o mecanismo de provisionamento do Terraform AWS Service Catalog pode assumir quando um usuário final lança um produto Terraform. HashiCorp

O perfil do IAM (função de inicialização) que você atribui posteriormente ao seu produto Terraform de bucket simples do Amazon S3 como uma restrição de inicialização deve ter as seguintes permissões:

- Acesso aos recursos da AWS subjacentes do seu produto Terraform. Neste tutorial, isso inclui acesso às operações `s3:CreateBucket*`, `s3:DeleteBucket*`, `s3:Get*`, `s3:List*` e `s3:PutBucketTagging` do Amazon S3.
- Acesso de leitura ao modelo do Amazon S3 em um bucket do Amazon S3 de propriedade do AWS Service Catalog
- Acesso às operações `CreateGroup`, `ListGroupResources`, `DeleteGroup` e `Tag` do grupo de recursos. Essas operações permitem ao AWS Service Catalog gerenciar grupos de recursos e tags.

Para criar uma função de lançamento na conta do administrador AWS Service Catalog

1. Enquanto estiver conectado à conta do administrador do AWS Service Catalog, siga as instruções para Criar novas políticas na guia JSON no Guia do Usuário do IAM.
2. Crie uma política para seu produto simples do Amazon S3 bucket Terraform. Essa política deve ser criada antes de você criar o perfil de lançamento e consiste nas seguintes permissões:

   - `s3` — concede ao AWS Service Catalog permissões completas para listar, ler, gravar, provisionar e marcar o produto Amazon S3.
   - `s3` — permite acesso aos buckets do Amazon S3 de propriedade do AWS Service Catalog. Para implantar o produto, AWS Service Catalog é necessário acesso aos artefatos de provisionamento.
   - `resourcegroups` — permite ao AWS Service Catalog criar, listar, excluir e marcar AWS Resource Groups.
   - `tag` — concede ao AWS Service Catalog permissões de marcação.

   > **Note**
   >
   > Dependendo dos recursos subjacentes que você deseja implantar, talvez seja necessário modificar o exemplo de política JSON.

   Cole o seguinte documento da política JSON:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3:ExistingObjectTag/servicecatalog:provisioning": "true"
                }
            }
        },
```

```
        {
            "Action": [
                "s3:CreateBucket*",
                "s3:DeleteBucket*",
                "s3:Get*",
                "s3:List*",
                "s3:PutBucketTagging"
            ],
            "Resource": "arn:aws:s3:::*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "resource-groups:CreateGroup",
                "resource-groups:ListGroupResources",
                "resource-groups:DeleteGroup",
                "resource-groups:Tag"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "tag:GetResources",
                "tag:GetTagKeys",
                "tag:GetTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

3. a. Escolha Próximo, Tags.

   b. Escolha Próximo, Revisar.

   c. Na página Revisar política, para o Nome , insira**`S3ResourceCreationAndArtifactAccessPolicy`** .

   d. Escolha Criar política.

4. No painel de navegação, escolha Roles (Funções) e Criar função.

5. Em Selecionar entidade confiável, escolha Política de confiança personalizada e, em seguida, insira a seguinte política JSON:

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

6. Escolha Próximo.
7. Na lista Políticas, selecione a `S3ResourceCreationAndArtifactAccessPolicy` que você criou.
8. Escolha Próximo.
9. Em Nome do perfil, insira **`SCLaunch-S3product`**.

> **Important**
>
> Os nomes do perfil de lançamento devem começar com “SCLaunch” seguido pelo nome do perfil desejado.

10. Selecione Criar perfil.

> **Important**
>
> Depois de criar a função de lançamento na sua conta de administrador AWS Service Catalog, você também deve criar uma função de lançamento idêntico na conta do usuário final do AWS Service Catalog. O perfil na conta do usuário final deve ter o mesmo nome e incluir a mesma política do perfil na conta do administrador.

Para criar uma função de lançamento na conta do usuário final AWS Service Catalog

1. Faça login como administrador na conta do usuário final e siga as instruções para Criar novas políticas na guia JSON no Guia do Usuário do IAM.
2. Repita as etapas 2 a 10 de Para criar uma função de lançamento na conta de administrador AWS Service Catalog acima.

> **Note**
>
> Ao criar uma função de lançamento na conta do usuário final AWS Service Catalog, certifique-se de usar o mesmo administrador **`AccountId`** na política de confiança personalizada.

Agora que você criou uma função de lançamento nas contas de administrador e usuário final, pode adicionar uma restrição de lançamento ao produto.

Etapa 6: Adicionar uma restrição de lançamento ao seu produto Terraform

> **Important**
>
> Você deve criar uma restrição de lançamento para os produtos HashiCorp Terraform. Sem uma restrição de lançamento, os usuários finais não podem provisionar o produto.

Depois de criar uma função de lançamento em sua conta de administrador, você estará pronto para associar a função de lançamento a uma restrição de lançamento em seu produto External ou Terraform Cloud.

Esta restrição de lançamento permitirá que o usuário final lance o produto e, depois, gerencie-o como um produto provisionado. Para ver mais informações, consulte Restrições de lançamento do AWS Service Catalog.

Usar uma restrição de lançamento permite que você siga as melhores práticas do IAM de manter as permissões do IAM do usuário final no mínimo. Para obter mais informações, consulte Conceder privilégio mínimo no Guia do usuário do IAM.

Para atribuir uma restrição de lançamento ao produto

1. Abra o AWS Service Catalog console em https://console.aws.amazon.com/servicecatalog.
2. Escolha Portfólios no console de navegação à esquerda.
3. Escolha o portfólio de bucket S3.
4. Na página Detalhes do portfólio, escolha a guia Restrições e escolha Criar restrição.
5. Em Produto, escolha bucket S3 simples. AWS Service Catalog seleciona automaticamente o tipo de restrição Lançamento.
6. Escolha Inserir nome do perfil e, em seguida, SCLaunch-S3Product.
7. Escolha Criar.

> **Note**
>
> O nome do perfil fornecido deve existir na conta que criou a restrição de lançamento e a conta do usuário que executa um produto com essa restrição de lançamento.

Etapa 7: Conceder acesso ao usuário final

Depois de aplicar a restrição de lançamento ao seu produto HashiCorp Terraform, você está pronto para conceder acesso aos usuários finais na conta spoke.

Neste tutorial, você concede acesso a usuários finais usando o compartilhamento de nomes da entidade principal. Os nomes da entidade principal são nomes de grupos, perfis e usuários que os administradores podem especificar em um portfólio e depois compartilhar com o portfólio. Quando você compartilha o portfólio, AWS Service Catalog verifique se esses Nomes de Entidades principais já existem. Se existirem, AWS Service Catalog associa automaticamente as entidades principais correspondentes do IAM ao portfólio compartilhado para conceder acesso aos usuários finais. Consulte Compartilhamento de um portfólio para obter mais informações.

Pré-requisitos

Se você não tiver criado um grupo do IAM para os usuários finais, consulte Conceder permissões a usuários finais do AWS Service Catalog.

Para dar acesso ao portfólio

1. Navegue até a página Portfólio e escolha o portfólio bucket S3.
2. Escolha a guia Acesso e, em seguida, escolha Conceder acesso.
3. No painel Tipo de acesso, escolha Nome da entidade principal.
4. No painel Nome da entidade principal, selecione o tipo de Nome da entidade principal e, em seguida, insira o Nome da entidade principal do usuário final desejado na conta spoke.
5. Escolha Conceder acesso.

Etapa 8: Compartilhar portfólio com o usuário final

O AWS Service Catalog administrador pode distribuir portfólios com contas de usuários finais usando account-to-account compartilhamento ou AWS Organizations compartilhamento. Neste tutorial, você está compartilhando seu portfólio com a organização a partir da conta de administrador (conta hub), que também é a conta de gerenciamento da organização.

Para compartilhar o portfólio da conta do hub de administração

1. Abra o AWS Service Catalog console em https://console.aws.amazon.com/servicecatalog/.

2. Na página Portfólios, selecione o portfólio de bucket do S3. No menu Ações, escolha Compartilhar.
3. Escolha AWS Organizations e, em seguida, filtre em sua estrutura organizacional.
4. No painel Organização da AWS, escolha a conta do usuário final (conta spoke).

   Você também pode selecionar um nó raiz para compartilhar o portfólio com toda a organização, uma Unidade Organizacional (UO) principal ou uma UO secundária dentro da sua organização com base na estrutura da sua organização. Para obter mais informações, consulte Compartilhar um portfólio.
5. No painel Configurações de compartilhamento, escolha Compartilhamento da entidade principal.
6. Escolha Compartilhar.

Depois de compartilhar com sucesso o portfólio com os usuários finais, a próxima etapa é verificar a experiência do usuário final e provisionar o produto Terraform.

Etapa 9: Testar a experiência do usuário final

Para verificar se os usuários finais podem acessar a visualização do console do usuário final e lançar seu produto **`Simple S3 bucket`** com êxito, faça login na AWS como o usuário final e execute estas tarefas.

Para verificar se o usuário final pode acessar o console de usuário final

- Abra o console do AWS Service Catalog em https://console.aws.amazon.com/servicecatalog/ para ver:
  - Products – os produtos que o usuário pode usar.
  - Provisioned products – os produtos provisionados que o usuário lançou.

Para verificar se o usuário final pode iniciar o produto Terraform

1. Na seção Produtos do console, escolha bucket S3 simples.
2. Escolha Lançar produto para iniciar o assistente que configura seu produto.
3. Na página Lançar bucket S3 simples, insira **`Amazon S3 product`** para o nome do produto provisionado.
4. Na página Parâmetros, insira o seguinte e escolha Próximo:

- bucket_name - forneça um nome exclusivo para o bucket do Amazon S3. Por exemplo, **`terraform-s3-product`**.

5. Escolha Lançar produto. O console exibe a página de detalhes da pilha para o lançamento do produto Amazon S3. O status inicial do produto é Em alteração. O AWS Service Catalog demora vários minutos para lançar o produto. Para ver o status atual, atualize o navegador. Após o lançamento bem-sucedido do produto, o status é Disponível.

   AWS Service Catalog cria um novo bucket do Amazon S3 chamado **`terraform-s3-product`**.

Etapa 10: Monitorar as operações de provisionamento do Terraform

Se quiser monitorar as operações de provisionamento, você pode revisar os CloudWatch registros da Amazon e qualquer fluxo de trabalho AWS Step Functions de provisionamento.

Há duas máquinas de estado para o fluxo de trabalho de provisionamento:

- `ManageProvisionedProductStateMachine` — AWS Service Catalog invoca essa máquina de estado ao provisionar um novo produto Terraform e ao atualizar um produto provisionado Terraform existente.
- `TerminateProvisionedProductStateMachine` — AWS Service Catalog invoca essa máquina de estado ao encerrar um produto provisionado existente do Terraform.

Para executar a máquina de monitoramento de estados

1. Abra o console de gerenciamento da AWS e faça login como administrador na conta do hub de administração em que o mecanismo de provisionamento do Terraform está instalado.
2. Abra o AWS Step Functions.
3. Na navegação à esquerda, escolha Máquinas de estado.
4. Escolha ManageProvisionedProductStateMachine.
5. Na lista Execuções, insira a ID do produto provisionado para localizar sua execução.

> **Note**
>
> AWS Service Catalog cria a ID do produto provisionado quando você provisiona o produto. A ID do produto provisionado é formatada da seguinte forma: **`pp-1111pwtn[ID number]`**.

6. Escolha a ID de execução.

Na página Detalhes da execução resultante, você pode visualizar todas as etapas do fluxo de trabalho de provisionamento. Você também pode revisar todas as etapas que falharam para identificar a causa da falha.

Segurança em AWS Service Catalog

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de uma arquitetura de data center e rede criada para atender aos requisitos das organizações mais sensíveis à segurança.

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

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa AWS os serviços na AWS nuvem. AWS também fornece serviços que você pode usar com segurança. Auditores de terceiros testam e verificam regularmente a eficácia da nossa segurança como parte dos Programas de conformidade da AWS.

  Para saber mais sobre os programas de conformidade que se aplicam a AWS Service Catalog, consulte AWS Serviços no escopo por programa de conformidade
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar AWS Service Catalog. Os tópicos a seguir mostram como configurar para atender AWS Service Catalog aos seus objetivos de segurança e conformidade. Você também conhecerá outros AWS serviços que o ajudarão a monitorar e proteger seus AWS Service Catalog recursos.

Tópicos

Proteção de dados em AWS Service Catalog

O modelo de responsabilidade AWS compartilhada modelo se aplica à proteção de dados em AWS Service Catalog. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as Perguntas Frequentes sobre Privacidade de Dados.. Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog AWS Shared Responsibility Model and GDPR no Blog de segurança da AWS .

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

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS disponíveis, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com AWS Service Catalog ou Serviços da AWS usa o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico.

Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Proteger dados com criptografia

Criptografia em repouso

AWS Service Catalog usa buckets Amazon S3 e bancos de dados Amazon DynamoDB que são criptografados em repouso usando chaves gerenciadas pela Amazon. Para saber mais, consulte as informações sobre criptografia em repouso fornecidas pelo Amazon S3 e pelo Amazon DynamoDB.

Criptografia em trânsito

AWS Service Catalog usa Transport Layer Security (TLS) e criptografia do lado do cliente das informações em trânsito entre o chamador e. AWS

Você pode acessar de forma privada as AWS Service Catalog APIs da sua Amazon Virtual Private Cloud (Amazon VPC) criando VPC endpoints. Com os VPC endpoints, o roteamento entre a VPC AWS Service Catalog é gerenciado pela AWS rede sem a necessidade de um gateway de internet, gateway NAT ou conexão VPN.

A última geração de VPC endpoints usada pelo AWS Service Catalog é alimentada por AWS PrivateLink, uma AWS tecnologia que permite a conectividade privada entre AWS serviços usando interfaces de rede elásticas com IPs privados em suas VPCs.

Gerenciamento de identidades e acesso no AWS Service Catalog

O acesso a AWS Service Catalog requer credenciais. Essas credenciais devem ter permissão para acessar AWS recursos, como um AWS Service Catalog portfólio ou produto. AWS Service Catalog se integra ao AWS Identity and Access Management (IAM) para permitir que você conceda AWS Service Catalog aos administradores as permissões necessárias para criar e gerenciar produtos e para conceder aos usuários AWS Service Catalog finais as permissões necessárias para lançar produtos e gerenciar produtos provisionados. Essas políticas são criadas e gerenciadas por administradores e usuários finais AWS ou individualmente por eles. Para controlar o acesso, você anexa essas políticas aos usuários, grupos e perfis você usa com o AWS Service Catalog.

Público

As permissões que você tem com AWS Identity and Access Management (IAM) pode depender do perfil que você desempenha no AWS Service Catalog.

As permissões que você tem por meio do AWS Identity and Access Management (IAM) podem depender do perfil que você tem no AWS Service Catalog.

Administrador - Como AWS Service Catalog administrador, você precisa de acesso total ao console do administrador e às permissões do IAM que permitem realizar tarefas como criar e gerenciar portfólios e produtos, gerenciar restrições e conceder acesso aos usuários finais.

Usuário final - Antes que seus usuários finais possam usar seus produtos, você precisa conceder a eles permissões que lhes dêem acesso ao console do usuário AWS Service Catalog final. Eles também podem ter permissões para executar produtos e gerenciar produtos provisionados.

Administrador do IAM – se você for um administrador do IAM, talvez queira saber detalhes sobre como pode gravar políticas para gerenciar o acesso ao AWS Service Catalog. Para ver exemplos de políticas AWS Service Catalog baseadas em identidade que você pode usar no IAM, consulte. the section called “AWS políticas gerenciadas”

Exemplos de políticas baseadas em identidade para AWS Service Catalog

Tópicos

Acesso ao console para usuários finais

As políticas **`AWSServiceCatalogEndUserFullAccess`** e **`AWSServiceCatalogEndUserReadOnlyAccess`** concedem acesso à visualização do console do usuário final do AWS Service Catalog . Quando um usuário que tem uma dessas políticas escolhe AWS Service Catalog no AWS Management Console, a visualização do console do usuário final exibe os produtos que ele tem permissão para lançar.

Antes que os usuários finais possam lançar com sucesso um produto AWS Service Catalog ao qual você concede acesso, você deve fornecer a eles permissões adicionais do IAM para permitir que eles usem cada um dos AWS recursos subjacentes no AWS CloudFormation modelo de um produto. Por exemplo, se um modelo de produto incluir o Amazon Relational Database Service (Amazon RDS), você deverá conceder permissões do Amazon RDS aos usuários para lançarem o produto.

Para saber como permitir que os usuários finais lancem produtos e, ao mesmo tempo, imponham permissões de acesso mínimo aos AWS recursos, consulte. the section called “Uso de restrições”

Se você aplicar a política **`AWSServiceCatalogEndUserReadOnlyAccess`**, seus usuários terão acesso ao console do usuário final, mas não terão as permissões necessárias para lançar produtos e gerenciar produtos provisionados. Você pode conceder essas permissões diretamente a um usuário final usando o IAM, mas se quiser limitar o acesso que os usuários finais têm aos AWS recursos, você deve anexar a política a uma função de lançamento. Em seguida, você usa AWS Service Catalog para aplicar a função de lançamento a uma restrição de lançamento do produto. Para obter mais informações sobre como aplicar uma função de lançamento, limitações de função de lançamento e uma função de lançamento de amostra, consulte Restrições de lançamento do AWS Service Catalog.

> **Note**
>
> Se você conceder aos usuários permissões de IAM para AWS Service Catalog administradores, a visualização do console do administrador será exibida em vez disso. Não conceda essas permissões aos usuários finais, a menos que você queira que eles tenham acesso à visualização do console do administrador.

Acesso ao produto para usuários finais

Antes que os usuários finais possam usar um produto ao qual você concede acesso, você deve fornecer a eles permissões adicionais do IAM para permitir que eles usem cada um dos AWS recursos subjacentes no AWS CloudFormation modelo de um produto. Por exemplo, se um modelo de produto incluir o Amazon Relational Database Service (Amazon RDS), você deverá conceder permissões do Amazon RDS aos usuários para lançarem o produto.

Se você aplicar a política **`AWSServiceCatalogEndUserReadOnlyAccess`**, seus usuários terão acesso à visualização do console do usuário final, mas não terão as permissões necessárias para lançar produtos e gerenciar produtos provisionados. Você pode conceder essas permissões diretamente a um usuário final no IAM, mas se quiser limitar o acesso que os usuários finais têm aos AWS recursos, você deve anexar a política a uma função de lançamento. Em seguida, você usa AWS Service Catalog para aplicar a função de lançamento a uma restrição de lançamento do produto. Para obter mais informações sobre como aplicar uma função de lançamento, limitações de função de lançamento e uma função de lançamento de amostra, consulte Restrições de lançamento do AWS Service Catalog.

Políticas de exemplo para gerenciamento de produtos provisionados

Você pode criar políticas personalizadas para ajudar a atender aos requisitos de segurança da organização. As seções a seguir descrevem como personalizar o nível de acesso para cada ação com suporte para níveis de usuário, função e conta. Você pode conceder acesso a usuários para visualizar, atualizar, encerrar e gerenciar produtos provisionados criados somente por esse usuário ou criados por outros sob sua função ou sob a conta à qual eles estão conectados. Esse acesso é hierárquico – a concessão de acesso em nível de conta também concede acesso em nível de perfil e em nível de usuário, enquanto que a adição de acesso em nível de perfil também concede acesso em nível de usuário, mas não concede acesso em nível de conta. Você pode especificar isso na política JSON usando um bloco `Condition` como `accountLevel`, `roleLevel` ou `userLevel`.

Esses exemplos também se aplicam aos níveis de acesso para operações de gravação de AWS Service Catalog API: `UpdateProvisionedProduct` e`TerminateProvisionedProduct`, e operações de leitura: `DescribeRecordScanProvisionedProducts`, `ListRecordHistory` e. As operações da API `ScanProvisionedProducts` e `ListRecordHistory` usam `AccessLevelFilterKey` como entrada, e os valores dessa chave correspondem aos níveis de bloco `Condition` abordado aqui (`accountLevel` equivale a um valor `AccessLevelFilterKey` para "Conta", `roleLevel` para "Função" e `userLevel` para "Usuário"). Para obter mais informações, consulte o Guia do Desenvolvedor do Service Catalog.

Exemplos

- Acesso completo de administrador a produtos provisionados
- Acesso de usuário final a produtos provisionados
- Acesso parcial de administrador a produtos provisionados

Acesso completo de administrador a produtos provisionados

A política a seguir permite acesso completo de leitura e gravação a produtos provisionados e registros no catálogo no nível de conta.

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

```
         ],
         "Resource":"*",
         "Condition": {
            "StringEquals": {
               "servicecatalog:accountLevel": "self"
            }
         }
      }
   ]
}
```

Essa política é funcionalmente equivalente à política a seguir:

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

Não especificar um `Condition` bloqueio em nenhuma política para AWS Service Catalog é tratado da mesma forma que especificar o acesso`"servicecatalog:accountLevel"`. Observe que o acesso `accountLevel` inclui o acesso `roleLevel` e `userLevel`.

Acesso de usuário final a produtos provisionados

A política a seguir restringe o acesso a operações de leitura e gravação somente aos produtos provisionados ou registros associados criados pelo usuário atual.

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

Acesso parcial de administrador a produtos provisionados

As duas políticas a seguir, se forem aplicadas ao mesmo usuário, permitem o que pode ser chamado de um tipo de "acesso de administrador parcial", fornecendo acesso de somente leitura completo e acesso de gravação limitado. Isso significa que o usuário pode ver qualquer produto provisionado ou registro associado na conta do catálogo, mas não pode executar nenhuma ação em qualquer produto provisionado ou registro que não seja de propriedade desse usuário.

A primeira política permite ao usuário acesso a operações de gravação nos produtos provisionados criados pelo usuário atual, mas não em produtos provisionados criados por outros usuários. A segunda política adiciona acesso completo a operações de leitura em produtos provisionados criados por todos (usuário, função ou conta).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "servicecatalog:DescribeProduct",
                "servicecatalog:DescribeProductView",
                "servicecatalog:DescribeProvisioningParameters",
```

```
                "servicecatalog:ListLaunchPaths",
                "servicecatalog:ProvisionProduct",
                "servicecatalog:SearchProducts",
                "servicecatalog:TerminateProvisionedProduct",
                "servicecatalog:UpdateProvisionedProduct"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "servicecatalog:userLevel": "self"
                }
            }
        }
    ]
}
```

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

AWS políticas gerenciadas para AWS Service Catalog AppRegistry

AWS política gerenciada: **AWSServiceCatalogAdminFullAccess**

Você pode anexar `AWSServiceCatalogAdminFullAccess` às suas entidades do IAM. AppRegistry também anexa essa política a uma função de serviço que permite AppRegistry realizar ações em seu nome.

Essa política concede permissões *`administrativas`* que permitem acesso total à visualização do console do administrador e concede permissão para criar e gerenciar produtos e portfólios.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `servicecatalog`— Permite aos diretores permissões completas para a visualização do console do administrador e a capacidade de criar e gerenciar portfólios e produtos, gerenciar restrições, conceder acesso aos usuários finais e realizar outras tarefas administrativas internas. AWS Service Catalog
- `cloudformation`— Permite permissões AWS Service Catalog completas para listar, ler, gravar e marcar AWS CloudFormation pilhas.
- `config`— Permite permissões AWS Service Catalog limitadas para portfólios, produtos e produtos provisionados via. AWS Config
- `iam` – concede às entidades principais permissões completas para visualizar e criar usuários, grupos ou perfis do serviço que são necessários para criar e gerenciar produtos e portfólios.
- `ssm`— AWS Service Catalog Permite AWS Systems Manager listar e ler documentos do Systems Manager na AWS conta corrente e AWS na região.

Veja a política: AWSServiceCatalogAdminFullAccess.

AWS política gerenciada: **AWSServiceCatalogAdminReadOnlyAccess**

Você pode anexar `AWSServiceCatalogAdminReadOnlyAccess` às suas entidades do IAM. AppRegistry também anexa essa política a uma função de serviço que permite AppRegistry realizar ações em seu nome.

Esta política concede permissões *`somente leitura`* que oferecem acesso completo à visualização do console do administrador. Esta política não concede acesso para criar ou gerenciar produtos e portfólios.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `servicecatalog` – concede às entidades principais permissões somente de leitura na visualização do console do administrador.
- `cloudformation`— Permite permissões AWS Service Catalog limitadas para listar e ler AWS CloudFormation pilhas.
- `config`— Permite permissões AWS Service Catalog limitadas para portfólios, produtos e produtos provisionados via. AWS Config
- `iam` – concede às entidade principais permissões limitadas para visualizar usuários, grupos ou perfis do serviço que são necessários para criar e gerenciar produtos e portfólios.
- `ssm`— AWS Service Catalog Permite AWS Systems Manager listar e ler documentos do Systems Manager na AWS conta corrente e AWS na região.

Veja a política: AWSServiceCatalogAdminReadOnlyAccess.

AWS política gerenciada: **`AWSServiceCatalogEndUserFullAccess`**

Você pode anexar `AWSServiceCatalogEndUserFullAccess` às suas entidades do IAM. AppRegistry também anexa essa política a uma função de serviço que permite AppRegistry realizar ações em seu nome.

Essa política concede ao *`colaborador`* permissões que concedem acesso total à visualização do console do usuário final e concede permissão para lançar produtos e gerenciar produtos provisionados.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `servicecatalog` – concede às entidades principais permissões completas à visualização do console do usuário final e a habilidade de lançar produtos e gerenciar produtos provisionados.
- `cloudformation`— Permite permissões AWS Service Catalog completas para listar, ler, gravar e marcar AWS CloudFormation pilhas.
- `config`— Permite permissões AWS Service Catalog limitadas para listar e ler detalhes sobre portfólios, produtos e produtos provisionados via. AWS Config

- `ssm`— Permite usar AWS Service Catalog AWS Systems Manager para ler documentos do Systems Manager na AWS conta corrente e AWS na região.

Veja a política: AWSServiceCatalogEndUserFullAccess.

AWS política gerenciada: **`AWSServiceCatalogEndUserReadOnlyAccess`**

Você pode anexar `AWSServiceCatalogEndUserReadOnlyAccess` às suas entidades do IAM. AppRegistry também anexa essa política a uma função de serviço que permite AppRegistry realizar ações em seu nome.

Esta política concede permissões *`somente leitura`* que oferecem acesso somente leitura à visualização do console do usuário final. Esta política não concede permissão para lançar produtos ou gerenciar produtos provisionados.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `servicecatalog` – concede às entidade principais permissões somente de leitura para a visualização do console do usuário final.
- `cloudformation`— Permite permissões AWS Service Catalog limitadas para listar e ler AWS CloudFormation pilhas.
- `config`— Permite permissões AWS Service Catalog limitadas para listar e ler detalhes sobre portfólios, produtos e produtos provisionados via. AWS Config
- `ssm`— Permite usar AWS Service Catalog AWS Systems Manager para ler documentos do Systems Manager na AWS conta corrente e AWS na região.

Veja a política: AWSServiceCatalogEndUserReadOnlyAccess.

AWS política gerenciada: **`AWSServiceCatalogSyncServiceRolePolicy`**

AWS Service Catalog anexa essa política à função `AWSServiceRoleForServiceCatalogSync` vinculada ao serviço (SLR), permitindo AWS Service Catalog sincronizar modelos em um repositório externo com produtos. AWS Service Catalog

Essa política concede permissões que permitem acesso limitado a AWS Service Catalog ações (por exemplo, chamadas de API) e a outras ações AWS de serviço que AWS Service Catalog dependem de.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `servicecatalog`— Permite que a função de sincronização de AWS Service Catalog artefatos tenha acesso limitado às APIs AWS Service Catalog públicas.
- `codeconnections`— Permite que a função de sincronização de AWS Service Catalog artefatos tenha acesso limitado às APIs CodeConnections públicas.
- `cloudformation`— Permite que a função de sincronização de AWS Service Catalog artefatos tenha acesso limitado às APIs AWS CloudFormation públicas.

Veja a política: AWSServiceCatalogSyncServiceRolePolicy.

Detalhes da função vinculada ao serviço

AWS Service Catalog usa os detalhes de permissão acima para a função `AWSServiceRoleForServiceCatalogSync` vinculada ao serviço que é criada quando um usuário cria ou atualiza um AWS Service Catalog produto que usa. CodeConnections Você pode modificar essa política usando a AWS CLI, a AWS API ou por meio do AWS Service Catalog console. Para mais informações sobre como criar, editar e excluir perfis vinculados a serviços, consulte Usar perfis vinculados a serviços (SLRs) para AWS Service Catalog.

As permissões incluídas na função `AWSServiceRoleForServiceCatalogSync` vinculada ao serviço permitem AWS Service Catalog realizar as seguintes ações em nome do cliente.

- `servicecatalog:ListProvisioningArtifacts`— Permite que a função de sincronização de AWS Service Catalog artefatos liste os artefatos de provisionamento de um determinado AWS Service Catalog produto que são sincronizados com um arquivo de modelo em um repositório.
- `servicecatalog:DescribeProductAsAdmin`— Permite que a função de sincronização de AWS Service Catalog artefatos use a `DescribeProductAsAdmin` API para obter detalhes de um AWS Service Catalog produto e seus artefatos provisionados associados que são sincronizados com um arquivo de modelo em um repositório. O perfil de sincronização de artefatos usa a saída dessa chamada para verificar o limite do Service Quota do produto para provisionamento de artefatos.
- `servicecatalog:DeleteProvisioningArtifact`— Permite que a função de sincronização de AWS Service Catalog artefatos exclua um artefato provisionado.
- `servicecatalog:ListServiceActionsForProvisioningArtifact`— Permite que a função de sincronização de AWS Service Catalog artefatos determine se as ações de serviço

estão associadas a um artefato de provisionamento e garanta que o artefato de provisionamento não seja excluído se uma ação de serviço estiver associada.

- `servicecatalog:DescribeProvisioningArtifact`— Permite que a função de sincronização de AWS Service Catalog artefatos recupere detalhes da `DescribeProvisioningArtifact` API, incluindo o ID do commit, que é fornecido na `SourceRevisionInfo` saída.
- `servicecatalog:CreateProvisioningArtifact`— Permite que a função de sincronização de AWS Service Catalog artefatos crie um novo artefato provisionado se uma alteração for detectada (por exemplo, um git-push for confirmado) no arquivo de modelo de origem no repositório externo.
- `servicecatalog:UpdateProvisioningArtifact`— Permite que a função de sincronização de AWS Service Catalog artefatos atualize o artefato provisionado para um produto conectado ou sincronizado.
- `codeconnections:UseConnection`— Permite que a função de sincronização de AWS Service Catalog artefatos use a conexão existente para atualizar e sincronizar um produto.
- `cloudformation:ValidateTemplate`— Permite que a função de sincronização de AWS Service Catalog artefatos tenha acesso limitado AWS CloudFormation para validar o formato do modelo que está sendo usado no repositório externo e AWS CloudFormation verificar se é compatível com o modelo.

AWS política gerenciada: **`AWSServiceCatalogOrgsDataSyncServiceRolePolicy`**

AWS Service Catalog anexa essa política à função `AWSServiceRoleForServiceCatalogOrgsDataSync` vinculada ao serviço (SLR), permitindo AWS Service Catalog sincronizar com. AWS Organizations

Essa política concede permissões que permitem acesso limitado a AWS Service Catalog ações (por exemplo, chamadas de API) e a outras ações AWS de serviço que AWS Service Catalog dependem de.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- `organizations`— Permite que a função AWS Service Catalog de sincronização de dados tenha acesso limitado às APIs AWS Organizations públicas.

Veja a política: AWSServiceCatalogOrgsDataSyncServiceRolePolicy.

Detalhes da função vinculada ao serviço

AWS Service Catalog usa os detalhes de permissão acima para a função `AWSServiceRoleForServiceCatalogOrgsDataSync` vinculada ao serviço que é criada quando um usuário ativa o acesso ao portfólio AWS Organizations compartilhado ou cria um compartilhamento do portfólio. Você pode modificar essa política usando a AWS CLI, a AWS API ou por meio do AWS Service Catalog console. Para mais informações sobre como criar, editar e excluir perfis vinculados a serviços, consulte Usar perfis vinculados a serviços (SLRs) para AWS Service Catalog.

As permissões incluídas na função `AWSServiceRoleForServiceCatalogOrgsDataSync` vinculada ao serviço permitem AWS Service Catalog realizar as seguintes ações em nome do cliente.

- `organizations:DescribeAccount`— Permite que a função AWS Service Catalog Organizations Data Sync recupere informações AWS Organizations relacionadas sobre a conta especificada.
- `organizations:DescribeOrganization`— Permite que a função AWS Service Catalog Organizations Data Sync recupere informações sobre a organização à qual a conta do usuário pertence.
- `organizations:ListAccounts`— Permite que a função AWS Service Catalog Organizations Data Sync liste as contas na organização do usuário.
- `organizations:ListChildren`— Permite que a função AWS Service Catalog Organizations Data Sync liste todas as unidades organizacionais (UOs) ou contas contidas na OU principal ou raiz especificada.
- `organizations:ListParents`— Permite que a função AWS Service Catalog Organizations Data Sync liste a raiz ou OUs que atuam como pais imediatos da OU ou conta secundária especificada.
- `organizations:ListAWSServiceAccessForOrganization`— Permite que a função AWS Service Catalog Organizations Data Sync recupere uma lista dos AWS serviços que o usuário habilitou para integrar à sua organização.

Políticas obsoletas

As políticas gerenciadas a seguir estão obsoletas:

- ServiceCatalogAdminFullAccess— Use AWSServiceCatalogAdminFullAccessem vez disso.
- ServiceCatalogAdminReadOnlyAccess— Use AWSServiceCatalogAdminReadOnlyAccessem vez disso.
- ServiceCatalogEndUserFullAccess— Use AWSServiceCatalogEndUserFullAccessem vez disso.
- ServiceCatalogEndUserAccess— Use AWSServiceCatalogEndUserReadOnlyAccessem vez disso.

Use o procedimento a seguir para garantir que administradores e usuários finais recebam permissões usando as políticas atuais.

Para migrar das políticas obsoletas para as políticas atuais, consulte Adicionar e remover permissões de identidade do IAM no Guia do Usuário do AWS Identity and Access Management .

AppRegistry atualizações nas políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas AppRegistry desde que esse serviço começou a rastrear essas alterações. Para receber alertas automáticos sobre alterações nessa página, assine o feed RSS na página Histórico do AppRegistry documento.

Alteração	Descrição	Data
AWSServiceCatalogSyncServiceRolePolicy— Atualizar política gerenciada	AWS Service Catalog atualizou a `AWSServiceCatalogSyncServiceRolePolicy` política para mudar `codestar-connections` para `codeconnections` .	7 de maio de 2024
AWSServiceCatalogAdminFullAccess— Atualizar política gerenciada	AWS Service Catalog atualizou a `AWSServiceCatalogAdminFullAccess` política para incluir as permissões necessárias para que o AWS Service Catalog administrador crie a função `AWSServiceRoleForServiceCatalogOrgsD`	14 de abril de 2023

Alteração	Descrição	Data
	`ataSync` vinculada ao serviço (SLR) em sua conta.	
AWSServiceCatalogOrgsDataSyncServiceRolePolicy: Nova política gerenciada	AWS Service Catalog adicionou o`AWSServiceCatalogOrgsDataSyncServiceRolePolicy`, que é anexado à função `AWSServiceRoleForServiceCatalogOrgsDataSync` vinculada ao serviço (SLR), permitindo o AWS Service Catalog a sincronização com. AWS Organizations Essa política permite acesso limitado a AWS Service Catalog ações (por exemplo, chamadas de API) e a outras ações AWS de serviço que AWS Service Catalog dependem de.	14 de abril de 2023
AWSServiceCatalogAdminFullAccess— Atualizar política gerenciada	AWS Service Catalog atualizou a `AWSServiceCatalogAdminFullAccess` política para incluir todas as permissões do AWS Service Catalog administrador e criar compatibilidade com AppRegistry o.	12 de janeiro de 2023

Alteração	Descrição	Data
AWSServiceCatalogSyncServiceRolePolicy: Nova política gerenciada	AWS Service Catalog adicionou a `AWSServiceCatalogSyncServiceRolePolicy` política, que é anexada à função `AWSServiceRoleForServiceCatalogSync` vinculada ao serviço (SLR). Essa política permite AWS Service Catalog sincronizar modelos em um repositório externo com AWS Service Catalog produtos.	18 de novembro de 2022
AWSServiceRoleForServiceCatalogSync— Nova função vinculada ao serviço	AWS Service Catalog adicionou a função `AWSServiceRoleForServiceCatalogSync` vinculada ao serviço (SLR). Essa função é necessária AWS Service Catalog para usar CodeConnections e criar, atualizar e descrever artefatos de AWS Service Catalog provisionamento para um produto.	18 de novembro de 2022

Alteração	Descrição	Data
AWSServiceCatalogAdminFullAccess— Política gerenciada atualizada	AWS Service Catalog atualizou a `AWSServiceCatalogAdminFullAccess` política para incluir todas as permissões necessárias para um AWS Service Catalog administrador. A política identifica as ações específicas que o administrador pode realizar em todos os AWS Service Catalog recursos, como criar, descrever, excluir e muito mais. Além disso, a política foi alterada para oferecer suporte a um recurso lançado recentemente, o Attribute Based Access Control (ABAC) for AWS Service Catalog. O ABAC permite que você use a política `AWSServiceCatalogAdminFullAccess` como um modelo para permitir ou negar ações em recursos AWS Service Catalog com base em tags. Para obter mais informações sobre ABAC, consulte O que é ABAC para a AWS?AWS Identity and Access Management	30 de setembro de 2022

Alteração	Descrição	Data
AppRegistry começou a rastrear alterações	AppRegistry começou a rastrear as mudanças em suas políticas AWS gerenciadas.	15 de setembro de 2022

Usar funções vinculadas ao serviço do AWS Service Catalog

AWS Service Catalog usa funções vinculadas ao serviço AWS Identity and Access Management (IAM). Uma função vinculada ao serviço é um tipo exclusivo de função do IAM vinculada diretamente a. AWS Service Catalog As funções vinculadas ao serviço são predefinidas AWS Service Catalog e incluem todas as permissões que o serviço exige para chamar outros AWS serviços em seu nome.

Uma função vinculada ao serviço facilita a configuração AWS Service Catalog porque você não precisa adicionar manualmente as permissões necessárias. AWS Service Catalog define as permissões de suas funções vinculadas ao serviço e, a menos que seja definido de outra forma, só AWS Service Catalog pode assumir suas funções. As permissões definidas incluem a política de confiança e a política de permissões, e essa política não pode ser anexada a nenhuma outra entidade do IAM.

Uma função vinculada ao serviço poderá ser excluída somente após excluir seus recursos relacionados. Isso protege seus AWS Service Catalog recursos porque você não pode remover inadvertidamente a permissão para acessar os recursos.

Para obter informações sobre outros serviços compatíveis com perfis vinculados aos serviços, consulte Serviços da AWS que funcionam com o IAM e procure os serviços que apresentam Sim na coluna Funções vinculadas aos serviços. Escolha um Sim com um link para visualizar a documentação da função vinculada a esse serviço.

Permissões de função vinculada ao serviço **`AWSServiceRoleForServiceCatalogSync`**

AWS Service Catalog pode usar a função vinculada ao serviço chamada **`AWSServiceRoleForServiceCatalogSync`**— Essa função vinculada ao serviço é necessária AWS Service Catalog para usar CodeConnections e criar, atualizar e descrever artefatos de AWS Service Catalog provisionamento de um produto.

A função vinculada ao serviço `AWSServiceRoleForServiceCatalogSync` confia nos seguintes serviços para aceitar a função:

- `sync.servicecatalog.amazonaws.com`

A política de permissões de função nomeada AWSServiceCatalogSyncServiceRolePolicy AWS Service Catalog permite concluir as seguintes ações nos recursos especificados:

- Ação: `Connection` em `CodeConnections`
- Ação: `Create, Update, and Describe` ativada `ProvisioningArtifact` para um AWS Service Catalog produto

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada a serviço. Para obter mais informações, consulte Permissões de função vinculada a serviços no Guia do Usuário do IAM.

Criando uma função vinculada ao serviço **`AWSServiceRoleForServiceCatalogSync`**

Você não precisa criar manualmente a função `AWSServiceRoleForServiceCatalogSync` vinculada ao serviço. AWS Service Catalog cria a função vinculada ao serviço para você automaticamente quando você estabelece CodeConnections na AWS Management Console AWS CLI, na ou na AWS API.

> **Important**
>
> Essa função vinculada ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os atributos compatíveis com essa função. Além disso, se você estava usando o AWS Service Catalog serviço antes de 18 de novembro de 2022, quando ele começou a oferecer suporte a funções vinculadas ao serviço, AWS Service Catalog criou a `AWSServiceRoleForServiceCatalogSync` função em sua conta. Para saber mais, consulte Uma nova função apareceu na minha conta do IAM.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você pode usar esse mesmo processo para recriar a função na sua conta. Quando você estabelece CodeConnections, AWS Service Catalog cria a função vinculada ao serviço para você novamente.

Você também pode usar o console do IAM para criar uma função vinculada ao serviço com o caso de uso de AWS Service Catalog produtos sincronizados. Na AWS CLI ou na AWS API, crie uma função vinculada ao serviço com o nome do `sync.servicecatalog.amazonaws.com` serviço. Para obter mais informações, consulte Criar uma função vinculada ao serviço no Manual do usuário do IAM. Se você excluir essa função vinculada ao serviço, será possível usar esse mesmo processo para criar a função novamente.

Permissões de função vinculada ao serviço **`AWSServiceRoleForServiceCatalogOrgsDataSync`**

AWS Service Catalog pode usar a função vinculada ao serviço chamada **`AWSServiceRoleForServiceCatalogOrgsDataSync`**— Essa função vinculada ao serviço é necessária para que AWS Service Catalog as organizações permaneçam sincronizadas. AWS Organizations

A função vinculada ao serviço `AWSServiceRoleForServiceCatalogOrgsDataSync` confia nos seguintes serviços para aceitar a função:

- `orgsdatasync.servicecatalog.amazonaws.com`

O perfil `AWSServiceRoleForServiceCatalogOrgsDataSync` vinculado ao serviço exige que você use a seguinte política de confiança, além da política `AWSServiceCatalogOrgsDataSyncServiceRolePolicy` gerenciada:

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

A política de permissões de função nomeada AWSServiceCatalogOrgsDataSyncServiceRolePolicy AWS Service Catalog permite concluir as seguintes ações nos recursos especificados:

- Ação: `DescribeAccount`, `DescribeOrganization`, e `ListAWSServiceAccessForOrganization` em `Organizations accounts`
- Ação: `ListAccounts`, `ListChildren`, e `ListParent` em `Organizations accounts`

Você deve configurar permissões para que uma entidade do IAM (por exemplo, um usuário, grupo ou função) crie, edite ou exclua uma função vinculada a serviço. Para obter mais informações, consulte Permissões de função vinculada a serviços no Guia do Usuário do IAM.

Criando uma função vinculada ao serviço **`AWSServiceRoleForServiceCatalogOrgsDataSync`**

Você não precisa criar manualmente a função `AWSServiceRoleForServiceCatalogOrgsDataSync` vinculada ao serviço. AWS Service Catalog considera sua ação de habilitar Compartilhamento com o AWS Organizations ou Compartilhar um portfólio como permissão AWS Service Catalog para criar uma SLR em segundo plano em seu nome.

AWS Service Catalog cria a função vinculada ao serviço para você automaticamente quando você solicita `EnableAWSOrganizationsAccess` ou `CreatePortfolioShare` na AWS Management Console AWS CLI, na ou na AWS API.

> **Important**
>
> Essa função vinculada ao serviço pode aparecer em sua conta se você concluiu uma ação em outro serviço que usa os atributos compatíveis com essa função. Para saber mais, consulte Uma nova função apareceu na minha conta do IAM.

Se excluir essa função vinculada ao serviço e precisar criá-la novamente, você pode usar esse mesmo processo para recriar a função na sua conta. Quando você solicita `EnableAWSOrganizationsAccess` o `CreatePortfolioShare`, AWS Service Catalog cria um perfil vinculado ao serviço para você novamente.

Editar uma função vinculada ao serviço para o AWS Service Catalog

AWS Service Catalog não permite que você edite as funções `AWSServiceRoleForServiceCatalogSync` ou funções

`AWSServiceRoleForServiceCatalogOrgsDataSync` vinculadas ao serviço. Depois que criar um perfil vinculado ao serviço, você não poderá alterar o nome do perfil, pois várias entidades podem fazer referência a ele. No entanto, será possível editar a descrição do perfil usando o IAM. Para obter mais informações, consulte Editar uma função vinculada a serviço no Guia do usuário do IAM.

Excluir uma função vinculada ao serviço para o AWS Service Catalog

Você pode usar o console do IAM, a AWS CLI ou a AWS API para excluir manualmente a `AWSServiceRoleForServiceCatalogSync` ou `AWSServiceRoleForServiceCatalogOrgsDataSync` a SLR. Para fazer isso, primeiro você deve remover manualmente todos os recursos que estão usando a função vinculada ao serviço (por exemplo, qualquer AWS Service Catalog produto sincronizado com um repositório externo) e, em seguida, a função vinculada ao serviço pode ser excluída manualmente.

Regiões compatíveis com funções vinculadas ao serviço do AWS Service Catalog

AWS Service Catalog suporta o uso de funções vinculadas ao serviço em todas as regiões em que o serviço está disponível. Para obter mais informações, consulte Regiões e endpoints da AWS.

Nome da região	Identidade da região	Support em AWS Service Catalog
Leste dos EUA (Norte da Virgínia)	us-east-1	Sim
Leste dos EUA (Ohio)	us-east-2	Sim
Oeste dos EUA (N. da Califórnia)	us-west-1	Sim
Oeste dos EUA (Oregon)	us-west-2	Sim
África (Cidade do Cabo)	af-south-1	Sim
Ásia-Pacífico (Hong Kong)	ap-east-1	Sim
Ásia-Pacífico (Jacarta)	ap-southeast-3	Sim
Ásia-Pacífico (Mumbai)	ap-south-1	Sim
Ásia-Pacífico (Osaka)	ap-northeast-3	Sim
Ásia-Pacífico (Seul)	ap-northeast-2	Sim

Nome da região	Identidade da região	Support em AWS Service Catalog
Ásia-Pacífico (Singapura)	ap-southeast-1	Sim
Ásia-Pacífico (Sydney)	ap-southeast-2	Sim
Ásia-Pacífico (Tóquio)	ap-northeast-1	Sim
Canadá (Central)	ca-central-1	Sim
Europa (Frankfurt)	eu-central-1	Sim
Europa (Irlanda)	eu-west-1	Sim
Europa (Londres)	eu-west-2	Sim
Europa (Milão)	eu-south-1	Sim
Europa (Paris)	eu-west-3	Sim
Europa (Estocolmo)	eu-north-1	Sim
Oriente Médio (Barém)	me-south-1	Sim
América do Sul (São Paulo)	sa-east-1	Sim
AWS GovCloud (Leste dos EUA)	us-gov-east-1	Não
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	Não

Solução de problemas AWS Service Catalog de identidade e acesso

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com AWS Service Catalog um IAM.

Tópicos

- Não estou autorizado a realizar uma ação em AWS Service Catalog
- Não estou autorizado a executar iam:PassRole

- Quero permitir que pessoas fora da minha AWS conta acessem meus AWS Service Catalog recursos

Não estou autorizado a realizar uma ação em AWS Service Catalog

Se isso AWS Management Console indicar que você não está autorizado a realizar uma ação, entre em contato com o administrador para obter ajuda. Caso seu administrador seja a pessoa que forneceu suas credenciais de início de sessão. O exemplo de erro a seguir ocorre quando o usuário mateojackson tenta usar o console para ver detalhes sobre um my-example-widget recurso fictício, mas não tem as permissões fictícias. `aws:GetWidget`

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

Neste caso, Mateo pede ao administrador para atualizar suas políticas para permitir a ele o acesso ao recurso `my-example-widget` usando a ação `aws:GetWidget`.

Não estou autorizado a executar **`iam:PassRole`**

Se você receber uma mensagem de erro informando que você não está autorizado a executar a ação `iam:PassRole`, entre em contato com o administrador para obter assistência. O administrador é a pessoa que forneceu o seu nome de usuário e senha. Peça a essa pessoa para atualizar suas políticas para permitir que você passe uma função para o AWS Service Catalog.

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

O erro de exemplo a seguir ocorre quando uma usuária chamada marymajor tenta usar o console para executar uma ação no AWS Service Catalog. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar a função para o serviço.

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

Nesse caso, Mary pede ao administrador que atualize suas políticas para permitir que ela execute a PassRole ação iam:.

Quero permitir que pessoas fora da minha AWS conta acessem meus AWS Service Catalog recursos

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem compatibilidade com políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se é AWS Service Catalog compatível com esses recursos, consulte AWS Identity and Access Management o Guia do AWS Service Catalog Administrador. AWS Service Catalog
- Para saber como fornecer acesso aos seus recursos em todas AWS as contas que você possui, consulte Como fornecer acesso a um usuário do IAM em outra AWS conta que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos para AWS contas de terceiros, consulte Como fornecer acesso a AWS contas pertencentes a terceiros no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte Conceder acesso a usuários autenticados externamente (federação de identidades) no Guia do usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em recursos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Controle de acesso

um AWS Service Catalog portfólio oferece aos administradores um nível de controle de acesso para seus grupos de usuários finais. Ao adicionar usuários a um portfólio, eles podem navegar e executar os produtos no portfólio. Para ter mais informações, consulte the section called “Gerenciamento de portfólios”.

Restrições

As restrições controlam quais regras são aplicadas aos usuários finais na execução de um produto de um portfólio específico. Use-as com o intuito de aplicar limites aos produtos para realizar a

governança e o controle de custos. Para obter mais informações sobre restrições, consulte the section called “Uso de restrições”.

AWS Service Catalog as restrições de lançamento oferecem mais controle sobre as permissões necessárias para um usuário final. Quando o administrador cria uma restrição de execução para um produto em um portfólio, essa restrição associa um ARN de função que é usado quando os usuários finais executam o produto desse portfólio. Usando esse padrão, você pode controlar o acesso à criação AWS de recursos. Para ter mais informações, consulte the section called “Restrições de lançamento”.

Registro e monitoramento em AWS Service Catalog

AWS Service Catalog integra-se com AWS CloudTrail, um serviço que captura todas as chamadas de AWS Service Catalog API e entrega os arquivos de log para um bucket do Amazon S3 que você especificar. Para obter mais informações, consulte Registrar chamadas de AWS Service Catalog API com CloudTrail.

Você também pode usar restrições de notificação para configurar notificações do Amazon SNS sobre eventos de pilha. Para ter mais informações, consulte the section called “Restrições de notificação”.

Validação de conformidade para AWS Service Catalog

Auditores terceirizados avaliam a segurança e a conformidade AWS Service Catalog como parte de vários programas de AWS conformidade, incluindo os seguintes:

- Controles do Sistema e da Organização (CSO)
- Padrão de segurança de dados do setor de cartão de pagamento (PCI DSS – Payment Card Industry Data Security Standard)
- Federal Risk and Authorization Management Program (FedRAMP)
- Health Insurance Portability and Accountability Act (HIPAA)

Para obter uma lista de AWS serviços no escopo de programas de conformidade específicos, consulte AWS Services in Scope by Compliance Program. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Fazer o download de Relatórios no AWS Artifact.

Sua responsabilidade de conformidade ao usar AWS Service Catalog depende da confidencialidade de seus dados, dos objetivos de conformidade da sua empresa e das leis e regulamentos aplicáveis. AWS fornece esses recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos focados em segurança e conformidade em. AWS
- Documento técnico sobre arquitetura para segurança e conformidade com a HIPAA — Este whitepaper descreve como as empresas podem usar para criar aplicativos compatíveis com a HIPAA. AWS
- Recursos de compatibilidade da AWS - esta coleção de guias e pastas de trabalho pode ser aplicada ao seu setor e local.
- AWS Config— Esse AWS serviço avalia se suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Esse AWS serviço fornece uma visão abrangente do seu estado de segurança interno, AWS que ajuda você a verificar sua conformidade com os padrões e as melhores práticas do setor de segurança.

Resiliência em AWS Service Catalog

A infraestrutura AWS global é construída em torno de AWS regiões e zonas de disponibilidade. AWS As regiões fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as Zonas de Disponibilidade, é possível projetar e operar aplicações e bancos de dados que executem o failover automaticamente entre as Zonas de Disponibilidade sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

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

Além da infraestrutura AWS global, AWS Service Catalog oferece ações de AWS Service Catalog autoatendimento. Com ações de autoatendimento, os clientes podem reduzir a manutenção administrativa e o treinamento do usuário final, aderindo às medidas de conformidade e segurança. Com as ações de autoatendimento, como administrador, você pode permitir que os usuários finais realizem tarefas operacionais, como backup e restauração, solução de problemas, execução de

comandos aprovados e solicitação de permissões no AWS Service Catalog. Para saber mais, consulte the section called “Usar ações de atendimento”.

Segurança de infraestrutura em AWS Service Catalog

Como serviço gerenciado, AWS Service Catalog é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar AWS Service Catalog pela rede. Os clientes devem oferecer suporte para:

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

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

Com AWS Service Catalog, você pode controlar as regiões nas quais os dados são armazenados. Portfólios e produtos só estão disponíveis nas regiões nas quais você os disponibilizou. Você pode usar a API `CopyProduct` para copiar um produto em outra região.

Melhores práticas de segurança para AWS Service Catalog

AWS Service Catalog fornece vários recursos de segurança a serem considerados ao desenvolver e implementar suas próprias políticas de segurança. As melhores práticas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas melhores práticas podem não ser adequadas ou suficientes para o seu ambiente, trate-as como considerações úteis em vez de prescrições.

Você pode definir regras que limitam os valores de parâmetro que um usuário informa ao executar um produto. Essas regras são chamadas de restrições de modelo porque elas limitam como

o modelo do AWS CloudFormation do produto é implantado. Use um editor simples para criar restrições de modelo e aplique-as individualmente aos produtos.

AWS Service Catalog aplica restrições ao provisionar um novo produto ou atualizar um produto que já está em uso. Ele sempre aplica a restrição mais rígida entre todas as restrições aplicadas ao portfólio e ao produto. Por exemplo, considere um cenário em que o produto permite que todas as instâncias do Amazon EC2 sejam lançadas e o portfólio tem duas restrições: uma que permite que todas as instâncias do EC2 do tipo que não seja GPU sejam inicializadas e uma que permite apenas que instâncias do EC2 t1.micro e m1.small sejam lançadas. Neste exemplo, AWS Service Catalog aplica a segunda restrição mais restritiva (t1.micro e m1.small).

Você pode limitar o acesso que os usuários finais têm aos AWS recursos ao anexar uma política do IAM a uma função de lançamento. Em seguida, você usa AWS Service Catalog para criar uma restrição de lançamento para usar a função ao lançar o produto.

Para saber mais sobre políticas gerenciadas para AWS Service Catalog, consulte Políticas AWS gerenciadas para AWS Service Catalog.

Gerenciar catálogos

O AWS Service Catalog fornece uma interface para gerenciamento de portfólios, produtos e restrições em um console de administrador.

> **Note**
>
> Para executar qualquer uma das tarefas desta seção, você deve ter permissões de administrador do AWS Service Catalog. Para ter mais informações, consulte Gerenciamento de identidades e acesso no AWS Service Catalog.

Tarefas

- Gerenciamento de portfólios
- Gerenciar produtos
- Uso de restrições do AWS Service Catalog
- Ações de atendimento do AWS Service Catalog
- Adição de produtos do AWS Marketplace ao seu portfólio
- Usando AWS CloudFormation StackSets
- Gerenciar orçamentos

Gerenciamento de portfólios

Você pode criar, visualizar e atualizar portfólios na página Portfólios no console do administrador do AWS Service Catalog.

Tarefas

- Criar, visualizar e excluir portfólios
- Visualizar detalhes do portfólio
- Criar e excluir portfólios
- Adicionar produtos
- Adição de restrições
- Conceder acesso aos usuários
- Compartilhar um portfólio

- Compartilhamento e importação de portfólios

Criar, visualizar e excluir portfólios

A página Portfólios exibe uma lista dos portfólios que você criou na região atual. Use essa página para criar novos portfólios, visualizar os detalhes de um portfólio ou excluir portfólios de sua conta.

Visualizar a página Portfólios

1. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/.
2. Selecione outra região conforme necessário.
3. Se você for novo no AWS Service Catalog, verá a página inicial do AWS Service Catalog. Selecione Comece a usar para criar um portfólio. Siga as instruções para criar seu primeiro portfólio e vá para a página Portfólios.

Ao usar o AWS Service Catalog, você pode retornar para a página Portfólios a qualquer momento; escolha Service Catalog na barra de navegação e, em seguida, Portfólios.

Visualizar detalhes do portfólio

No console do administrador do AWS Service Catalog, a página Portfolio details (Detalhes do portfólio) lista as configurações de um portfólio. Use esta página para gerenciar os produtos no portfólio, conceder aos usuários acesso aos produtos TagOptions e aplicar restrições.

Para visualizar a página Portfolio details

1. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/.
2. Escolha o portfólio que você deseja gerenciar.

Criar e excluir portfólios

Use a página Portfólios para criar e excluir portfólios.

Para criar um novo portfólio

1. No menu de navegação à esquerda, escolha Portfólios.
2. Escolha Criar portfólio.

3. Na página Criar portfólio, insira as informações solicitadas.
4. Escolha Criar. O AWS Service Catalog cria o portfólio e exibe os detalhes do portfólio.

Para excluir um portfólio

> **Note**
>
> Você só pode excluir portfólios locais. Você pode remover portfólios importados (compartilhados), mas não pode excluir portfólios importados.

Antes de excluir um portfólio, você deve remover todos os seus produtos, restrições, grupos, funções, usuários, compartilhamentos e. TagOptions Para fazer isso, abra um portfólio para exibir os Detalhes do portfólio. Em seguida, escolha uma guia para removê-los.

> **Note**
>
> Para evitar erros, remova as restrições do portfólio antes de remover qualquer produto.

1. No menu de navegação à esquerda, escolha Portfólios.
2. Selecione o relatório que você deseja excluir.
3. Escolha Excluir. Você só pode excluir portfólios locais. Se você estiver tentando excluir um portfólio importado (compartilhado), o menu Ações não estará disponível.
4. Na janela de confirmação, escolha Excluir.

Adicionar produtos

Você pode adicionar produtos a um portfólio fazendo o upload de um novo produto diretamente em um portfólio existente ou associando um produto existente do seu catálogo ao portfólio.

> **Note**
>
> Ao criar um produto AWS Service Catalog, você pode carregar um modelo AWS CloudFormation ou arquivo de configuração do Terraform. O modelo AWS CloudFormation é armazenado em um bucket do Amazon Simple Storage Service (Amazon S3), e o nome do bucket começa com “cf-templates-”. Você também precisa ter permissão para recuperar

objetos de buckets adicionais ao provisionar um produto. Para obter mais informações, consulte Criar produtos.

Adicionar um novo produto

Você adiciona novos produtos diretamente na página Detalhes do portfólio. Quando você cria um produto nessa página, o AWS Service Catalog o adiciona ao portfólio selecionado no momento.

Para adicionar um novo produto

1. Vá até a página Portfólios e, em seguida, escolha o nome do portfólio ao qual você deseja adicionar o produto.
2. Na página Detalhes do portfólio, expanda a seção Produtos e, em seguida, escolha Fazer upload de produto novo.
3. Em Enter product details, insira o seguinte:

   - Nome do produto – o nome do produto.
   - Descrição do produto (opcional) - a descrição do produto. Essa descrição é mostrada na lista de produtos para ajudar o usuário a escolher o produto correto.
   - Descrição – a descrição completa. Essa descrição é mostrada na lista de produtos para ajudar o usuário a escolher o produto correto.
   - Proprietário ou distribuidor — o nome ou endereço de e-mail do proprietário. As informações de contato do distribuidor são opcionais.
   - Vendedor (opcional) – o nome do publicador do aplicativo. Esse campo permite que os usuários classifiquem sua lista de produtos para facilitar a localização dos produtos necessários.
4. Na página Version details, insira o seguinte:

   - Escolha o modelo — para produtos AWS CloudFormation, escolha seu próprio arquivo de modelo, um modelo AWS CloudFormation de uma unidade local ou uma URL que aponte para um modelo armazenado no Amazon S3, um modelo existente do Stack ARN AWS CloudFormation ou um arquivo de modelo armazenado em um repositório externo.

     Para produtos Terraform, escolha seu próprio arquivo de modelo, um arquivo de configuração tar.gz de uma unidade local ou uma URL que aponta para um modelo armazenado no Amazon S3 ou um arquivo de configuração tar.gz armazenado em um repositório externo.

- Nome da versão (opcional) - o nome da versão do produto (por exemplo, “v1”, “v2beta”). Espaços não são permitidos.
- Description (opcional) – uma descrição da versão do produto incluindo como essa versão difere da versão anterior.

5. Em Enter support details, insira o seguinte:

   - Contato por e-mail (opcional) – o endereço de e-mail para relatório de problemas com o produto.
   - Link de suporte (opcional) – uma URL de um site onde os usuários podem localizar informações de suporte ou abrir tickets. A URL deve começar com `http://` ou `https://`. Os administradores são responsáveis por manter a precisão e o acesso às informações de suporte.
   - Descrição do suporte (opcional) - uma descrição de como os usuários devem usar o Contato por e-mail e o Link de suporte.

6. Escolha Criar produto.

Adicionar um produto existente

Você pode adicionar produtos existentes a um portfólio em três locais: a lista Portfólios, a página Detalhes do portfólio, ou a página Lista de produtos.

Para adicionar um produto existente a um portfólio

1. Navegue até a página Portfólios.
2. Escolha um portfólio. Em seguida, escolha Ações - Adicionar produto ao portfólio.
3. Escolha um produto e, em seguida, escolha Adicionar produto ao portfólio.

Remover um produto de um portfólio

Quando você não quiser mais que os usuários usem um produto, remova-o do portfólio. O produto ainda estará disponível em seu catálogo na página Produtos e você ainda poderá adicioná-lo a outros portfólios. Você pode remover vários produtos de um portfólio de uma vez.

Para remover um produto de um portfólio

1. Navegue até a página Portfólios e escolha o portfólio que contém o produto. A página Detalhes do portfólio é aberta.
2. Expanda a seção Produtos.
3. Escolha um ou mais produtos e, em seguida, Remover.
4. Confirme sua escolha.

Adição de restrições

Você deve adicionar restrições para controlar como os usuários interagem com os produtos. Para obter mais informações sobre os tipos de restrições às quais o AWS Service Catalog oferece suporte, consulte Uso de restrições do AWS Service Catalog.

Você adiciona restrições aos produtos depois que eles são colocados em um portfólio.

Para adicionar uma restrição a um produto

1. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/.
2. Escolha Portfólios e selecione um portfólio.
3. Na página de detalhes do portfólio, expanda a seção Criar restrição e selecione Adicionar restrições.
4. Para Produto, selecione o produto ao qual aplicar a restrição.
5. Em Tipo de restrição, escolha uma das seguintes opções:

   Lançamento - permite atribuir um perfil do IAM ao produto usado para provisionar os recursos da AWS. Para ter mais informações, consulte Restrições de lançamento do AWS Service Catalog.

   Notificação - permite transmitir notificações de produtos a um tópico do Amazon SNS. Para ter mais informações, consulte Restrições de notificação do AWS Service Catalog.

   Modelo - permite limitar as opções disponíveis para os usuários finais quando lançam um produto. Um modelo consiste de um arquivo de texto formatado em JSON que contém uma ou mais regras. As regras são adicionadas ao modelo do AWS CloudFormation usado pelo produto. Para ter mais informações, consulte Regras de restrições de modelo.

Conjunto de pilhas — permite que você configure a implantação do produto em contas e regiões usando AWS CloudFormation StackSets. Para ter mais informações, consulte Restrições do conjunto de pilhas do AWS Service Catalog.

Atualização de tags — permite que você atualize tags depois que o produto tiver sido provisionado. Para ver mais informações, consulte Restrições de atualização de Tag do AWS Service Catalog.

6. Escolha Continuar e insira as informações necessárias.

Para editar uma restrição

1. Faça login ao AWS Management Console e abra o console do administrador do AWS Service Catalog em https://console.aws.amazon.com/catalog/.
2. Escolha Portfólios e selecione um portfólio.
3. Na página Detalhes do portfólio, expanda a seção Criar restrição e selecione a restrição para editar.
4. Escolha Editar restrições.
5. Edite a restrição conforme o necessário e escolha Salvar.

Conceder acesso aos usuários

Dê aos usuários acesso aos portfólios por meio de grupos ou funções. A melhor maneira de fornecer acesso ao portfólio para muitos usuários é colocar os usuários em um grupo do IAM e conceder acesso a esse grupo. Dessa forma, você pode simplesmente adicionar e remover usuários do grupo para gerenciar o acesso ao portfólio. Para obter mais informações, consulte Usuários e grupos do IAM no Guia do usuário do IAM.

Além do acesso a um portfólio, os usuários também devem ter acesso ao console do usuário final do AWS Service Catalog. Você concede acesso ao console aplicando permissões no IAM. Para ter mais informações, consulte Gerenciamento de identidades e acesso no AWS Service Catalog.

Se quiser compartilhar um portfólio e suas entidades principais com outras contas, você pode associar nomes de entidades principais (grupos, funções ou usuários) ao Portfólio. Os nomes das entidades principais são compartilhados com o Portfólio e usados nas contas dos destinatários para conceder acesso aos usuários finais.

Para conceder acesso ao portfólio a usuários ou grupos

1. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/.
2. No painel de navegação, escolha Administração e, em seguida, escolha Portfólios.
3. Escolha um portfólio ao qual você deseja conceder acesso a grupos, perfis ou usuários. AWS Service Catalog direciona para a página de Detalhes do portfólio.
4. Na página Detalhes do portfólio, escolha a guia Acesso.
5. Em Acesso ao portfólio, escolha Conceder acesso.
6. Em Tipo, escolha Nome da entidade principal e, em seguida, selecione o Tipo de grupo/, perfil/, ou usuário/. É possível adicionar até 9 nomes de entidades principais.
7. Escolha Conceder acesso para associar a entidade principal ao portfólio atual.

Para remover o acesso a um portfólio

1. Na página Detalhes do portfólio, escolha um grupo, perfil ou nome de usuário.
2. Em seguida, escolha Remover acesso.

Compartilhar um portfólio

Para permitir que um AWS Service Catalog administrador de outra AWS conta distribua seus produtos aos usuários finais, compartilhe seu AWS Service Catalog portfólio com eles usando account-to-account compartilhamento ouAWS Organizations.

Quando você compartilha um portfólio usando account-to-account compartilhamento ou Organizations, você está compartilhando uma referência desse portfólio. Os produtos e as restrições no portfólio importado permanecem sincronizados com as alterações que você faz no portfólio compartilhado, o portfólio original que você compartilhou.

O destinatário não pode alterar os produtos ou as restrições, mas pode adicionar o acesso ao AWS Identity and Access Management para usuários finais.

> **Note**
>
> Não é possível compartilhar um recurso compartilhado. Isso inclui portfólios que contêm um produto compartilhado.

Um ccount-to-account compartilhamento

Para concluir estas etapas, você deve obter a ID da conta da AWS de destino. O ID é fornecido na página Minha conta no AWS Management Console da conta de destino.

Como compartilhar um portfólio com uma conta da AWS

1. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/.
2. No menu de navegação à esquerda, selecione Portfólios e o portfólio que você deseja compartilhar. No menu Ações, selecione Compartilhar.
3. Em Inserir ID da conta, insira a ID da conta da AWS com a qual você está compartilhando. (Opcional) Selecione TagOption Compartilhamento. Em seguida, escolha Compartilhar.
4. Envie o URL ao administrador do AWS Service Catalog da conta de destino. A URL abre a página Importar Portfólio com o ARN do portfólio compartilhado fornecido automaticamente.

Importação de um portfólio

Se um administrador do AWS Service Catalog de outra conta da AWS compartilhar um portfólio com você, importe-o para sua conta e distribua os produtos para seus usuários finais.

Você não precisa importar um portfólio se o portfólio foi compartilhado por meio do AWS Organizations.

Para importar o portfólio, você deve ter uma URL para importar o portfólio do administrador.

Para ver todos os portfólios importados, abra o console do AWS Service Catalog em https://console.aws.amazon.com/servicecatalog/. Na página Portfólios, selecione a guia Importado. Revise a tabela Portfólios importados.

Compartilhamento com o AWS Organizations

Você pode compartilhar portfólios do AWS Service Catalog usando o AWS Organizations.

Primeiro, você deve decidir se está compartilhando a partir da conta de gerenciamento ou de uma conta de administração delegada. Se você não quiser compartilhar a partir de sua conta de gerenciamento, registre uma conta de administração delegada e use-a para compartilhar. Para obter mais informações, consulte Registrar um administrador delegado, no Guia do desenvolvedor do AWS CloudFormation.

Depois, você deve decidir com quem compartilhar. Você pode compartilhar com as seguintes entidades:

- Uma conta da organização.
- Uma unidade organizacional (OU).
- A própria organização. (Essa ação compartilha com todas as contas da organização.)

Como compartilhar de uma conta de gerenciamento

Você pode compartilhar um portfólio com uma organização ao usar sua estrutura organizacional ou inserir a ID de um nó organizacional.

Para compartilhar um portfólio com uma organização usando a estrutura organizacional

1. Abra o AWS Service Catalog console em https://console.aws.amazon.com/servicecatalog/.
2. Na página Portfólios, selecione o portfólio que você deseja compartilhar. No menu Ações, selecione Compartilhar.
3. Selecione AWS Organizations e filtre em sua estrutura organizacional.

   Você pode selecionar o nó raiz para compartilhar o portfólio com toda a sua organização, uma Unidade Organizacional (UO) principal, uma UO secundária ou uma conta da AWS dentro da sua organização.

   O compartilhamento com uma UO principal compartilha o portfólio com todas as contas e UOs secundárias dentro dessa UO principal.

   Você pode selecionar Exibir AWS contas somente para ver uma lista de todas as contas da AWS em sua organização.

Para compartilhar um portfólio com uma organização inserindo a ID do nó organizacional

1. Abra o AWS Service Catalog console em https://console.aws.amazon.com/servicecatalog/.
2. Na página Portfólios, selecione o portfólio que você deseja compartilhar. No menu Ações, selecione Compartilhar.
3. Selecione Nó da organização.

   Selecione se você deseja compartilhar com toda a sua organização, uma conta da AWS dentro da sua organização ou uma UO.

Insira a ID do nó organizacional que você selecionou, que pode ser encontrada no console AWS Organizations em https://console.aws.amazon.com/organizations/.

Compartilhar de uma conta de administrador delegado

A conta mestra de uma organização pode registrar e cancelar o registro de outras contas como administradores delegados da organização.

Um administrador delegado pode compartilhar recursos do AWS Service Catalog na organização dele da mesma maneira que uma conta mestra. Ele tem autorização para criar, excluir e compartilhar portfólios.

Para registrar ou cancelar o registro de um administrador delegado, você deve usar a API ou a CLI do gerenciamento de contas. Para obter mais informações, consulte RegisterDelegatedAdministrator e DeregisterDelegatedAdministrator na Referência da API do AWS Organizations.

> **Note**
>
> Antes que você possa designar um representante, o administrador deve chamar `EnableAWSOrganizationsAccess`.

O procedimento para compartilhar um portfólio de uma conta de administrador delegado é o mesmo que compartilhar de uma conta, conforme visto acima em the section called “Como compartilhar de uma conta de gerenciamento”.

Se um membro tiver o registro cancelado como administrador delegado, ocorrerá o seguinte:

- Os compartilhamentos de portfólio que foram criados por meio dessa conta serão removidos.
- Ele não poderá mais criar compartilhamentos de portfólio.

> **Note**
>
> Se o portfólio e os compartilhamentos criados por um administrador delegado não forem removidos após o administrador delegado ter o registro cancelado, registre e cancele o registro do administrador delegado novamente. Essa ação removerá o portfólio e os compartilhamentos criados por essa conta.

Mover contas dentro da sua organização

Se você mover uma conta dentro da sua organização, os portfólios AWS Service Catalog compartilhados com a conta poderão mudar.

As contas só têm acesso aos portfólios compartilhados com a organização ou unidade organizacional de destino.

Compartilhamento TagOptions ao compartilhar portfólios

Como administrador, você pode criar um compartilhamento para incluir TagOptions. TagOptions são pares de valores-chave que permitem aos administradores:

- Definir e aplicar a taxonomia das tags.
- Definir as opções de tags e associá-las a produtos e portfólios.
- Compartilhar opções de tags associadas a portfólios e produtos com outras contas.

Quando você adiciona ou remove opções de tag na conta principal, a alteração aparece automaticamente nas contas dos destinatários. Nas contas de destinatários, quando um usuário final provisiona um produto com TagOptions, ele deve escolher valores para tags que se tornam tags no produto provisionado.

Nas contas de destinatários, os administradores podem associar locais adicionais TagOptions ao portfólio importado para impor regras de marcação específicas para essa conta.

> **Note**
>
> Para compartilhar um portfólio, você precisa da ID da conta da AWS do consumidor. Encontre a ID da conta da AWS em Minha conta no console.

> **Note**
>
> Se a TagOption tiver um único valor, AWS aplicará automaticamente esse valor durante o processo de provisionamento.

Para compartilhar TagOptions ao compartilhar portfólios

1. No menu de navegação à esquerda, escolha Portfólios.
2. Em Portfólios locais, escolha e abra um portfólio.
3. Escolha Compartilhar na lista acima e, em seguida, escolha o botão Compartilhar.
4. Escolha compartilhar com outra conta da AWS ou organização.
5. Insira o número de identificação da conta de 12 dígitos, selecione Habilitar e escolha Compartilhar.

   A conta que você compartilhou é exibida na seção Contas compartilhadas com. Indica se TagOptions estamos habilitados.

Você também pode atualizar um compartilhamento de portfólio para incluí-lo TagOptions. Todos os TagOptions que pertencem ao portfólio e ao produto agora são compartilhados nessa conta.

Para atualizar um compartilhamento de portfólio para incluir TagOptions

1. No menu de navegação à esquerda, escolha Portfólios.
2. Em Portfólio local, escolha e abra um portfólio.
3. Escolha Compartilhar na lista acima.
4. Em Contas compartilhadas com, escolha uma ID de conta e, em seguida, escolha Ações.
5. Selecione Atualizar cancelar compartilhamento ou Cancelar compartilhamento.

   Ao selecionar Atualizar e cancelar compartilhamento, escolha Habilitar para iniciar o compartilhamento. TagOptions A conta que você compartilhou é exibida na seção Contas compartilhadas com.

   Ao selecionar Cancelar compartilhamento, confirme que não deseja mais compartilhar a conta.

Compartilhar Nomes de Entidades principais ao compartilhar portfólios

Como administrador, você pode criar um compartilhamento de portfólio que inclua Nomes de Entidades principais. Os Nomes de Entidades principais são nomes de grupos, perfis e usuários que os administradores podem especificar em um portfólio e depois compartilhar com o portfólio. Quando você compartilha o portfólio, AWS Service Catalog verifique se esses Nomes de Entidades principais já existem. Se existirem, AWS Service Catalog associe automaticamente as entidades principais do IAM correspondentes ao Portfólio compartilhado para conceder acesso aos usuários.

> **Note**
>
> Quando você associa uma entidade principal a um portfólio, um possível caminho de escalação de privilégios pode ocorrer quando então esse portfólio é compartilhado com outras contas. Para um usuário em uma conta de destinatário que não é um administrador do AWS Service Catalog, mas tem a capacidade de criar Entidades principais (usuários/perfis), esse usuário pode criar uma Entidade principal de IAM que corresponda à associação do nome da entidade principal do portfólio. Embora esse usuário talvez não saiba quais nomes de entidade principal estão associados ao AWS Service Catalog, pode conseguir adivinhar o usuário. Se esse possível caminho de escalação for motivo de preocupação, o AWS Service Catalog recomenda o uso de `PrincipalType` as `IAM`. Com essa configuração, o `PrincipalARN` já deve existir na conta do destinatário para que possa ser associado.

Quando você adiciona ou remove Nomes de Entidades principais na conta principal, AWS Service Catalog automaticamente aplica as alterações nas contas dos destinatários. Os usuários na conta do destinatário podem então realizar tarefas com base em seu perfil:

- Os usuários finais podem provisionar, atualizar e encerrar o produto do portfólio.
- Os administradores podem associar outras Entidades principais do IAM ao portfólio importado para conceder acesso a usuários finais específicos dessa conta.

> **Note**
>
> O compartilhamento de Nomes de entidades principais está disponível apenas para AWS Organizations.

Compartilhar Nomes de Entidades principais ao compartilhar portfólios

1. No menu de navegação à esquerda, escolha Portfólios.
2. Em Portfólios locais, escolha o portfólio que você deseja compartilhar.
3. No menu Ações, escolha Compartilhar.
4. Selecione uma organização em AWS Organizations.
5. Selecione a raiz da organização inteira, uma unidade organizacional (UO) ou um membro da organização.

6. Nas configurações de compartilhamento, ative a opção Compartilhamento de Entidade principal.

Você também pode atualizar um compartilhamento de portfólio para incluir o compartilhamento do Nome da Entidade principal. Isso compartilha todos os Nomes de Entidades principais que pertencem a esse portfólio com a conta do destinatário.

Para atualizar um compartilhamento de portfólio para ativar ou desativar os Nomes de Entidades principais

1. No menu de navegação à esquerda, escolha Portfólios.
2. Em Portfólio local, escolha o portfólio que você deseja atualizar.
3. Escolha a guia Compartilhar.
4. Selecione o compartilhamento que você deseja atualizar e escolha Compartilhar.
5. Escolha Atualizar compartilhamento e, em seguida, escolha Habilitar para iniciar o compartilhamento principal. AWS Service Catalog então compartilha os Nomes da Entidades principais nas contas dos destinatários.

Desabilite o compartilhamento de entidades principais se quiser parar de compartilhar os Nomes da Entidades principais com contas de destinatários.

Usar curingas ao compartilhar Nomes de Entidades principais

AWS Service Catalog suporta a concessão de acesso ao portfólio aos Nomes das Entidades principais do IAM (usuário, grupo ou perfil) com curingas, como ‘*’ ou ‘?’. Usar padrões curinga permite que você cubra vários Nomes de Entidades principais do IAM ao mesmo tempo. O caminho do ARN e o nome da entidade principal permitem caracteres curinga ilimitados.

Exemplos de um ARN curinga aceitável:

- **`arn:aws:iam:::role/ResourceName_*`**
- **`arn:aws:iam:::role/*/ResourceName_?`**

Exemplos de um ARN curinga inaceitável:

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

No formato ARN da entidade principal do IAM (**`arn:partition:iam:::resource-type/resource-path/resource-name`**), os valores válidos incluem usuário/, grupo/ ou perfil/. O “?” e “*” são permitidos somente após o tipo de recurso no segmento resource-id. Você pode usar caracteres especiais em qualquer lugar dentro do resource-id.

O caractere “*” também corresponde ao caractere “/”, permitindo que caminhos sejam formados dentro do resource-id. Por exemplo: .

`arn:aws:iam:::role/*/ResourceName_?` corresponde a ambos **`arn:aws:iam:::role/pathA/pathB/ResourceName_1`** e **`arn:aws:iam:::role/pathA/ResourceName_1`**.

Compartilhamento e importação de portfólios

Para disponibilizar seus produtos do AWS Service Catalog aos usuários que não estiverem em sua conta da Contas da AWS, como usuários que pertencem a outras organizações ou outras contas da Contas da AWS em sua organização, você pode compartilhar seus portfólios com eles. Você pode compartilhar de várias maneiras, incluindo account-to-account compartilhamento, compartilhamento organizacional e implantação de catálogos usando conjuntos de pilhas.

Antes de compartilhar seus produtos e portfólios com outras contas, você deve decidir se deseja compartilhar uma referência do catálogo ou implantar uma cópia do catálogo em cada conta de destinatário. Observe que, se você implantar uma cópia, deverá reimplantar se houver atualizações que deseja propagar para as contas de destinatário.

Você pode usar conjuntos de pilhas para implantar seu catálogo em várias contas ao mesmo tempo. Se você quiser compartilhar uma referência (uma versão importada do seu portfólio que permanece sincronizada com o original), você pode usar o account-to-account compartilhamento ou compartilhar usandoAWS Organizations.

Se quiser usar conjuntos de pilhas para implantar uma cópia do catálogo, consulte Como configurar um catálogo de várias regiões e várias contas de produtos do AWS Service Catalog padrão da empresa.

Ao compartilhar um portfólio usando o account-to-account compartilhamento ouAWS Organizations, você permite que um AWS Service Catalog administrador de outra AWS conta importe seu portfólio para a conta e distribua os produtos aos usuários finais dessa conta.

Esse portfólio importado não é uma cópia independente. Os produtos e as restrições no portfólio importado permanecem sincronizados com as alterações que você faz no portfólio compartilhado, o portfólio original que você compartilhou. O administrador destinatário, com quem você compartilhou

um portfólio, não pode alterar os produtos nem as restrições, mas pode adicionar acesso ao AWS Identity and Access Management (IAM) para os usuários finais. Para ter mais informações, consulte Conceder acesso aos usuários.

O administrador destinatário pode distribuir os produtos para usuários finais que pertençam à conta da AWS dele das seguintes formas:

- Ao adicionar usuários, grupos e perfis ao portfólio importado.
- Ao adicionar produtos do portfólio importado a um portfólio local, um portfólio separado que o administrador destinatário cria e que pertence à conta da AWS dele. O administrador destinatário então adiciona usuários, grupos e perfis ao portfólio local. Qualquer restrição originalmente aplicadas aos produtos no portfólio compartilhado também estão presentes no portfólio local. O administrador destinatário pode adicionar outras restrições ao portfólio local, mas não pode remover as restrições importadas do portfólio compartilhado.

Quando você adiciona produtos ou restrições ao portfólio compartilhado ou remove produtos ou restrições dele, a alteração se propaga para todas as instâncias do portfólio importado. Por exemplo, se você remover um produto do portfólio compartilhado, ele também será removido do portfólio importado. Ele também será removido de todos portfólios locais aos quais o produto foi adicionado. Se um usuário final tiver lançado um produto antes de você removê-lo, o produto provisionado por ele continuará executando, mas ficará indisponível para futuros lançamentos.

Se você aplicar uma restrição de lançamento a um produto em um portfólio compartilhado, ela será propagada para todas as instâncias importadas do produto. Para substituir esta restrição de lançamento, o administrador destinatário adiciona o produto a um portfólio local e, em seguida, aplica uma restrição de lançamento diferente. A restrição de lançamento em vigor define uma função de lançamento para o produto.

O perfil de lançamento é um perfil do IAM que o AWS Service Catalog usa para provisionar recursos da AWS (como instâncias do Amazon EC2 ou bancos de dados Amazon RDS) quando um usuário final lança o produto. Como administrador, é possível optar por designar um ARN de perfil de lançamento específico ou um nome de perfil local. Se você usar o perfil da ARN, o perfil será usado mesmo que o usuário final pertença a uma conta da AWS diferente da que tem o perfil de execução. Se você usar um nome de perfil local, o perfil do IAM com esse nome na conta do usuário final será usada.

Para obter mais informações sobre restrições e funções de lançamento, consulte Restrições de lançamento do AWS Service Catalog. Como a conta da AWS que tem a função de lançamento

provisiona os recursos da AWS, essa conta está sujeita a cobranças de uso desses recursos. Para obter mais informações, consulte Preços do AWS Service Catalog.

Este vídeo mostra como compartilhar portfólios entre contas em AWS Service Catalog.

Compartilhe (https://www.youtube.com/embed/BVSohYOppjk%22%3EShare) portfólios entre contas em AWS Service Catalog.

> **Note**
>
> Você não pode compartilhar novamente os produtos de um portfólio que tenha sido importado ou compartilhado.

> **Note**
>
> As importações de portfólio devem ocorrer na mesma região entre as contas gerenciais e dependentes.

Relação entre portfólios importados e compartilhados

Essa tabela resume a relação entre um portfólio importado e um portfólio compartilhado, além das ações que um administrador que importa um portfólio pode e não pode realizar no portfólio e nos produtos que ele contém.

Elemento do portfólio compartilhado	Relação de portfólio importado	O administrador destinatário pode	O administrador destinatário não pode
Produtos e suas versões	Herdado. Se o criador do portfólio adicionar ou remover produtos no portfólio compartilhado, a alteração será propagada para o portfólio importado.	Adicionar produtos importados a portfólios locais. Os produtos permanecem sincronizados com o portfólio compartilhado.	Carregar ou adicionar produtos ao portfólio importado ou remover produtos do portfólio importado.

Elemento do portfólio compartilhado	Relação de portfólio importado	O administrador destinatário pode	O administrador destinatário não pode
Restrições de lançamento	Herdado. Se o criador do portfólio adicionar ou remover restrições de lançamento em um produto compartilhado, a alteração será propagada para todas as instâncias importadas do produto. Se o administrador destinatário adicionar um produto importado a um portfólio local, a restrição de lançamento importada aplicada a esse produto estará presente no portfólio compartilhado.	Em um portfólio local, o administrador pode aplicar restrições de lançamento que afetam o lançamento local do produto.	Adicionar ou remover restrições de lançamento no portfólio importado.

Elemento do portfólio compartilhado	Relação de portfólio importado	O administrador destinatário pode	O administrador destinatário não pode
Restrições de modelo	Herdado. Se o criador do portfólio adicionar ou remover restrições de modelo em um produto compartilhado, a alteração será propagada para todas as instâncias importadas do produto. Se o administrador destinatário adicionar um produto importado a um portfólio local, a restrição de modelo importada não será herdada pelo portfólio local.	Em um portfólio local, o administrador pode adicionar restrições de modelo que restringem o produto local.	Remover as restrições de modelo importadas.
Usuários, grupos e funções	Não herdado.	Adicionar usuários, grupos e perfis que estejam na conta de administrador da AWS.	Não aplicável.

Gerenciar produtos

Você pode criar e atualizar produtos criando uma nova versão com base em um modelo atualizado e agrupar produtos em portfólios para distribuí-los aos usuários.

As novas versões de produtos são propagadas para todos os usuários que tenham acesso ao produto por meio de um portfólio. Quando você distribui uma atualização, os usuários finais podem atualizar produtos provisionados existentes.

Tarefas

- Visualizar a página de produtos
- Criar produtos
- Adicionar produtos a portfólios
- Atualizar produtos
- Sincronização de produtos com arquivos de modelo do GitHub, GitHub Enterprise ou Bitbucket
- Excluir produtos
- Gerenciar versões

Visualizar a página de produtos

Você gerencia os produtos na página Lista de produtos no console do administrador do AWS Service Catalog.

Visualizar a página Lista de produtos

1. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/.
2. Escolha Lista de produtos.

Criar produtos

Você cria os produtos na página Products (Produtos) no console do administrador do AWS Service Catalog.

> **Note**
>
> A criação de produtos Terraform exige configuração adicional, incluindo um mecanismo de provisionamento do Terraform e um perfil de lançamento. Para obter mais informações, consulte Conceitos básicos de um produto Terraform.

Para criar um novo produto do AWS Service Catalog

1. Navegue até a página Lista de produtos.
2. Escolha Criar produto e, em seguida, escolha Criar produto.
3. Detalhes do produto - permite que você escolha o tipo de produto que deseja criar. AWS Service Catalog oferece suporte aos tipos de produtos AWS CloudFormation, Terraform Cloud e Externo (suporta Terraform Community Edition). Os detalhes do produto também contêm os metadados que aparecem quando você pesquisa e visualiza produtos em uma lista ou página de detalhes. Insira o seguinte:

   - Nome do produto – o nome do produto.
   - Descrição do produto - a descrição aparece na lista de produtos para ajudar você a escolher o produto correto.
   - Proprietário - a pessoa ou organização que publica este produto. O proprietário pode ser o nome da sua organização de TI ou administrador.
   - Distribuidor (opcional) - o nome do publicador do aplicativo. Esse campo permite que os usuários classifiquem sua lista de produtos para facilitar a localização dos produtos necessários.
4. Os detalhes da versão permitem que você adicione seu arquivo de modelo e crie seu produto. Insira o seguinte:

   - Escolha o método - há quatro maneiras de adicionar um arquivo de modelo.
     - Use um arquivo de modelo local - carregue um modelo AWS CloudFormation ou um arquivo de configuração tar.gz do Terraform a partir de uma unidade local.
     - Use uma URL do Amazon S3 - especifique uma URL que aponte para um modelo AWS CloudFormation ou arquivo de configuração tar.gz do Terraform armazenado no Amazon S3. Se você especificar uma URL do Amazon S3, ele deverá começar com `https://`.
     - Use um repositório externo: especifique seu repositório de código GitHub, GitHub Enterprise ou Bitbucket. AWS Service Catalogpermite sincronizar produtos com arquivos de modelo. Para produtos Terraform, é necessário que o formato do arquivo de modelo seja um único arquivo arquivado em Tar e compactado em Gzip.
     - Use uma CloudFormation pilha existente - insira o ARN de uma CloudFormation pilha existente. Este método não oferece suporte a produtos Terraform Cloud ou externos.
   - Nome da versão (opcional) - o nome da versão do produto (por exemplo, “v1”, “v2beta”). Espaços não são permitidos.

- Descrição (opcional) - uma descrição da versão do produto, incluindo como essa versão difere da versão anterior.
- Orientação - Gerenciado na guia Versões em uma página Detalhes do produto. Quando uma versão do produto é criada, durante o fluxo de trabalho de criação do produto, a orientação para essa versão é definida como padrão. Para saber mais sobre orientação, consulte Gerenciamento de versões.

5. Detalhes do suporte identificam a organização dentro da sua empresa e fornecem um ponto de contato para suporte. Insira o seguinte:

   - Contato por e-mail (opcional) – o endereço de e-mail para relatório de problemas com o produto.
   - Link de suporte (opcional) – uma URL de um site onde os usuários podem localizar informações de suporte ou abrir tickets. A URL deve começar com `http://` ou `https://`. Os administradores são responsáveis por manter a precisão e o acesso às informações de suporte.
   - Descrição do suporte (opcional) – uma descrição de como os usuários devem usar o Contato por e-mail e o Link de suporte.

6. Gerenciar tags (opcional) - além de usar tags para categorizar seus recursos, você também pode usá-las para autenticar suas permissões para criar esse recurso.
7. Criar produto - depois de preencher o formulário, selecione Criar produto. Após alguns segundos, o produto será exibido na página Lista de produtos. Talvez seja necessário atualizar o navegador para ver o produto.

Você também pode usar CodePipeline para criar e configurar um pipeline para implantar seu modelo de produto AWS Service Catalog e entregar as alterações que você fez no seu repositório de origem. Para obter mais informações, consulte Tutorial: criar um pipeline que seja implantado no AWS Service Catalog.

Você pode definir propriedades de parâmetros em seu modelo AWS CloudFormation ou no modelo do Terraform e aplicar essas regras durante o provisionamento. Essas propriedades podem definir o comprimento mínimo e máximo, os valores mínimo e máximo, os valores permitidos e uma expressão regular para o valor. AWS Service Catalog emite um aviso durante o provisionamento se o valor fornecido não estiver de acordo com a propriedade do parâmetro. Para saber mais sobre as propriedades dos parâmetros, consulte Parâmetros no Guia do Usuário AWS CloudFormation.

Solução de problemas

É necessário ter permissão para recuperar objetos dos buckets do Amazon S3. Caso contrário, você poderá encontrar a seguinte mensagem de erro ao iniciar ou atualizar um produto.

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

Se você encontrar essa mensagem, certifique-se de ter permissão para recuperar objetos dos seguintes buckets:

- O bucket em que o modelo do artefato de provisionamento é armazenado.
- O bucket que começa com “cf-templates-*” e onde AWS Service Catalog armazena o modelo do artefato de provisionamento.
- O bucket interno que começa com “sc-*” e onde AWS Service Catalog armazena os metadados. Não será possível ver esse bucket na sua conta.

O exemplo de política a seguir mostra as permissões mínimas necessárias para recuperar objetos dos 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-*/*"
          ]
      }
```

Adicionar produtos a portfólios

Você pode adicionar produtos em qualquer número de portfólios. Quando um produto é atualizado, todos os portfólios que contêm o produto recebem automaticamente a nova versão, incluindo portfólios compartilhados.

Para adicionar um produto de seu catálogo a um portfólio

1. Navegue até a página Lista de produtos.
2. Selecione um produto e, em seguida, escolha Ações. No menu suspenso, escolha Adicionar produto ao portfólio. Você será direcionado para a página Adicionar ***name-of-product*** ao portfólio.
3. Escolha um portfólio e, em seguida, escolha Adicionar produto ao portfólio.

Ao adicionar um produto Terraform a um portfólio, o produto requer uma restrição de lançamento. Você deve selecionar um perfil do IAM na sua conta, inserir um ARN do perfil do IAM ou inserir um nome de perfil. Se você especificar o nome do perfil, quando uma conta usar a restrição de lançamento, o perfil do IAM com esse nome na conta será usado. Isso permite que as restrições de perfil de lançamento sejam independentes da conta para que seja possível criar menos recursos por conta compartilhada. Para obter detalhes e instruções, consulte Etapa 6: Adicionar uma restrição de lançamento ao seu produto Terraform

Um portfólio pode conter vários produtos que são uma mistura dos tipos de produtos AWS CloudFormation e Terraform.

Atualizar produtos

Quando você precisa atualizar o modelo de um produto, você cria uma nova versão do produto. Novas versões do produto são disponibilizadas automaticamente para todos os usuários que têm acesso a um portfólio que contém o produto.

> **Note**
>
> Ao atualizar um produto existente, você não pode alterar o tipo de produto (AWS CloudFormation ou Terraform). Por exemplo, se você atualizar um produto do AWS CloudFormation, não poderá substituir o modelo AWS CloudFormation existente por um arquivo de configuração tar.gz do Terraform. Você deve atualizar o arquivo AWS CloudFormation de modelo existente com um novo arquivo AWS CloudFormation de modelo.

Os usuários finais que estiverem executando um produto provisionado da versão anterior do produto no momento podem atualizar seu produto provisionado para a nova versão. Quando uma nova versão de um produto está disponível, os usuários podem usar o comando Atualizar produto provisionado nas páginas Lista de produto provisionado ou Detalhes do produto provisionado.

Antes de criar uma nova versão de um produto, AWS Service Catalog recomenda que você teste as atualizações do produto no AWS CloudFormation ou no mecanismo Terraform para garantir que funcionem corretamente.

Para criar uma nova versão do produto

1. Navegue até a página Lista de produtos.
2. Escolha o produto que você deseja atualizar. Você será direcionado para a página de Detalhes do produto.
3. Na página Detalhes do produto, expanda a guia Versões e, em seguida, escolha Criar nova versão.
4. Em Detalhes da versão, faça o seguinte:
   - Escolha o modelo - há quatro maneiras de adicionar um arquivo de modelo.

     Use um arquivo de modelo local - carregue um modelo AWS CloudFormation ou um arquivo de configuração tar.gz do Terraform a partir de uma unidade local.

     Use uma URL do Amazon S3 - especifique uma URL que aponte para um modelo AWS CloudFormation ou arquivo de configuração tar.gz do Terraform armazenado no Amazon S3. Se você especificar uma URL do Amazon S3, dele deverá começar com https://.

     Use um repositório externo: especifique seu repositório de código GitHub, GitHub Enterprise ou Bitbucket. AWS Service Catalogpermite sincronizar produtos com arquivos de modelo. Para produtos Terraform, é necessário que o formato do arquivo de modelo seja um único arquivo arquivado em Tar e compactado em Gzip.

     Use uma CloudFormation pilha existente - insira o ARN de uma CloudFormation pilha existente. Este método não oferece suporte a produtos Terraform Cloud ou externos.
   - Bloco de versão - nome da versão do produto (por exemplo, “v1”, “v2beta”). Espaços não são permitidos.
   - Descrição (opcional) — uma descrição da versão do produto incluindo como essa versão difere da versão anterior.
5. Escolha Criar versão de produto.

Você também pode usar CodePipeline para criar e configurar um pipeline para implantar seu modelo de produto e entregar suas alterações em seu repositório de origem. AWS Service Catalog Para

obter mais informações, consulte Tutorial: criar um pipeline que seja implantado no AWS Service Catalog.

Sincronização de produtos com arquivos de modelo do GitHub, GitHub Enterprise ou Bitbucket

AWS Service Catalog permite sincronizar produtos com arquivos de modelo que são gerenciados por meio de um provedor de repositório externo. AWS Service Catalog refere-se a produtos com esse tipo de conexão de modelo como produtos sincronizados com Git. As opções de repositório incluem GitHub GitHub Enterprise ou Bitbucket. Depois de autorizar sua conta Conta da AWS com um repositório externo, você pode criar novos AWS Service Catalog produtos ou atualizar produtos existentes para sincronizar com um arquivo de modelo no repositório. Quando alterações são feitas no arquivo de modelo e confirmadas no repositório (por exemplo, usando git-push), AWS Service Catalog automaticamente detecta as alterações e cria uma nova versão do produto (artefato).

Tópicos

Permissões necessárias para sincronizar produtos com arquivos de modelo externos

Você pode usar a política a seguir AWS Identity and Access Management (IAM) como modelo para permitir que AWS Service Catalog os administradores sincronizem produtos com arquivos de modelo de um repositório externo. Essa política inclui as permissões necessárias de ambos CodeConnections AWS Service Catalog e. AWS Service Catalog recomenda que você copie o modelo de política abaixo e também use a política AWS Service Catalog`AWSServiceCatalogAdminFullAccess` gerenciada ao habilitar produtos sincronizados com o repositório.

```
{
```

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

Crie uma conexão de conta

Antes de sincronizar um arquivo de modelo com um AWS Service Catalog produto, você deve criar e autorizar uma conexão única. account-to-account Você usa essa conexão para especificar os detalhes do repositório que contém o arquivo de modelo desejado. Você pode criar uma conexão usando o AWS Service Catalog console, o CodeConnections console AWS Command Line Interface (CLI) ou CodeConnections as APIs.

Depois de estabelecer uma conexão, você pode usar o AWS Service Catalog console, a AWS Service Catalog API ou a CLI para criar um produto sincronizado AWS Service Catalog . AWS Service Catalog os administradores podem criar produtos novos ou atualizar AWS Service Catalog produtos existentes com base em um arquivo de modelo em um repositório e ramificação. Se uma alteração for confirmada no repositório, a AWS Service Catalog detectará automaticamente e criará uma nova versão do produto. As versões anteriores do produto são mantidas até o limite de versão prescrito e atribuiu um status obsoleto.

Além disso, cria AWS Service Catalog automaticamente uma função vinculada ao serviço (SLR) após a criação da conexão. Essa SLR permite AWS Service Catalog detectar qualquer alteração no arquivo de modelo que esteja confirmada no repositório. A SLR também permite AWS Service Catalog criar automaticamente novas versões de produtos para produtos sincronizados. Para obter mais informações sobre permissões e funcionalidades da SLR, consulte Perfis vinculados ao serviço para AWS Service Catalog.

Como criar um novo produto sincronizado com o Git

1. No painel de navegação, escolha Lista de produtos e, em seguida, selecione Criar produto.
2. Insira os Detalhes do produto.
3. Em Detalhes da versão, escolha Especificar seu repositório de código usando um AWS CodeStar provedor e, em seguida, escolha o link Criar uma nova AWS CodeStar conexão.
4. Depois de criar a conexão, atualize a lista de conexões e selecione a nova conexão. Especifique os detalhes do repositório, incluindo o repositório, a ramificação e o caminho do arquivo de modelo.

   Para obter mais informações sobre o uso de arquivos de configuração Terraform, consulte Sincronização de produtos Terraform com arquivos de modelo do GitHub, GitHub Enterprise ou Bitbucket .

   a. (Opcional ao criar um novo recurso de AWS Service Catalog produto) Na seção Support Details, adicione metadados do produto.

   b. (Opcional ao criar um novo recurso de AWS Service Catalog produto) Na seção Tags, escolha Adicionar nova tag e insira os pares de chave e valor.
5. Selecione Criar novo produto.

Para criar vários produtos sincronizados com o Git

1. No painel de navegação esquerdo do AWS Service Catalog console, escolha Lista de produtos e, em seguida, escolha Criar vários produtos gerenciados pelo git.
2. Insira os Detalhes comuns do produto.
3. Em Detalhes do repositório externo, selecione uma conexão AWS CodeStar e, em seguida, especifique o repositório e a ramificação.
4. No painel Adicionar produtos, insira o Caminho do arquivo de modelo e o Nome do produto. Escolha Adicionar novo item e continue adicionando produtos conforme desejado.
5. Depois de adicionar todos os produtos desejados, escolha Criar produtos em massa.

Para conectar um AWS Service Catalog produto existente a um repositório externo

1. No painel de navegação esquerdo do AWS Service Catalog console, escolha Lista de produtos e, em seguida, escolha Conectar produtos a um repositório externo.
2. Na página Selecionar produtos, escolha os produtos que você deseja conectar a um repositório externo e escolha Próximo.
3. Na página Especificar detalhes da fonte, selecione uma AWS CodeStar conexão existente e, em seguida, especifique o repositório, a ramificação e o caminho do arquivo de modelo.
4. Escolha Próximo.
5. Na página Revisar e enviar, verifique os detalhes da conexão e escolha Conectar produtos a um repositório externo.

Visualizar conexões de produtos sincronizadas com o Git

Você pode usar o AWS Service Catalog console, a API ou visualizar AWS CLI os detalhes da conexão do repositório. Para AWS Service Catalog produtos vinculados a um arquivo de modelo, você pode recuperar informações sobre a conexão do repositório e a última vez em que o modelo foi sincronizado com o produto a partir do Status da última sincronização.

> **Note**
>
> Você pode visualizar as informações do repositório e o Status da última sincronização no nível do produto. Os usuários devem ter permissões do IAM nas CodeConnections APIs para visualizar os detalhes do repositório. Consulte Permissões necessárias para sincronizar

AWS Service Catalog produtos com arquivos de modelo para obter mais informações sobre a política necessária para essas permissões do IAM.

Para visualizar os detalhes da conexão e do repositório usando AWS Management Console

1. No painel de navegação à esquerda, escolha Lista de produtos.
2. Selecione o produto na lista.
3. Na página Produto, navegue até a seção Detalhes da fonte do produto.
4. Para ver a ID da revisão de origem de uma versão do produto, escolha o link Última versão criada. A seção Detalhes da versão exibe a ID da revisão de origem.

Para visualizar os detalhes da conexão e do repositório usando AWS CLI

A partir do AWS CLI, execute os seguintes comandos:

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

$ aws servicecatalog describe-provisioning-artifact

$ aws servicecatalog search-product-as-admin

$ aws servicecatalog list-provisioning-artifacts
```

Atualizar conexões de produtos sincronizadas com o Git

Você pode atualizar as conexões de contas existentes e os produtos sincronizados com o Git usando o AWS Service Catalog console, AWS Service Catalog a API ou. AWS CLI

Para saber como conectar um AWS Service Catalog produto existente a um arquivo de modelo, consulte Criação de novas conexões de produto sincronizadas com o Git.

Para atualizar os produtos existentes para produtos sincronizados com o Git

1. No painel de navegação à esquerda, escolha Lista de produtos e, em seguida, escolha uma das seguintes opções:
   - Para atualizar um único produto, selecione o produto, navegue até a seção Detalhes da fonte do produto e escolha Editar detalhes.

- Para atualizar vários produtos, escolha Conectar produtos a um repositório externo, selecione até dez produtos e escolha Próximo.

2. Na seção Detalhes da fonte do produto, execute as seguintes atualizações:

   - Especificar a conexão.
   - Especificar o repositório.
   - Especificar a ramificação.
   - Nomear o arquivo de modelo.

3. Escolha Salvar alterações.

> **Note**
>
> Para produtos que ainda não estão conectados a um repositório externo, você pode usar a opção Conectar a um repositório externo exibida no alerta na parte superior da página de informações do produto após selecionar o produto.

Você também pode usar o AWS Service Catalog console ou AWS CLI o

- Conectar um AWS Service Catalog produto existente a um arquivo de modelo em um repositório externo
- Atualize os metadados do produto, incluindo nome, descrição e tags do produto.
- Reconfigure (atualize a sincronização para usar uma fonte de repositório diferente) uma conexão para um produto AWS Service Catalog conectado anteriormente.

Para atualizar os detalhes da conexão e do repositório usando o console AWS Service Catalog

1. No painel de navegação esquerdo do AWS Service Catalog console, escolha Lista de produtos e selecione um produto que esteja atualmente conectado a um repositório externo.
2. Na seção Detalhes da fonte do produto, escolha Editar fonte do produto.
3. Na seção Detalhes da fonte do produto, especifique o novo repositório desejado.
4. Escolha Salvar alterações.

Para atualizar os detalhes da conexão e do repositório usando AWS CLI

A partir da AWS CLI execução dos `$ aws servicecatalog update-provisioning-artifact` comandos `$ aws servicecatalog update-product` e.

Excluir conexões de produtos sincronizadas com o Git

Você pode excluir uma conexão entre um AWS Service Catalog produto e um arquivo de modelo usando o AWS Service Catalog console, a CodeConnections API ou AWS CLI. Quando você desconecta um produto de um arquivo de modelo, o AWS Service Catalog produto sincronizado muda para um produto gerenciado regularmente. Depois de desconectar o produto, se o arquivo de modelo for alterado e confirmado no repositório conectado anteriormente, as alterações não serão refletidas. Para reconectar um AWS Service Catalog produto a um arquivo de modelo em um repositório externo, consulte Atualização de conexões e produtos sincronizados AWS Service Catalog.

Para desconectar um produto sincronizado com o Git usando o console AWS Service Catalog

1. No AWS Management Console, escolha Lista de produtos no painel de navegação esquerdo.
2. Selecione um produto na lista.
3. Na página Produto, navegue até a seção Detalhes da fonte do produto.
4. Escolha Desconectar.
5. Confirme a ação e escolha Desconectar.

Para desconectar um produto sincronizado com o Git usando AWS CLI

A partir do AWS CLI, execute o `$ aws servicecatalog update-product` comando. Na entrada `ConnectionParameters`, remova a conexão especificada.

Para excluir uma conexão usando a CodeConnections API ou AWS CLI

Na CodeConnections API ou AWS CLI, execute o `$ aws codestar-connections delete-connection` comando.

Sincronização de produtos Terraform com arquivos de modelo do GitHub, GitHub Enterprise ou Bitbucket

Ao criar um produto sincronizado com o Git usando um arquivo de configuração do Terraform, o caminho do arquivo aceita somente o formato tar.gz. Os formatos de pasta do Terraform não são aceitos no caminho do arquivo.

Região da AWS suporte para produtos sincronizados com Git

AWS Service Catalog suporta produtos sincronizados com o Git Regiões da AWS conforme indicado na tabela abaixo.

Região da AWS nome	Região da AWS identidade	Suporte para produtos sincronizados com o Git
Leste dos EUA (Norte da Virgínia)	us-east-1	Sim
Leste dos EUA (Ohio)	us-east-2	Sim
Oeste dos EUA (Norte da Califórnia)	us-west-1	Sim
Oeste dos EUA (Oregon)	us-west-2	Sim
África (Cidade do Cabo)	af-south-1	Não
Ásia-Pacífico (Hong Kong)	ap-east-1	Não
Ásia-Pacífico (Jacarta)	ap-southeast-3	Não
Ásia-Pacífico (Mumbai)	ap-south-1	Sim
Asia Pacific (Osaka)	ap-northeast-3	Não
Ásia-Pacífico (Seul)	ap-northeast-2	Sim
Ásia-Pacífico (Singapura)	ap-southeast-1	Sim
Ásia-Pacífico (Sydney)	ap-southeast-2	Sim
Ásia-Pacífico (Tóquio)	ap-northeast-1	Sim
Canadá (Central)	ca-central-1	Sim
Europa (Frankfurt)	eu-central-1	Sim
Europa (Irlanda)	eu-west-1	Sim
Europa (Londres)	eu-west-2	Sim

Região da AWS nome	Região da AWS identidade	Suporte para produtos sincronizados com o Git
Europa (Milão)	eu-south-1	Não
Europa (Paris)	eu-west-3	Sim
Europa (Estocolmo)	eu-north-1	Sim
Oriente Médio (Barém)	me-south-1	Não
América do Sul (São Paulo)	sa-east-1	Sim
AWS GovCloud (Leste dos EUA)	us-gov-east-1	Não
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	Não

Excluir produtos

Quando você exclui um produto, AWS Service Catalog remove todas as versões do produto de cada portfólio que o contém.

AWS Service Catalog permite excluir um produto usando o console do AWS Service Catalog ou a AWS CLI. Para excluir um produto com sucesso, você deve primeiro desassociar todos os recursos associados ao produto. Exemplos de associações de recursos de produtos incluem associações de portfólio TagOptions, orçamentos e ações de serviço.

> **Important**
>
> Você não pode recuperar um produto depois que ele for excluído.

Para excluir um produto usando o console do AWS Service Catalog

1. Navegue até a página Portfólios e selecione o portfólio que contém o produto que você deseja excluir.
2. Selecione o produto que você deseja excluir e escolha Excluir na parte superior direita do painel de produtos.

3. Para produtos sem recursos associados, confirme o produto que você deseja excluir digitando excluir na caixa de texto e escolha Excluir.

   Para produtos com recursos associados, prossiga para a etapa 4.
4. Na janela Excluir produto, revise a tabela Associações, que exibe todos os recursos associados ao produto. AWS Service Catalog tenta desassociar esses recursos quando você exclui o produto.
5. Confirme que você deseja excluir o produto e remover todos os recursos associados inserindo excluir na caixa de texto.
6. Escolha Desassociar e excluir.

Se AWS Service Catalog não conseguir desassociar todos os recursos do produto, o produto não será excluído. A janela Excluir produto exibe o número de dissociações com falha e uma descrição de cada falha. Para obter mais informações sobre como resolver dissociações de recursos com falha ao excluir um produto, consulte Resolver dissociações de recursos com falha ao excluir um produto abaixo.

Tópicos

- Excluir produtos usando o AWS CLI
- Resolver falhas na dissociação de recursos ao excluir um produto

Excluir produtos usando o AWS CLI

AWS Service Catalog permite que você use o AWS Command Line Interface(AWS CLI) para excluir produtos do seu portfólio. A AWS CLI é uma ferramenta de código aberto que permite interagir com os serviços da AWS usando comandos no shell da linha de comando. O perfil AWS Service Catalog de exclusão forçada requer um alias da AWS CLI, que é um atalho que você pode criar na AWS CLI para encurtar comandos ou scripts que utiliza com frequência.

Pré-requisitos

- Instale e configure a AWS CLI. Para obter mais informações, consulte Instalação ou atualização da versão mais recente da AWS CLI e Configuração básica. Usar, no mínimo, a AWS CLI versão 1.11.24 ou 2.0.0.

- O alias da CLI de exclusão do produto requer um terminal compatível com bash e o processador JQ de linha de comando JSON. Para obter mais informações sobre como instalar o processador JSON de linha de comando, consulte Download jq.
- Crie um alias da AWS CLI para chamadas de API `Disassociation` em lote, permitindo que você exclua um produto em um único comando.

Para excluir um produto com sucesso, você deve primeiro desassociar todos os recursos associados ao produto. Exemplos de associações de recursos de produtos incluem associações de portfólio, orçamentos, opções de tags e ações de atendimento. Ao usar a CLI para excluir um produto, o alias `force-delete-product` da CLI permite que você chame a API `Disassociate` para desassociar quaisquer recursos que impeçam a API `DeleteProduct`. Isso evita uma chamada separada para dissociações individuais.

> **Note**
>
> Os caminhos de arquivo mostrados nos procedimentos abaixo podem variar dependendo do sistema operacional usado para realizar essas ações.

Criação de um alias AWS CLI para excluir produtos AWS Service Catalog

Ao usar o AWS CLI para excluir um produto AWS Service Catalog, o alias `force-delete-product` da CLI permite que você chame a API `Disassociate` para desassociar quaisquer recursos que impeçam a chamada `DeleteProduct`.

Crie um arquivo **`alias`** em sua pasta de configuração da AWS CLI.

1. No console AWS CLI, navegue até a pasta de configuração. Por padrão, a pasta de configuração é `~/.aws/` no Linux e no macOS ou `%USERPROFILE%\.aws\` no Windows.
2. Crie uma subpasta chamada `cli` usando a navegação de arquivos ou digitando o seguinte comando em seu terminal preferido:

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

   O caminho padrão da pasta `cli` resultante é `~/.aws/cli/` no Linux e no macOS ou `%USERPROFILE%\.aws\cli` no Windows.

3. Na nova pasta `cli`, crie um arquivo de texto chamado `alias` sem extensão de arquivo. Você pode criar o arquivo `alias` usando a navegação de arquivos ou digitando o seguinte comando no terminal de sua preferência:

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

4. Entre `[toplevel]` na primeira linha.
5. Salve o arquivo.

Em seguida, você pode adicionar o force-delete-product alias ao seu `alias` arquivo colando manualmente o script de alias no arquivo ou usando um comando na janela do terminal.

Adicione manualmente o force-delete-product alias ao seu arquivo **`alias`**

1. No console da AWS CLI, navegue até a pasta AWS CLI de configuração e abra o arquivo `alias`.
2. Insira o seguinte alias de código no arquivo, abaixo da linha `[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. Salve o arquivo.

Use a janela do terminal para adicionar o force-delete-product alias ao seu arquivo **`alias`**

1. Abra uma janela de terminal e execute o seguinte comando:

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

2. Cole o script de alias na janela do terminal e pressione CTRL+D para sair do comando `cat`.

Ligue para o force-delete-product pseudônimo

1. Na janela do terminal, execute os comandos seguintes para chamar o alias do produto excluído

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

   O exemplo abaixo mostra o comando alias `force-delete-product` e sua resposta 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. Digite y para confirmar se você deseja excluir o produto.

Depois de excluir o produto com sucesso, a janela do terminal exibe os seguintes resultados

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

Recursos adicionais

Para obter mais informações sobre AWS CLI, usando aliases e excluindo produtos AWS Service Catalog, consulte os seguintes recursos:

- Criação e uso de aliases AWS CLI no Guia do Usuário AWS Command Line Interface(CLI).
- Repositório do alias AWS CLI do repositório git.
- Excluir produtos do AWS Service Catalog.
- AWSre:Invent 2016: O usuário AWS CLI efetivo em. YouTube

Resolver falhas na dissociação de recursos ao excluir um produto

Se sua tentativa anterior de excluir um produto falhou devido a exceções de dissociação de recursos, consulte a lista de exceções e suas resoluções abaixo.

> **Note**
>
> Se você fechou a janela Excluir produtos antes de receber a mensagem de falha na dissociação de recursos, poderá seguir as etapas de um a três na seção Excluir um produto em andamento para abrir a janela novamente.

Como resolver uma falha na dissociação de recursos

Na janela Excluir produto, revise a coluna Status da tabela de associações. Identifique a exceção de falha na dissociação de recursos e as resoluções sugeridas:

Tipo de exceção de status	Causa	Resolução
Produto prod-****	AWS Service Catalognão foi possível excluir o produto porque o produto ainda tem orçamentos associados TagOptions, pelo menos um `ProvisioningArtifact` com ações associadas, o produto ainda está atribuído a um portfólio, o produto tem usuários ou o produto tem restrições.	Tente excluir o produto novamente.
Usuário: `username` não tem autorização para executar:	O usuário que está tentando excluir o produto não tem as permissões necessárias para desassociar os recursos do produto.	AWS Service Catalog recomenda entrar em contato com o administrador da sua conta para obter mais informações sobre como desassociar recursos de produtos que você atualmente não tem permissão para desassociar.

Gerenciar versões

Você atribui versões do produto ao criar um produto, além de poder atualizar versões de produto a qualquer momento.

As versões têm um modelo do AWS CloudFormation, um título, uma descrição, um status e orientações.

Status da versão

Uma versão pode ter um dos três status:

- Active (Ativa) – uma versão ativa aparece na lista de versões e permite que os usuários a lancem.
- Inactive (Inativa) – uma versão inativa está oculta na lista de versões. Os produtos provisionados existentes lançados a partir desta versão não serão afetados.
- Excluído - se uma versão for excluída, ela será removida da lista de versões. A exclusão de uma versão não pode ser desfeita.

Orientação da versão

Você pode definir a orientação da versão para fornecer informações a usuários finais sobre a versão do produto. A orientação da versão afeta somente as versões de produto ativas.

Há duas opções para a orientação da versão:

- Nenhum - por padrão, as versões do produto não têm nenhuma orientação. Os usuários finais podem usar essa versão para atualizar e lançar produtos provisionados.
- Obsoleto - os usuários não podem lançar novos produtos provisionados usando uma versão obsoleta do produto. Se um produto provisionado lançado anteriormente usa uma versão agora obsoleta, os usuários só podem atualizar esse produto provisionado usando a versão existente ou uma nova versão.

Atualizar versões

Você atribui versões do produto ao criar um produto e também pode atualizar uma versão a qualquer momento. Para obter mais informações sobre como criar um produto, consulte Criar produtos.

Como atualizar uma versão do produto

1. No console do AWS Service Catalog, escolha Products (Produtos).
2. Na lista de produtos, escolha o produto cuja versão deseja atualizar.
3. Na página Product details (Detalhes do produto), escolha a guia Versions (Versões) e escolha a versão que deseja atualizar.
4. Na página Version details (Detalhes da versão), edite a versão do produto e escolha Save changes (Salvar alterações).

Uso de restrições do AWS Service Catalog

Você aplica restrições para controlar as regras que serão aplicadas a um produto em um portfólio específico quando os usuários finais o iniciarem. Quando os usuários finais iniciarem o produto, verão as regras aplicadas usando as restrições. Você pode aplicar restrições a um produto após ele ser inserido em um portfólio. As restrições são ativadas logo após sua criação e são aplicadas a todas as versões atuais de um produto que ainda não foram lançadas.

Restrições

- Restrições de lançamento do AWS Service Catalog
- Restrições de notificação do AWS Service Catalog
- Restrições de atualização de tags do AWS Service Catalog
- Restrições do conjunto de pilhas do AWS Service Catalog
- Restrições de modelo do AWS Service Catalog

Restrições de lançamento do AWS Service Catalog

Uma restrição de lançamento especifica um perfil (IAM) do AWS Identity and Access Management que o AWS Service Catalog assume quando um usuário final lança um produto. Um perfil do IAM é um conjunto de permissões que um usuário ou serviço da AWS pode assumir temporariamente para usar os serviços da AWS. Como exemplo de apresentação, consulte:

- Tipo de produto AWS CloudFormation: Etapa 6: Adicionar uma restrição de lançamento para atribuir um perfil do IAM
- Tipo de produto Terraform Open Source ou Terraform Cloud: Etapa 5: Criar funções de lançamento

As restrições de lançamento se aplicam aos produtos do portfólio (associação produto-portfólio). As restrições de lançamento não se aplicam ao nível do portfólio ou a um produto em todos os portfólios. Para associar uma restrição de lançamento a todos os produtos em um portfólio, aplique a restrição de lançamento a cada produto individualmente.

Sem uma restrição de lançamento, os usuários finais devem lançar e gerenciar produtos usando suas próprias credenciais do IAM. Para fazer isso, eles devem ter permissões para o AWS CloudFormation, os serviços da AWS usados pelos produtos e o AWS Service Catalog. Ao usar um perfil de lançamento, você pode limitar as permissões dos usuários finais ao mínimo de que eles

precisam para esse produto. Para obter mais informações sobre as permissões dos usuários finais, consulte Gerenciamento de identidades e acesso no AWS Service Catalog.

Para criar e atribuir perfis do IAM, você deve ter as seguintes permissões administrativas do IAM:

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

Configuração de uma função de lançamento

O perfil do IAM que você atribui a um produto como restrição de lançamento deve ter permissões para usar o seguinte:

Para produtos Cloudformation

- A política gerenciada do `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess` AWS CloudFormation
- Os serviços usados no modelo do AWS CloudFormation para o produto
- Leia o acesso ao modelo AWS CloudFormation em um bucket Amazon S3 de propriedade do serviço.

Para produtos Terraform

- Os serviços usados no modelo do Amazon S3 para o produto
- Leia o acesso ao modelo Amazon S3 em um bucket Amazon S3 de propriedade do serviço.
- `resource-groups:Tag` para marcação em uma instância do Amazon EC2 (assumida pelo mecanismo de provisionamento do Terraform ao realizar operações de provisionamento)
- `resource-groups:CreateGroup` para marcação de grupos de recursos (assumida por AWS Service Catalog para criar grupos de recursos e atribuir tags)

A política de confiança do perfil do IAM deve permitir ao AWS Service Catalog Assumir o perfil. No procedimento abaixo, a política de confiança será definida automaticamente quando você selecionar AWS Service Catalog como tipo de perfil. Se você não estiver usando o console, consulte a seção

Criar políticas de confiança para serviços da AWS que assumem perfis em Como usar políticas de confiança com perfis do IAM.

> **Note**
>
> As permissões `servicecatalog:ProvisionProduct`, `servicecatalog:TerminateProvisionedProduct` e `servicecatalog:UpdateProvisionedProduct` não podem ser atribuídas na função de lançamento. Você deve usar perfis do IAM, como mostrado nas etapas da política em linha na seção Ceder permissões para Usuários finais do AWS Service Catalog.

> **Note**
>
> Para visualizar os produtos e recursos provisionados do Cloudformation no console do AWS Service Catalog, os usuários finais precisam de acesso de leitura do AWS CloudFormation. A visualização de produtos e recursos provisionados no console não usa o perfil de lançamento.

Para criar uma função de lançamento

1. Abra o console IAM em https://console.aws.amazon.com/iam/.

   Os produtos Terraform exigem configurações adicionais de perfil de lançamento. Para obter mais informações, consulte a Etapa 5: Criar perfis de lançamento em Conceitos básicos de um produto Terraform Open Source.
2. Escolha Perfis.
3. Escolha Criar nova função.
4. Insira um nome de função e escolha Next Step.
5. Em Perfis de serviço da AWS próximo a AWS Service Catalog, escolha Selecionar.
6. Na página Attach Policy (Anexar política), escolha Next Step (Próxima etapa).
7. Para criar a função, escolha Create Role (Criar função).

Para anexar uma política à nova função

1. Escolha a função que você criou para visualizar a página de detalhes da função.

2. Escolha a guia Permissions (Permissões) e expanda a seção Inline Policies. Em seguida, escolha click here (clique aqui).
3. Escolha Custom Policy e depois Select.
4. Insira um nome para a política, depois cole o seguinte no editor Policy Document (Documento da política):

```
          "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObject"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "s3:ExistingObjectTag/servicecatalog:provisioning":"true"
            }
         }
   ]
}
```

> **Note**
>
> Ao configurar um perfil de lançamento para uma restrição de lançamento, você deve usar esta string: `"s3:ExistingObjectTag/servicecatalog:provisioning":"true"`.

5. Adicione uma linha à política para cada serviço adicional que o produto usa. Por exemplo, para adicionar a permissão para o Amazon Relational Database Service (Amazon RDS), digite uma vírgula no final da última linha, na lista `Action` e adicione a seguinte linha:

```
"rds:*"
```

6. Escolha Aplicar política.

Aplicação de uma restrição de lançamento

Depois de configurar o perfil de lançamento, atribua o perfil ao produto como uma restrição de lançamento. Essa ação pede ao AWS Service Catalog que assuma o perfil quando um usuário final lançar o produto.

Para atribuir a função a um produto

1. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/.
2. Escolha o portfólio que contenha o produto.
3. Escolha a guia Constraints (Restrições) e Create constraint (Criar restrição).
4. Escolha o produto em Product (Produto) e selecione Launch (Iniciar) em Constraint type (Tipo de restrição). Escolha Continuar.
5. Na seção Restrição de lançamento, é possível selecionar um perfil do IAM em sua conta, inserir um ARN de perfil do IAM ou inserir o nome do perfil.

   Se você especificar o nome do perfil, quando uma conta usar a restrição de lançamento, é esse perfil do IAM que a conta usará. Essa abordagem permite que as restrições de perfil de lançamento sejam independentes da conta para que seja possível criar menos recursos por conta compartilhada.

   > **Note**
   >
   > O nome do perfil fornecido deve existir na conta que criou a restrição de lançamento e a conta do usuário que executa um produto com essa restrição de lançamento.

6. Depois de especificar a função do IAM, escolha Create (Criar).

Adicionar Confused Deputy à restrição de lançamento

AWS Service Catalog oferece suporte à proteção Confused Deputy para as APIs que são executadas com uma solicitação Assumir Perfil. Ao adicionar uma restrição de lançamento, você pode restringir o acesso ao perfil de lançamento usando as condições `sourceAccount` e `sourceArn` da política de confiança do perfil de lançamento. Isso garante que o perfil de lançamento seja chamado por uma fonte confiável.

No exemplo a seguir, o usuário final AWS Service Catalog pertence à conta 111111111111. Quando o administrador AWS Service Catalog cria um `LaunchConstraint` para um produto, o usuário

final pode especificar as seguintes condições na política de confiança do perfil de lançamento para restringir Assumir Perfil à conta 111111111111.

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

}
```

Um usuário que provisiona um produto com o `LaunchConstraint` deve ter o mesmo `AccountId` (111111111111). Caso contrário, a operação falhará com um erro `AccessDenied`, impedindo o uso indevido do perfil de lançamento.

As seguintes APIs AWS Service Catalog são protegidas para a proteção do Confused Deputy:

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

A proteção `sourceArn` para AWS Service Catalog somente oferece suporte a ARNs modelados, como “`arn:<aws-partition>:servicecatalog:<region>:<accountId>:`” Ela não oferece suporte a ARNs de recursos específicos.

Verificar a restrição de lançamento

Verifique se o AWS Service Catalog usa o perfil para lançar o produto e se o produto provisionado foi criado com êxito ao lançar o produto pelo console do AWS Service Catalog. Para testar uma restrição antes de liberá-lo aos usuários, crie um portfólio de teste que contenha os mesmos produtos e teste as restrições com esse portfólio.

Para iniciar um produto

1. No menu do console do AWS Service Catalog, escolha Service Catalog, Usuário final.
2. Escolha o produto para abrir a página Detalhes do produto. Na tabela Opções de lançamento, verifique se o nome do recurso da Amazon (ARN) do perfil é exibido.
3. Escolha Lançar produto.
4. Siga as etapas de lançamento, preenchendo todas as informações necessárias.
5. Verifique se o produto inicia corretamente.

Restrições de notificação do AWS Service Catalog

> **Note**
>
> AWS Service Catalog não suporta restrições de notificação para produtos Terraform Open Source ou Terraform Cloud.

A restrição de notificação especifica um tópico do Amazon SNS para receber notificações sobre eventos de pilha.

Use o procedimento a seguir para criar um tópico do SNS e inscreva-se nele.

Para criar um tópico do SNS e uma inscrição

1. Abra o console do Amazon SNS em https://console.aws.amazon.com/sns/v3/home.
2. Escolha Criar tópico.
3. Digite o nome de um tópico e escolha Create topic (Criar tópico).
4. Selecione Criar assinatura.
5. Em Protocol (Protocolo), selecione Email. Em Endpoint, digite um endereço de e-mail que você pode usar para receber as notificações. Selecione Create subscription.
6. Você receberá um e-mail de confirmação com a linha de assunto `AWS Notification - Subscription Confirmation`. Abra o e-mail e siga as instruções para concluir a sua assinatura.

Use o procedimento a seguir para aplicar uma restrição de notificação usando o tópico do SNS que você criou usando o procedimento anterior.

Para aplicar uma restrição de notificação a um produto

1. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/.
2. Escolha o portfólio que contenha o produto.
3. Expanda Constraints (Restrições) e escolha Add constraints (Adicionar restrições).
4. Escolha o produto em Produto e defina Tipo de restrição como Notificação. Escolha Continuar.
5. Escolha Choose a topic from your account (Escolher um tópico da sua conta) e selecione o tópico do SNS que você criou em Topic Name (Nome do tópico).
6. Selecione Enviar.

Restrições de atualização de tags do AWS Service Catalog

> **Note**
>
> AWS Service Catalog não suporta restrições de atualização de tags para produtos Terraform Open Source.

Com as restrições de atualização de tags, os administradores do AWS Service Catalog podem permitir ou não que os usuários finais atualizem tags nos recursos associados a um produto provisionado. Se a atualização de tags for permitida, as novas tags associadas ao produto ou portfólio serão aplicadas aos recursos provisionados durante uma atualização de produto provisionado.

Para habilitar as atualizações de tags a um produto

1. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/.
2. Escolha o portfólio que contém o produto que deseja atualizar.
3. Escolha a guia Restrições e Adicionar restrições.
4. Em Constraint type (Tipo de restrição) e selecione Tag Update (Atualização de tag).
5. Escolha o produto em Product (Produto) e selecione Continue (Continuar).
6. Na Tag Updates page (Página de atualizações de tag), selecione Enable Tag Updates (Habilitar atualizações de tag).
7. Selecione Enviar.

Restrições do conjunto de pilhas do AWS Service Catalog

> **Note**
>
> - AWS Service Catalog não suporta restrições de conjunto de pilhas para produtos Terraform Open Source.
> - AutoTags atualmente não são compatíveis com AWS CloudFormation StackSets.

Uma restrição de conjunto de pilhas permite que você configure as opções de implantação do produto usando o. AWS CloudFormation StackSets Você pode especificar várias contas e regiões para o lançamento do produto. Os usuários finais podem gerenciar essas contas e determinar onde os produtos são implantados e a ordem de implantação.

Para aplicar uma restrição do conjunto de pilhas a um produto

1. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/.
2. Escolha o portfólio com o produto que você deseja.
3. Escolha a guia Restrições e Criar restrições.
4. Em Produto, escolha o produto. Em Tipo de restrição, escolha Conjunto de pilhas.
5. Configure as contas, regiões e permissões para as restrições do seu conjunto de pilhas.
   - Nas Configurações da conta, identifique as contas nas quais você deseja criar produtos.
   - Nas Configurações de região, escolha as regiões geográficas para implantar produtos e a ordem em que você deseja que esses produtos sejam implantados nessas regiões.
   - Em Permissões, escolha uma função de StackSet administrador do IAM para gerenciar suas contas de destino. Se você não escolher uma função, StackSets usa o ARN padrão. Saiba mais sobre a configuração de permissões do conjunto de pilhas.
6. Escolha Create (Criar).

Restrições de modelo do AWS Service Catalog

> **Note**
>
> AWS Service Catalog não suporta restrições de modelo para produtos Terraform Open Source ou Terraform Cloud.

Para limitar as opções disponíveis para os usuários finais quando lançam um produto, você aplica restrições de modelo. Aplique restrições de modelo para garantir que os usuários finais possam usar produtos sem violar os requisitos de conformidade da sua organização. Você aplica restrições de modelo a um produto em um portfólio do AWS Service Catalog. Um portfólio deve conter um ou mais produtos para que você possa definir restrições de modelo.

Uma restrição de modelo consiste em uma ou mais regras que restringem os valores permitidos para parâmetros que são definidos no modelo subjacente do produto do AWS CloudFormation. Os parâmetros em um modelo do AWS CloudFormation definem o conjunto de valores que os usuários podem especificar ao criar uma pilha. Por exemplo, um parâmetro pode definir os vários tipos de instância que os usuários podem escolher ao lançar uma pilha que inclui instâncias do EC2.

Se os valores do conjunto de parâmetros em um modelo forem muito amplos para o público-alvo de seu portfólio, você poderá definir restrições de modelo para limitar os valores que os usuários podem escolher ao lançar um produto. Por exemplo, se os parâmetros do modelo incluírem tipos de instância do EC2 muito grandes para usuários que devem usar apenas tipos de instância pequena (como `t2.micro` ou `t2.small`), você poderá adicionar uma restrição de modelo para limitar os tipos de instância que os usuários finais podem escolher. Para obter mais informações sobre os parâmetros de modelos do AWS CloudFormation, consulte Parâmetros no Guia do usuário do AWS CloudFormation.

As restrições de modelo estão vinculadas em um portfólio. Se você aplicar restrições de modelo a um produto em um portfólio e incluir o produto em outro portfólio, as restrições não se aplicarão ao produto no segundo portfólio.

Se você aplicar uma restrição de modelo a um produto que já foi compartilhado com usuários, a restrição ficará ativa imediatamente para todos os lançamentos de produtos subsequentes e para todas as versões do produto no portfólio.

Você define as regras de restrições de modelo usando um editor de regras ou escrevendo as regras como texto JSON no console do administrador do AWS Service Catalog. Para obter mais informações sobre regras, incluindo sintaxe e exemplos, consulte Regras de restrições de modelo.

Para testar uma restrição antes de liberá-lo aos usuários, crie um portfólio de teste que contenha os mesmos produtos e teste as restrições com esse portfólio.

Para aplicar restrições de modelo a um produto

1. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/.
2. Na página Portfólios, escolha o portfólio que contém o produto ao qual você deseja aplicar uma restrição de modelo.
3. Expanda a seção Restrições e escolha Adicionar restrições.
4. Na janela Selecionar produto e tipo, para Produto escolha o produto para o qual você deseja definir as restrições de modelo. Em seguida, para Tipo de restrição, escolha Modelo. Escolha Continuar.
5. Na página Criador de restrição de modelo, edite as regras de restrição usando o editor JSON ou a interface do criador de regras.

   - Para editar o código JSON da regra, escolha a guia Editor de texto da restrição. Nessa guia, são fornecidos vários exemplos para ajudá-lo a começar.

     Para criar as regras usando a interface de um construtor de regras, escolha a guia Criador de regra. Nessa guia, você pode escolher qualquer parâmetro especificado no modelo para o produto, e pode especificar os valores permitidos para esse parâmetro. Dependendo do tipo de parâmetro, você especificará os valores permitidos escolhendo itens em uma lista de verificação, especificando um número ou especificando um conjunto de valores em uma lista separada por vírgulas.

     Quando acabar de reorganizar as regras, escolha Adicionar regra. A regra aparecerá na tabela na guia Criador de regra. Para revisar e editar a saída do JSON, escolha a guia Editor de texto de restrição.
6. Quando concluir a edição das regras de sua restrição, escolha Enviar. Para ver a restrição, vá para a página de detalhes do portfólio e expanda Restrições.

Regras de restrições de modelo

As regras que definem restrições de modelo em um portfólio do AWS Service Catalog descrevem quando os usuários finais podem usar o modelo e os valores que eles podem especificar como parâmetros que são declarados no modelo do AWS CloudFormation usado para criar o produto que estão tentando usar. As regras são úteis para evitar que os usuários finais especifiquem inadvertidamente um valor incorreto. Por exemplo, você pode adicionar uma regra para verificar se os usuários finais especificaram uma sub-rede válida em uma determinada VPC ou usaram tipos de instância `m1.small` para ambientes de teste. O AWS CloudFormation usa regras para validar valores de parâmetros antes de criar os recursos para o produto.

Cada regra consiste em duas propriedades: uma condição de regra (opcional) e declarações (obrigatório). A condição da regra determina quando uma regra entra em vigor. As declarações descrevem os valores que os usuários podem especificar para um determinado parâmetro. Se você não definir uma condição de regra, as declarações da regra sempre entram em vigor. Para definir uma condição e declarações de regra, você usa funções intrínsecas específicas à regra, que são funções que podem ser usadas apenas na seção `Rules` de um modelo. Você pode aninhar funções, mas o resultado final de uma condição de regra ou declaração deve ser verdadeiro ou falso.

Como exemplo, suponha que você declarou um parâmetro de VPC e de sub-rede na seção `Parameters`. Você pode criar uma regra que valide que uma determinada sub-rede está em uma determinada VPC. Dessa forma, quando um usuário especificar uma VPC, o AWS CloudFormation avaliará a declaração para verificar se o valor do parâmetro de sub-rede está na VPC antes de criar ou atualizar a pilha. Se o valor do parâmetro for inválido, o AWS CloudFormation não criará ou atualizará a pilha. Se os usuários não especificarem uma VPC, o AWS CloudFormation não verificará o valor do parâmetro de sub-rede.

Sintaxe

A seção `Rules` de um modelo consiste no nome da chave `Rules`, seguido por dois-pontos. As chaves incluem todas as declarações da regra. Se você declarar várias regras, elas serão separadas por vírgulas. Para cada regra, você declara um nome lógico entre aspas seguido por uma vírgula e chaves que incluem a condição da regra e as declarações.

Uma regra pode incluir uma propriedade `RuleCondition` e deve incluir uma propriedade `Assertions`. Para cada regra, você pode definir apenas uma condição de regra. Você pode definir uma ou mais declarações, dentro da propriedade `Assertions`. Você define uma condição e declarações de regra usando funções intrínsecas específicas, conforme mostrado no seguinte pseudomodelo:

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

O pseudomodelo mostra uma seção `Rules` que contém duas regras chamadas `Rule01` e `Rule02`. A `Rule01` inclui uma condição de regra e duas declarações. Se a função na condição da regra for verdadeira, as duas funções em cada declaração serão avaliadas e aplicadas. Se a condição da regra for falsa, a regra não entrará em vigor. A `Rule02` sempre entra em vigor porque não é uma condição de regra, o que significa que a declaração é sempre avaliada e aplicada.

Para obter informações sobre funções intrínsecas específicas de regra para definir condições de regra e declarações, consulte Funções de regra daAWS no Guia do usuário AWS CloudFormation.

Exemplo: verificar um valor de parâmetro condicionalmente

As duas regras a seguir verificam o valor do parâmetro `InstanceType`. Dependendo do valor do parâmetro Environment (`test` ou `prod`), o usuário deve especificar `m1.small` ou `m1.large` para o parâmetro `InstanceType`. Os parâmetros `InstanceType` e `Environment` já devem estar declarados na seção `Parameters` do mesmo modelo.

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

Ações de atendimento do AWS Service Catalog

> **Note**
>
> AWS Service Catalog não suporta ações de atendimento para produtos Terraform Open Source ou Terraform Cloud.

O AWS Service Catalog permite que você reduza a manutenção administrativa e o treinamento do usuário final, sem deixar de cumprir as medidas de segurança e de conformidade. Com as ações

de atendimento, o administrador pode permitir que usuários finais realizem tarefas operacionais, resolvam problemas, executem comandos aprovados ou solicitem permissões no AWS Service Catalog. Use documentos do AWS Systems Manager para definir ações de atendimento. Os documentos do AWS Systems Manager concedem acesso a ações predefinidas que implantam as melhores práticas da AWS, como a interrupção e reinicialização do Amazon EC2, e também é possível definir ações personalizadas.

Neste tutorial, você vai permitir que os usuários finais reiniciem uma instância do Amazon EC2. Adicione as permissões necessárias, defina a ação de atendimento, associe-a com um produto e teste a experiência do usuário final ao usar a ação com um produto provisionado.

Pré-requisitos

Este tutorial pressupõe que você tenha permissão total de administrador na AWS, que você já conhece o AWS Service Catalog e que você já tem um conjunto básico de produtos, portfólios e usuários. Se você não conhecer bem o AWS Service Catalog, conclua as tarefas Configuração e Conceitos básicos antes de usar este tutorial.

Tópicos

Etapa 1: Configurar permissões de usuários finais

Os usuários finais devem ter as permissões necessárias para visualizar e executar ações de atendimento específicas. Neste exemplo, o usuário final precisa de permissão para acessar o atributo de ações de serviço do AWS Service Catalog e para reiniciar o Amazon EC2.

Para atualizar as permissões

1. Abra o console do AWS Identity and Access Management (IAM) em https://console.aws.amazon.com/iam/.

2. No menu, localize grupos de usuários.
3. Escolha os grupos que os usuários finais usarão para acessar os recursos do AWS Service Catalog. Neste exemplo, nós selecionamos o grupo de usuário final. Em sua própria implementação, escolha o grupo que é usado pelos usuários finais relevantes.
4. Na guia Permissions (Permissões) da página de detalhes do grupo, crie uma nova política ou edite uma existente. Neste exemplo, adicionamos permissões à política existente selecionando a política personalizada criada para as permissões “Provisionar” e “Encerrar” no AWS Service Catalog.
5. Na página Policy (Política), escolhaEdit Policy (Editar política) para adicionar as permissões necessárias. Você pode usar o editor visual ou o editor JSON para alterar a política. Neste exemplo, usamos o editor JSON para adicionar as permissões. Neste tutorial, adicione as seguintes permissões à política:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "Stmt1536341175150",
   "Action": [
    "servicecatalog:ListServiceActionsForProvisioningArtifact",
    "servicecatalog:ExecuteprovisionedProductServiceAction",
    "ssm:DescribeDocument",
    "ssm:GetAutomationExecution",
    "ssm:StartAutomationExecution",
    "ssm:StopAutomationExecution",
    "cloudformation:ListStackResources",
    "ec2:DescribeInstanceStatus",
    "ec2:StartInstances",
    "ec2:StopInstances"
   ],
   "Effect": "Allow",
   "Resource": "*"
  }
 ]
}
```

6. Depois de editar a política, revise e aprove a alteração. Os usuários no grupo de usuários finais agora têm as permissões necessárias para reiniciar o Amazon EC2 no AWS Service Catalog.

Etapa 2: Criar uma ação de atendimento

Em seguida, crie uma ação de atendimento para reiniciar as instâncias do Amazon EC2.

1. Abra o AWS Service Catalog console em https://console.aws.amazon.com/sc/.
2. No menu, escolha Service actions (Ações de atendimento).
3. Na página Ações de atendimento, escolha Criar ação.
4. Na página Create action (Criar ação), selecione um documento do AWS Systems Manager para definir a ação de atendimento. A ação Reiniciar instância do Amazon EC2 é definida por um documento do AWS Systems Manager. Então, mantemos a opção padrão no menu suspenso, Documentos da Amazon.
5. Pesquise e escolha a ação AWS-Restartec2Instance.
6. Forneça um nome e uma descrição para a ação que faça sentido para o ambiente e a equipe. O usuário final verá esta descrição. Portanto, escolha algo que ajude a entender o que ela faz.
7. Em Configuração de parâmetro e destino, escolha o parâmetro de documento SSM que será o destino da ação (por exemplo, o ID da instância) e escolha o destino do parâmetro. Selecione Add parameter (Adicionar parâmetro) para adicionar outros parâmetros.
8. Em Permissions (Permissões), escolha uma função. Estamos usando permissões padrão para este exemplo. Outras configurações de permissões são possíveis e são definidas nesta página.
9. Após revisar a configuração, escolha Create action (Criar ação).
10. Na próxima página, uma confirmação é exibida quando a ação é criada e está pronta para uso.

Etapa 3: Associar a ação de atendimento a uma versão do produto

Depois de definir uma ação, você deve associar um produto a ela.

1. Na página Ações de serviço, escolha AWS-RestartEC2instance e, em seguida, escolha Associar ação.
2. Na página Associate action (Associar ação), escolha o produto no qual você quer que os usuários finais realizem as ações de atendimento. Neste exemplo, escolhemos o Linux Desktop.
3. Selecione a versão do produto. Você pode usar a caixa de seleção superior para selecionar todas as versões.
4. Escolha Associate action (Associar ação).
5. Uma mensagem de confirmação é exibida na próxima página.

Você acabou de criar a ação de atendimento no AWS Service Catalog. A próxima etapa deste tutorial é usar a ação de atendimento como usuário final.

Etapa 4: Testar a experiência do usuário final

Os usuários finais podem executar ações de atendimento em produtos provisionados. Para os fins deste tutorial, o usuário final deve ter pelo menos um produto provisionado. O produto provisionado deve ser lançado a partir da versão de produto que você associou à ação de atendimento na etapa anterior.

Como acessar a ação de atendimento como usuário final

1. Faça login no console do AWS Service Catalog como usuário final.
2. No painel de navegação do AWS Service Catalog, escolha Provisioned products list (Lista de produtos provisionados). A lista mostra os produtos que são provisionados para a conta do usuário final.
3. Na página Provisioned products list (Lista de produtos provisionados), escolha a instância provisionada.
4. Na página Detalhes do produto provisionado, escolha Ações no canto superior direito e, depois, a ação AWS-RestartEC2instance.
5. Confirme que você quer executar a ação personalizada. Você receberá a confirmação de que a ação foi enviada.

Etapa 5: Gerenciar ações de serviço com AWS CloudFormation

Você pode criar ações de serviço e suas associações com recursos AWS CloudFormation. Para mais informações, consulte o seguinte no Guia do usuário do AWS CloudFormation:

- AWS::ServiceCatalog::CloudFormationProduto ProvisioningArtifactProperties
- AWS::ServiceCatalog::ServiceActionAssociação

> **Note**
>
> Se você gerencia associações de ações de serviço com recursos AWS CloudFormation, não adicione nem remova ações de serviço por meio do AWS Command Line Interface ou AWS

Management Console. Quando você executa uma atualização de pilha, todas as alterações nas ações de serviço feitas fora da AWS CloudFormation são substituídas.

Etapa 6: Solução de problemas

Se a execução da ação de serviço falhar, será possível encontrar a mensagem de erro na seção Outputs (Saídas) do evento de execução da ação de serviço na página Provisioned product (Produto provisionado). Veja a seguir as explicações para as mensagens de erro comuns que podem ser encontradas.

> **Note**
>
> O texto exato da mensagem de erro está sujeito a alterações, portanto, você deve evitar usá-los em qualquer tipo de processo automatizado.

Internal failure (Falha interna)

O AWS Service Catalog teve um erro interno. Tente novamente mais tarde. Se o erro persistir, entre em contato com o suporte ao cliente.

Ocorreu um erro (ThrottlingException) ao chamar a StartAutomationExecution operação

A execução da ação de serviço foi limitada pelo serviço de back-end, como o SSM.

Access denied while assuming the role (Acesso negado ao assumir a função)

O AWS Service Catalog não pôde assumir a função especificada na definição da ação de serviço. Certifique-se de que a entidade principal servicecatalog.amazonaws.com ou uma entidade principal regional, como servicecatalog.us-east-1.amazonaws.com, esteja na lista de permissões na política de confiança do perfil.

Ocorreu um erro (AccessDeniedException) ao chamar a StartAutomationExecution operação: O usuário não está autorizado a executar: ssm: StartAutomationExecution no recurso.

A função especificada na definição da ação de serviço não tem permissões para invocar ssm:. StartAutomationExecution Verifique se o perfil tem as permissões do SSM apropriadas.

Não é possível encontrar nenhum recurso com o tipo ***`TargetType`***no produto provisionado

O produto provisionado não contém recursos que correspondam ao tipo de destino especificado no documento do SSM, como AWS::EC2::Instance. Verifique o produto provisionado para esses recursos ou verifique se o documento está correto.

Document with that name does not exist (Não existe um documento com esse nome)

O documento especificado na definição da ação de serviço não existe.

Failed to describe SSM Automation document (Falha ao descrever o documento de automação do SSM)

O AWS Service Catalog encontrou uma exceção desconhecida do SSM ao tentar descrever o documento especificado.

Failed to retrieve credentials for role (Falha ao recuperar credenciais para a função)

O AWS Service Catalog encontrou um erro desconhecido ao assumir a função especificada.

O parâmetro tem o valor ***InvalidValue***"" não encontrado em ***{ValidValue1}, {ValidValue2}***

O valor do parâmetro passado para o SSM não está na lista de valores permitidos para o documento. Verifique se os parâmetros fornecidos são válidos e tente novamente.

Erro de tipo de parâmetro O valor fornecido para não ***ParameterName***é uma string válida.

O valor do parâmetro passado para o SSM não é válido para o tipo no documento.

Parameter is not defined in service action definition (O parâmetro não está definido na definição da ação do serviço)

Um parâmetro passado para o AWS Service Catalog não está definido na definição da ação de serviço. É possível usar somente parâmetros definidos na definição da ação de serviço.

Falha na etapa ao executar/cancelar a ação. ***A mensagem de erro.*** Consulte o Guia de Solução de Problemas do Serviço de Automação para obter mais detalhes sobre o diagnóstico.

Uma etapa do documento de automação do SSM falhou. Consulte o erro na mensagem para solucionar mais problemas.

Os valores a seguir para o parâmetro não são permitidos porque não estão no produto provisionado: ***InvalidResourceId***

O usuário solicitou ação em um recurso que não está no produto provisionado.

TargetType não definido para o documento de automação SSM

As ações de serviço exigem que os documentos de automação do SSM tenham um TargetType definido. Verifique seu documento de automação do SSM.

Adição de produtos do AWS Marketplace ao seu portfólio

Você pode adicionar produtos do AWS Marketplace aos seus portfólios para disponibilizá-los aos usuários finais do AWS Service Catalog.

O AWS Marketplace é uma loja online em que você pode encontrar, assinar e começar a usar imediatamente uma ampla seleção de software e serviços. Os tipos de produtos no AWS Marketplace incluem bancos de dados, servidores de aplicativos, ferramentas de teste, ferramentas de monitoramento, ferramentas de gerenciamento de conteúdo e software de business intelligence. O AWS Marketplace está disponível em https://aws.amazon.com/marketplace. Observe que você não pode adicionar produtos de software como serviço (SaaS) de AWS Marketplace a AWS Service Catalog.

Você distribui um produto AWS Marketplace aos usuários finais do AWS Service Catalog copiando o produto com o modelo AWS CloudFormation ao AWS Service Catalog e adicionando o produto a um portfólio.

> **Note**
>
> AWS Service Catalog não oferece suporte à distribuição de produtos AWS Marketplace para usuários finais do AWS Service Catalog usando um modelo de produto Terraform Open Source ou Terraform Cloud.

O AWS Marketplace é diretamente compatível com o AWS Service Catalog, ou você também pode se inscrever e adicionar produtos usando a opção manual. Recomendamos adicionar produtos usando a funcionalidade especificamente desenvolvida para o AWS Service Catalog.

Gerenciamento de produtos do AWS Marketplace usando o AWS Service Catalog

Você pode adicionar os produtos inscritos do AWS Marketplace diretamente ao AWS Service Catalog usando uma interface personalizada. Em AWS Marketplace, escolha Service Catalog.

Para obter mais informações, consulte Cópia de produtos para AWS Service Catalog, na Ajuda e perguntas frequentes do AWS Marketplace.

Gerenciamento e adição manuais de produtos do AWS Marketplace

Realize as seguintes etapas para se inscrever em um produto do AWS Marketplace, definir esse produto em um modelo do AWS CloudFormation e adicionar o modelo a um portfólio do AWS Service Catalog.

Para se inscrever em um produto do AWS Marketplace

1. Acesso o AWS Marketplace em https://aws.amazon.com/marketplace.
2. Procure produtos ou pesquise o produto que você deseja adicionar ao seu portfólio do AWS Service Catalog. Escolha o produto para visualizar a página de detalhes do produto.
3. Escolha Continuar para visualizar a página de distribuição e, em seguida, a guia Lançamento manual.

   As informações na página de distribuição incluem os tipos de instâncias compatíveis do Amazon Elastic Compute Cloud (Amazon EC2), as Regiões da AWS compatíveis, e a ID da imagem de máquina da Amazon (AMI) que o produto usa para cada região da AWS. Observe que algumas opções afetam o custo. Você usará essas informações para personalizar o modelo do AWS CloudFormation nas etapas posteriores.
4. Escolha Accept Terms para se inscrever no produto.

   Depois de se inscrever em um produto, poderá acessar a qualquer momento as informações sobre o produto na respectiva página de distribuição no AWS Marketplace escolhendo Your Software (Seu software) e, em seguida, o produto.

Para definir seu produto do AWS Marketplace em um modelo do AWS CloudFormation

Para concluir as etapas a seguir, você poderá usar um dos modelos de exemplo do AWS CloudFormation como ponto de partida. Depois, você personalizará o modelo para que ele represente seu produto do AWS Marketplace. Para acessar os modelos de exemplo, consulte Modelos de exemplo no Guia do usuário do AWS CloudFormation.

1. Na página de modelos de exemplo, no Guia do usuário AWS CloudFormation, escolha a região da AWS para seu produto. Seu produto AWS Marketplace deve ser compatível com a região da

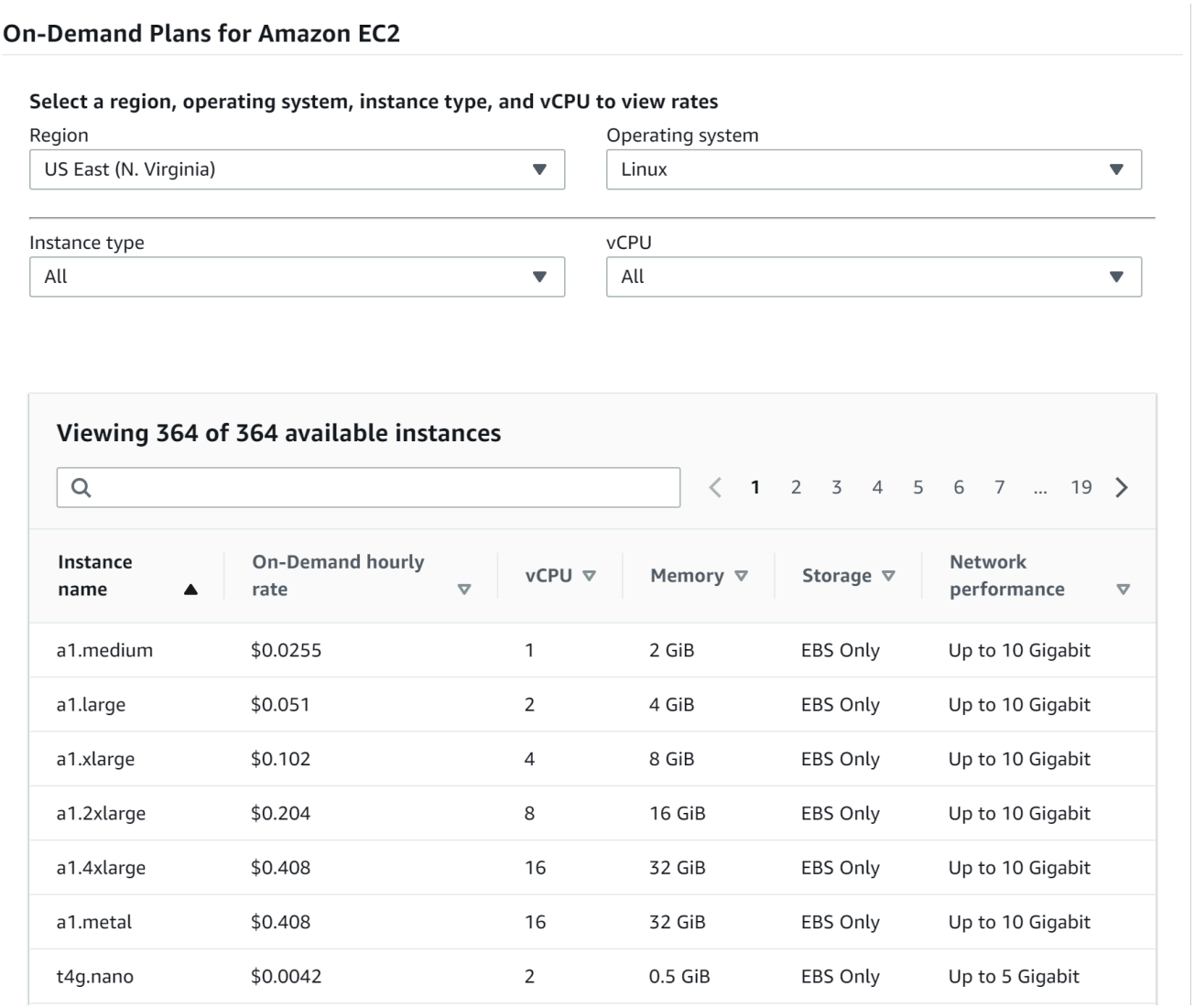
AWS. Você pode visualizar as regiões compatíveis na página de distribuição do produto no AWS Marketplace.

2. Para ver uma lista dos modelos de exemplo de serviço que são apropriados para a região, escolha o link Serviços.
3. Você pode usar como ponto de partida qualquer um dos exemplos que são apropriados para as suas necessidades. As etapas neste procedimento usam o modelo da instância do Amazon EC2 em um grupo de segurança. Para visualizar o modelo de exemplo, escolha View e, em seguida, salve uma cópia do modelo localmente para que você possa editá-lo. Seu arquivo local deve ter a extensão `.template`.
4. Abra o arquivo de modelo em um editor de texto.
5. Personalize a descrição na parte superior do modelo. A descrição ficará parecida com o seguinte:

   ```
   "Description": "Launches a LAMP stack from AWS Marketplace",
   ```

6. Personalize o parâmetro `InstanceType` para que ele inclua apenas os tipos de instância do EC2 compatíveis com o seu produto. Se o seu modelo incluir tipos de instâncias do EC2 incompatíveis, o produto não será lançado para os usuários finais.

   a. Na página de distribuição de produto do AWS Marketplace, visualize os tipos de instâncias do EC2 compatíveis na seção Detalhes de preço.



b. No seu modelo, altere o tipo de instância padrão para um tipo de instância do EC2 compatível de sua escolha.

c. Edite a lista `AllowedValues` para que ela inclua apenas os tipos de instâncias do EC2 compatíveis com o seu produto.

d. Remova os tipos de instância do EC2 que você não deseja que seus usuários finais usem ao lançar o produto pela lista `AllowedValues`.

Ao finalizar a edição do parâmetro `InstanceType`, ele pode ser semelhante ao exemplo a seguir:

```
"InstanceType" : {
  "Description" : "EC2 instance type",
  "Type" : "String",
```

```
      "Default" : "m1.small",
      "AllowedValues" : [ "t1.micro", "m1.small", "m1.medium", "m1.large",
 "m1.xlarge", "m2.xlarge", "m2.2xlarge", "m2.4xlarge", "c1.medium", "c1.xlarge",
 "c3.large", "c3.large", "c3.xlarge", "c3.xlarge", "c3.4xlarge", "c3.8xlarge" ],
      "ConstraintDescription" : "Must be a valid EC2 instance type."
    },
```

7. Na seção `Mappings` do seu modelo, edite os mapeamentos `AWSInstanceType2Arch` de modo que apenas os tipos de instâncias do EC2 e arquiteturas compatíveis sejam incluídos.

   a. Para editar a lista de mapeamentos, remova todos os tipos de instâncias do EC2 que não estão incluídos na lista `AllowedValues` referente ao parâmetro `InstanceType`.

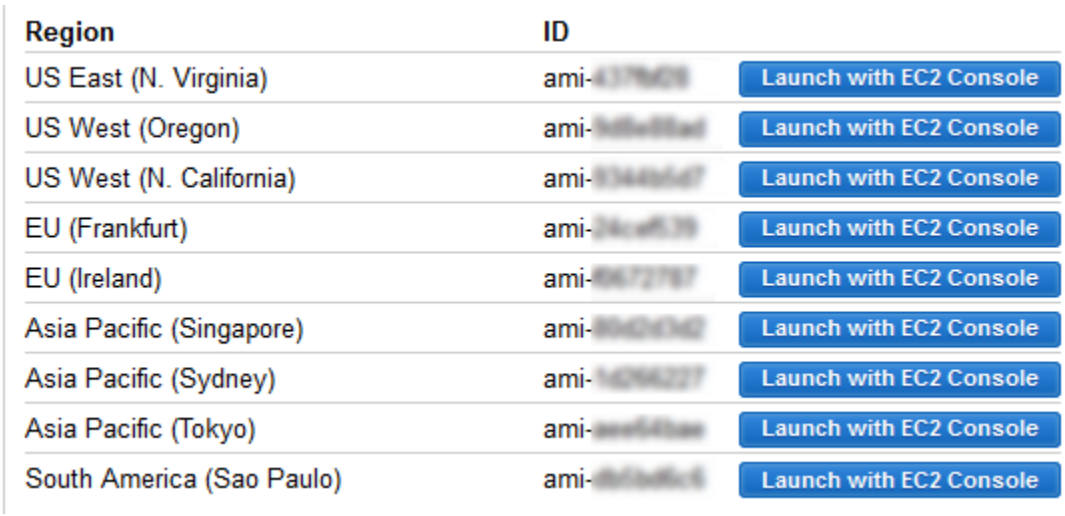
   b. Edite o valor `Arch` de cada tipo de instância do EC2 para que seja o tipo de arquitetura compatível com o seu produto. Os valores válidos são `PV64`, `HVM64` e `HVMG2`. Para saber qual arquitetura é compatível com seu produto, consulte a página de detalhes do produto no AWS Marketplace. Para saber quais arquiteturas são compatíveis com as famílias de instâncias do EC2, consulte Matriz de tipo de instância do Amazon Linux AMI.

   Depois que você terminar de editar os mapeamentos `AWSInstanceType2Arch`, a aparência poderá ser semelhante ao exemplo a seguir:

```
    "AWSInstanceType2Arch" : {
      "t1.micro"    : { "Arch" : "PV64"  },
      "m1.small"    : { "Arch" : "PV64"  },
      "m1.medium"   : { "Arch" : "PV64"  },
      "m1.large"    : { "Arch" : "PV64"  },
      "m1.xlarge"   : { "Arch" : "PV64"  },
      "m2.xlarge"   : { "Arch" : "PV64"  },
      "m2.2xlarge"  : { "Arch" : "PV64"  },
      "m2.4xlarge"  : { "Arch" : "PV64"  },
      "c1.medium"   : { "Arch" : "PV64"  },
      "c1.xlarge"   : { "Arch" : "PV64"  },
      "c3.large"    : { "Arch" : "PV64"  },
      "c3.xlarge"   : { "Arch" : "PV64"  },
      "c3.2xlarge"  : { "Arch" : "PV64"  },
      "c3.4xlarge"  : { "Arch" : "PV64"  },
      "c3.8xlarge"  : { "Arch" : "PV64"  }
    }
,
```

8. Na seção `Mappings` do seu modelo, edite os mapeamentos `AWSRegionArch2AMI` para associar cada região da AWS à arquitetura correspondente e à ID da AMI do seu produto.

   a. Na página de distribuição do produto no AWS Marketplace, visualize o ID da AMI que seu produto usa para cada região da AWS, como no exemplo a seguir:



Region	ID	
US East (N. Virginia)	ami-	Launch with EC2 Console
US West (Oregon)	ami-	Launch with EC2 Console
US West (N. California)	ami-	Launch with EC2 Console
EU (Frankfurt)	ami-	Launch with EC2 Console
EU (Ireland)	ami-	Launch with EC2 Console
Asia Pacific (Singapore)	ami-	Launch with EC2 Console
Asia Pacific (Sydney)	ami-	Launch with EC2 Console
Asia Pacific (Tokyo)	ami-	Launch with EC2 Console
South America (Sao Paulo)	ami-	Launch with EC2 Console

   b. No seu modelo, remova os mapeamentos de todas as regiões da AWS às quais você não oferece suporte.

   c. Edite o mapeamento de cada região para remover as arquiteturas incompatíveis (`PV64`, `HVM64` ou `HVMG2`) e seus respectivos IDs de AMI.

   d. Para cada mapeamento restante de região da AWS e arquitetura, especifique a ID de AMI correspondente pela página de detalhes do produto no AWS Marketplace.

   Depois que você terminar de editar os mapeamentos `AWSRegionArch2AMI`, seu código poderá ser semelhante ao exemplo a seguir:

```
"AWSRegionArch2AMI" : {
  "us-east-1"        : {"PV64" : "ami-nnnnnnnn"},
  "us-west-2"        : {"PV64" : "ami-nnnnnnnn"},
  "us-west-1"        : {"PV64" : "ami-nnnnnnnn"},
  "eu-west-1"        : {"PV64" : "ami-nnnnnnnn"},
  "eu-central-1"     : {"PV64" : "ami-nnnnnnnn"},
  "ap-northeast-1"   : {"PV64" : "ami-nnnnnnnn"},
  "ap-southeast-1"   : {"PV64" : "ami-nnnnnnnn"},
  "ap-southeast-2"   : {"PV64" : "ami-nnnnnnnn"},
  "sa-east-1"        : {"PV64" : "ami-nnnnnnnn"}
```

```
    }
```

Agora, você pode usar o modelo para adicionar o produto a um portfólio do AWS Service Catalog. Se você quiser fazer alterações adicionais, consulte Como trabalhar com modelos do AWS CloudFormation para saber mais sobre modelos.

Para adicionar seu produto do AWS Marketplace a um portfólio do AWS Service Catalog

1. Faça login no AWS Management Console e navegue até o console AWS Service Catalog do administrador em https://console.aws.amazon.com/servicecatalog/.
2. Na página Portfólios, escolha o portfólio ao qual você deseja adicionar seu produto do AWS Marketplace.
3. Na página de detalhes do portfólio, escolha Fazer upload de produto novo.
4. Digite os detalhes do produto e suporte solicitados.
5. Na página Version details, escolha Upload a template file (Atualizar um arquivo de modelo), escolha Browse (Buscar), depois selecione seu arquivo de modelo.
6. Digite um título e a descrição da versão.
7. Escolha Próximo.
8. Na página Revisar, verifique se o resumo está correto e, em seguida, escolha Confirmar e fazer upload. O produto é adicionado ao seu portfólio. Ele agora está disponível para usuários finais que têm acesso ao portfólio.

Usando AWS CloudFormation StackSets

> **Note**
>
> AutoTags atualmente não são compatíveis com AWS CloudFormation StackSets.

Você pode usar AWS CloudFormation StackSets para lançar AWS Service Catalog produtos em várias Regiões da AWS contas. Você pode especificar a ordem na qual os produtos são implantados sequencialmente em Regiões da AWS. Entre contas, os produtos são implantados em paralelo. Ao lançar, os usuários podem especificar a tolerância a falhas e o número máximo de contas para a implantação em paralelo. Para obter mais informações, consulte Trabalhar com AWS CloudFormation StackSets.

Conjunto de pilhas vs. instâncias da pilha

Com um conjunto de pilhas é possível criar pilhas nas contas da AWS em várias regiões da AWS usando um único modelo do AWS CloudFormation.

Uma instância de pilha se refere a uma pilha em uma conta de destino dentro de uma região da AWS e está associada a apenas um conjunto de pilhas.

Para obter mais informações, consulte Conceitos do StackSets.

Restrições do conjunto de pilhas

No AWS Service Catalog, você pode usar restrições do conjunto de pilhas para configurar opções de implantação de produtos.

AWS Service Catalogsuporta restrições de conjunto de pilhas em dois produtosAWS GovCloud (US) Regions: AWS GovCloud (Oeste dos EUA) e AWS GovCloud (Leste dos EUA).

Para mais informações, consulte Restrições do conjunto de pilhas do AWS Service Catalog.

Gerenciar orçamentos

É possível usar o Orçamentos da AWS para acompanhar seu uso e custos de serviço no AWS Service Catalog. É possível associar orçamentos a produtos e portfólios do AWS Service Catalog.

> **Note**
>
> AWS Service Catalog não oferece suporte a orçamentos para produtos Terraform Open Source.

O Orçamentos da AWS permite que você defina orçamentos personalizados que enviam alertas quando o uso ou os custos excedem (ou tendem a exceder) o valor orçado. Informações sobre o Orçamentos da AWS estão disponíveis em https://aws.amazon.com/aws-cost-management/aws-budgets.

Tarefas

- Pré-requisitos
- Como criar um orçamento

- Associar um orçamento
- Visualizar um orçamento
- Desassociar um orçamento

Pré-requisitos

Antes de usar o Orçamentos da AWS, é necessário ativar tags de alocação de custos no console do AWS Billing and Cost Management. Para obter mais informações, consulte Ativar tags de alocação de custos definidos pelo usuário no guia de usuário do AWS Billing and Cost Management.

> **Note**
>
> As tags levam até 24 horas para serem ativadas.

Também é necessário habilitar o acesso do usuário ao console do AWS Billing and Cost Management para todos os usuários ou grupos que usarão o recurso Orçamentos. É possível fazer isso criando uma nova política para seus usuários.

Para permitir que os usuários do criem orçamentos, também é necessário permitir que os usuários visualizem informações de faturamento. Se quiser usar notificações do Amazon SNS, será possível fornecer aos usuários a capacidade de criar notificações do Amazon SNS notifications, conforme mostrado no exemplo de política abaixo.

Como criar a política de orçamentos

1. Abra o console IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação, escolha Policies.
3. No painel de conteúdo, escolha Criar política.
4. Escolha a guia JSON e copie o texto do documento de política JSON a seguir. Cole este texto na caixa de texto do JSON.

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

```
            "Sid": "Stmt1435216493000",
            "Effect": "Allow",
            "Action": [
                "aws-portal:ViewBilling",
                "aws-portal:ModifyBilling",
                "budgets:ViewBudget",
                "budgets:ModifyBudget"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "Stmt1435216552000",
            "Effect": "Allow",
            "Action": [
                "sns:*"
            ],
            "Resource": [
                "arn:aws:sns:us-east-1"
            ]
        }
    ]
}
```

5. Ao concluir, selecione Revisar política. O Validador de política indica se há qualquer erro de sintaxe.
6. Na página Review (Revisar), atribua um nome à sua política. Analise o Resumo da política para ver as permissões concedidas pela sua política e, em seguida, escolha Criar política para salvar seu trabalho.

   A nova política é exibida na lista de políticas gerenciadas e está pronta para ser anexada a seus usuários e grupos. Para obter mais informações, consulte Criar e anexar uma política gerenciada pelo cliente no Guia do usuário do AWS Identity and Access Management.

Como criar um orçamento

No console do administrador do AWS Service Catalog, as páginas Produtos e Portfólios listam informações sobre produtos e portfólios existentes e permitem que você realize ações neles. Para criar um orçamento, primeiro decida a qual produto ou portfólio você deseja associar o orçamento.

Para criar um orçamento

1. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/.
2. Escolha Lista de produtos ou Portfólios.
3. Selecione o produto ou portfólio ao qual você deseja adicionar um orçamento.
4. Abra o menu Ações e escolha Criar orçamento.
5. Na página Budget creation (Criação de orçamento), associe um tipo de tag ao seu orçamento.

   Existem dois tipos de tags: AutoTags TagOptions e. AutoTags identificar o portfólio, o produto e o usuário que lançou um produto. AWS Service Catalogaplica essas tags automaticamente aos recursos provisionados. A TagOption é um par de valores-chave definido pelo administrador que é gerenciado em. AWS Service Catalog

   Para que os gastos que ocorrem em um portfólio ou produto reflitam no orçamento associado, eles devem ter a mesma tag. Observe que uma chave de tag que está sendo usada pela primeira vez pode levar 24 horas para ser ativada. Para ter mais informações, consulte the section called “Pré-requisitos”.
6. Escolha Criado em AWS Budgets. Você será direcionado para a página Defina seu orçamento. Continue a configuração do orçamento seguindo as etapas em Criar um orçamento.

> **Note**
>
> Depois de criar um orçamento, você deve associá-lo ao produto ou portfólio.

Associar um orçamento

Cada portfólio ou produto pode ter um orçamento associado a ele. Cada orçamento pode ser associado a vários portfólios e produtos.

Ao associar um orçamento a um produto ou portfólio, será possível exibir informações sobre o orçamento na página de detalhes desse produto ou portfólio. Para que os gastos que ocorrem no produto ou portfólio sejam refletidos no orçamento, é necessário associar as mesmas tags no orçamento e no produto ou portfólio.

> **Note**
>
> Se você excluir um orçamento de AWS Budgets, as associações existentes com produtos e portfólios do AWS Service Catalog ainda existirão, mas o AWS Service Catalog não poderá exibir nenhuma informação sobre o orçamento excluído.

Como associar um orçamento

1. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/.
2. Escolha Lista de produtos ou Portfólios.
3. Selecione o produto ou portfólio ao qual você deseja associar um orçamento.
4. Abra o menu Ações, e, em seguida, escolha Associar orçamento.
5. Na página Associação de orçamento, selecione um orçamento existente e, em seguida, Continuar.
6. A tabela produtos ou portfólios agora incluirá dados para o orçamento que você acabou de adicionar.

Visualizar um orçamento

Se um orçamento estiver associado a um produto, será possível visualizar informações sobre o orçamento na página Detalhes do produto e Lista de produtos. Se um orçamento estiver associado a um portfólio, será possível visualizar informações sobre o orçamento nas páginas Portfólios e Detalhes do portfólio.

As páginas Portfólios e Lista de produtos exibem informações de orçamento para recursos existentes. É possível ver colunas exibindo Current vs. budget (Atual versus orçamento) e Forecast vs. budget (Previsão versus orçamento).

Ao escolher um produto ou portfólio, você é direcionado para uma página de detalhes. Essas páginas Detalhes do portfólio e Detalhes do produto têm uma seção com informações detalhadas sobre o orçamento associado. É possível ver o valor orçado, o gasto atual e o gasto previsto. Você também tem a opção de visualizar detalhes do orçamento e editar o orçamento.

Desassociar um orçamento

É possível desassociar um orçamento de um portfólio ou produto.

> **Note**
>
> Se você excluir um orçamento de orçamentos AWS, as associações existentes com produtos e portfólios do AWS Service Catalog ainda existirão, mas o AWS Service Catalog não poderá exibir nenhuma informação sobre o orçamento excluído.

Como desassociar um orçamento

1. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/.
2. Escolha Lista de produtos ou Portfólios.
3. Selecione o produto ou portfólio do qual você deseja desassociar um orçamento.
4. Escolha Ações. No menu suspenso, escolha Desassociar orçamento. Um alerta de confirmação é exibido.
5. Depois de confirmar que deseja desassociar o orçamento do produto ou portfólio, escolha Confirmar.

Gerenciar produtos provisionados

O AWS Service Catalog fornece uma interface para gerenciamento de produtos provisionados. Você pode visualizar, atualizar e encerrar todos os produtos provisionados de seu catálogo com base no nível de acesso. Consulte as seções a seguir para obter procedimentos de exemplo.

Tópicos

Gerenciar todos os produtos provisionados como administrador

Para gerenciar todos os produtos provisionados da conta, você precisa do `AWSServiceCatalogAdminFullAccess` ou uma permissão de IAM equivalente para acessar operações de gravação do produto provisionado. Para ter mais informações, consulte Gerenciamento de identidades e acesso no AWS Service Catalog.

> **Tip**
>
> Para o encadeamento estático de produtos provisionados, você deve referenciar as saídas de produtos provisionados em um modelo de produto-artefato antes que o produto provisionado seja provisionado. Para obter mais informações, incluindo um exemplo, consulte o seguinte:
>
> - AWS::ServiceCatalog::CloudFormationProvisionedProduct no AWS CloudFormation Guia do usuário.
> - DescribeProvisioningParameters (ProvisioningArtifactOutputKeys) no Guia do AWS Service Catalog desenvolvedor.

Para visualizar e gerenciar todos os produtos provisionados

1. Abra o AWS Service Catalog console em https://console.aws.amazon.com/servicecatalog/.

   Se você já estiver conectado ao console do AWS Service Catalog, escolha Catálogo de Serviço e, em seguida, Usuário final.
2. Se necessário, role para baixo até a seção Produtos provisionados.
3. Na seção Produtos provisionados, escolha a lista Exibir: e selecione o nível de acesso que você deseja ver: Usuário, Perfil ou Conta. Essa ação exibe todos os produtos provisionados no catálogo.
4. Escolha um produto provisionado para visualizar, atualizar ou encerrar. Para obter mais detalhes sobre as informações fornecidas nessa visualização, consulte Visualizar informações sobre produtos provisionados.

Alterar o proprietário do produto provisionado

Você pode alterar o proprietário de um produto provisionado a qualquer momento. É necessário saber o ARN do usuário ou da função que deseja definir como o novo proprietário.

Por padrão, esse recurso está disponível para administradores que usam a política gerenciada `AWSServiceCatalogAdminFullAccess`. Você pode habilitá-lo para usuários finais concedendo a eles a permissão `servicecatalog:UpdateProvisionedProductProperties` no AWS Identity and Access Management (IAM).

Como alterar o proprietário de um produto provisionado

1. No console do AWS Service Catalog, escolha Provisioned products list (Lista de produtos provisionados).
2. Localize o produto provisionado que deseja atualizar, escolha os três pontos ao lado dele e selecione Alterar proprietário do produto provisionado).Você também pode encontrar a opção Change owner (Alterar proprietário) na página de detalhes do produto provisionado, no menu Actions (Ações).
3. Na caixa de diálogo, insira o ARN do usuário ou da função que deseja definir como o novo proprietário. Um ARN começa com `arn:` e inclui outras informações separadas por dois pontos ou barras, por exemplo, `arn:aws:iam::123456789012:user/NewOwner`.
4. Selecione Enviar. Será exibida uma mensagem de êxito quando o proprietário for atualizado.

Consulte também

- UpdateProvisionedProductProperties

Atualizar modelos para produtos provisionados

Você pode alterar o modelo atual de um produto provisionado para um modelo diferente. Por exemplo, se você tiver um produto EC2 no Service Catalog, poderá atualizar esse produto EC2 para manter a mesma ID do produto provisionado, mas alterar o modelo para um bucket do S3.

> **Note**
>
> A atualização de modelos não é suportada para produtos provisionados do Terraform Open Source ou do Terraform Cloud. Se quiser usar um modelo diferente para um produto Terraform existente, você deve excluir o produto e, em seguida, criar um novo produto usando o modelo desejado.

Para atualizar modelos para produtos provisionados

1. No menu de navegação à esquerda, escolha Produtos provisionados.
2. Em Produtos provisionados, escolha um produto provisionado e selecione Ações, Atualizar.

   Observe que você também pode selecionar Ações, Atualizar na página de Detalhes do produto provisionado.
3. (Opcional) Em Detalhes do produto, escolha Alterar produto.

   Em Alterar produto, observe este aviso:

   A alteração do produto atualizará esse produto provisionado para um modelo de produto diferente. Isso pode encerrar recursos e criar novos recursos.

   Você pode atualizar um produto provisionado para uma versão diferente dentro do mesmo produto.
4. (Opcional) Em Produtos, escolha o produto que você deseja atualizar com um modelo diferente. Em seguida, escolha Alterar.

   Em Detalhes do produto, observe este aviso:

[Nome do produto] será atualizado de [nome do modelo atual] para [nome do novo modelo]. No entanto, o nome do seu produto provisionado, [Nome do produto provisionado], não mudará.

Você pode atualizar um produto provisionado para uma versão diferente dentro do mesmo produto.

5. Em Versões do produto, escolha a versão do produto que você deseja.
6. Em Parâmetros, escolha os parâmetros apropriados.
7. Escolha Atualizar.

   Em Detalhes do produto provisionado, você pode ver os detalhes da atualização. O nome do produto provisionado não muda, mas o produto provisionado agora tem um modelo diferente.

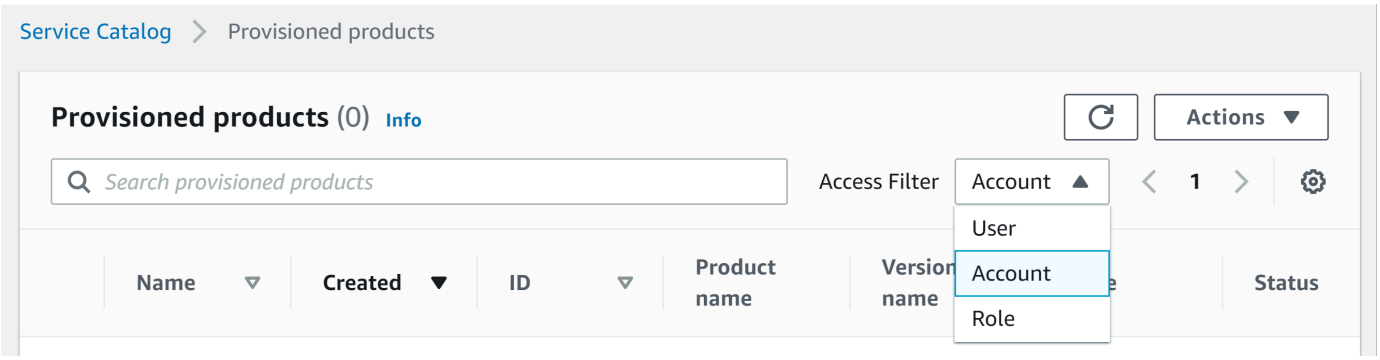
Tutorial: Identificar alocação de recursos do usuário

Você pode identificar o usuário que provisionou um produto e os recursos associados ao produto usando o console do AWS Service Catalog. Este tutorial ajuda a converter este exemplo para seus próprios produtos provisionados específicos.

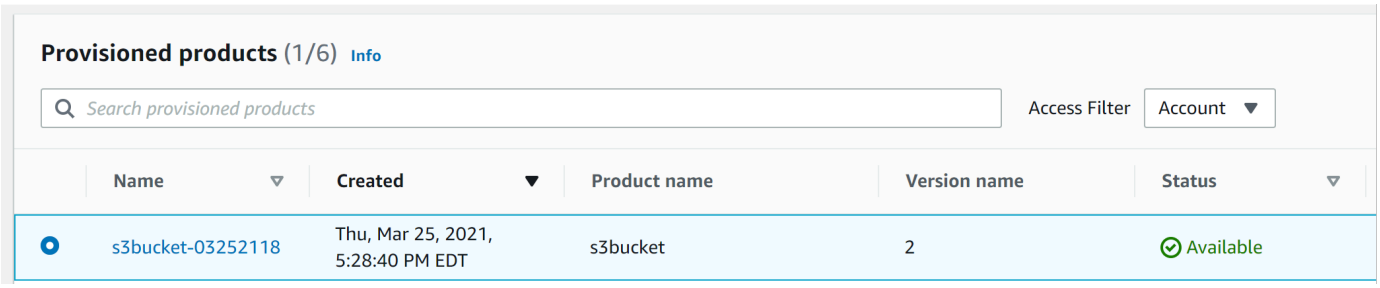
Para gerenciar todos os produtos provisionados da conta, você precisa do `AWSServiceCatalogAdminFullAccess` ou de acesso equivalente para as operações de gravação do produto provisionado. Para obter mais informações, consulte Gerenciamento de identidade e acesso no Guia do Administrador do AWS Service Catalog.

Para identificar o usuário que provisionou um produto e os recursos associados

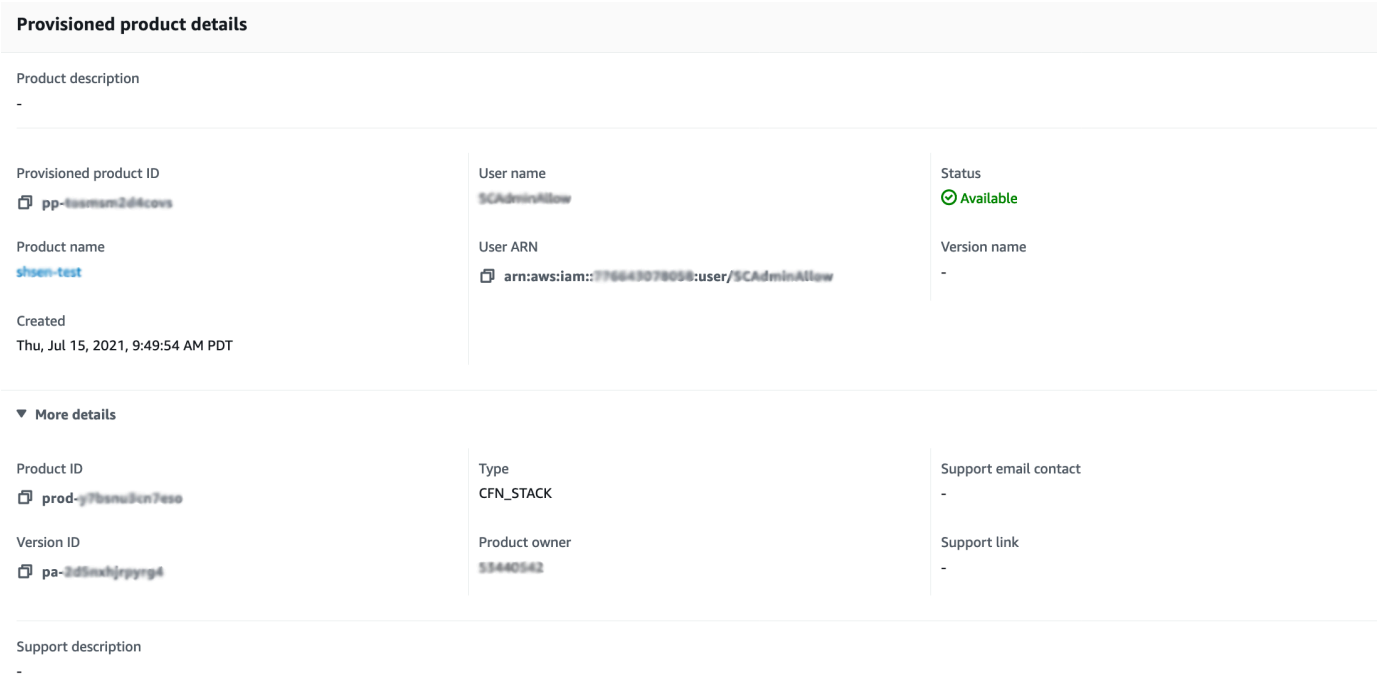
1. Abra https://console.aws.amazon.com/servicecatalog.
2. No menu de navegação à esquerda, escolha Produtos provisionados.
3. No menu suspenso Filtro de acesso, escolha Conta.



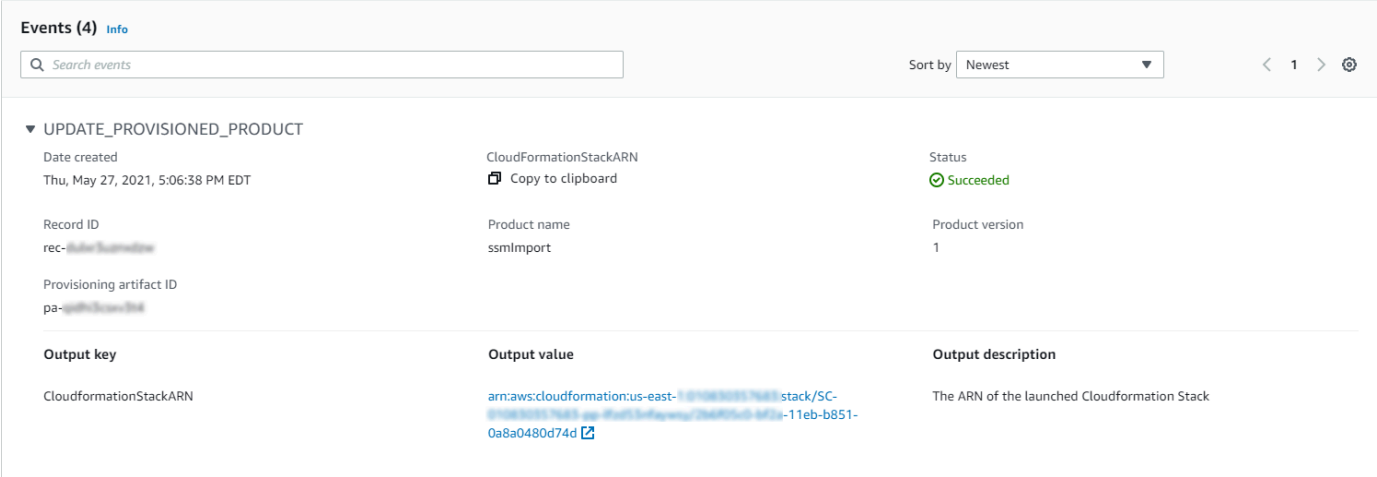
4. Na visualização Conta, escolha e abra um produto provisionado para exibir seus detalhes.



Você pode ver os detalhes do produto provisionado.



5. Role para baixo até a seção Eventos. Observe os valores para `Provisioned product ID` e `CloudformationStackARN`.



6. Use a ID do produto provisionado para identificar o registro do AWS CloudTrail que corresponde a este lançamento e identifique o usuário solicitante (normalmente, ele é inserido como um endereço de e-mail durante a federação). Neste exemplo, é "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. Use o valor de `CloudformationStack`ARN para identificar eventos do AWS CloudFormation para localizar informações sobre os recursos criados. Você também pode usar a API do AWS CloudFormation para obter essas informações. Para obter mais informações, consulte Referência de API do AWS CloudFormation.

Observe que você pode executar as etapas de 1 a 4 usando a API do AWS Service Catalog ou o AWS CLI. Para obter mais informações, consulte o Guia do Desenvolvedor do AWS Service Catalog e AWS Service Catalog Referência de Linha de Comando.

Gerenciar erros de status do produto Terraform Open Source

As falhas de `ProvisionProduct` do Terraform Open Source são roteadas para o estado `TAINTED`, permitindo que cada produto provisionado continue para `UpdateProvisionedProduct`. Quando isso ocorre:

- `UpdateProvisionedProduct` não faz uma tentativa de atualizar ou corrigir tags, nem de criar ou modificar um grupo de recursos.
- `UpdateProvisionedProduct` não considera falhas de operações de provisionamento anteriores ao decidir se o produto provisionado deve ser definido como `AVAILABLE` ou `TAINTED`.

AWS Service Catalog só aplica tags durante `ProvisionProduct`. Qualquer falha na marcação resultante de uma falha na operação do `ProvisionProduct` não é resolvida automaticamente.

Exemplos de erros de status

Exemplo 1: AWS Service Catalog não cria um grupo de recursos durante `ProvisionProduct`

No cenário abaixo, você tem um produto provisionado no estado `AVAILABLE`, mesmo que não haja um grupo de recursos de suporte e sem nenhuma tag aplicada aos recursos.

1. Sua ação inicia `ProvisionProduct`.
2. O mecanismo de provisionamento do Terraform responde ao `ProvisionProduct` com uma falha no fluxo de trabalho e não fornece um `ResourceIdentifier`.
3. O fluxo de trabalho `ProvisionProduct` não cria um grupo de recursos e, em seguida, define o estado do produto provisionado como `ERROR`.
4. Em seguida, você inicia a operação `Updateprovisionedproduct`.
5. O mecanismo de provisionamento do Terraform responde indicando “sucesso”.
6. Como resultado, o fluxo de trabalho do `UpdateprovisionedProduct` define o estado do produto provisionado como `AVAILABLE`, mas não cria um grupo de recursos nem tenta aplicar tags.

Exemplo 2: AWS Service Catalog cria novos recursos durante `UpdateProvisionedProduct`

No cenário abaixo, você tem um produto provisionado no estado `AVAILABLE`, mesmo que os novos recursos não tenham nenhuma tag aplicada.

1. Sua ação inicia `ProvisionProduct`.
2. O mecanismo de provisionamento do Terraform responde indicando “sucesso” e fornece uma `ResourceIdentifier`.
3. O fluxo de trabalho do `ProvisionProduct` cria um grupo de recursos e aplica tags a todos os recursos identificados.
4. Você inicia `UpdateProvisionedProduct` em um novo artefato que cria novos recursos.
5. O mecanismo de provisionamento do Terraform responde indicando “sucesso”.
6. O fluxo de trabalho do `UpdateProvisionedProduct` define o estado do produto provisionado como `AVAILABLE`, mas não tenta aplicar nenhuma tag adicional aos novos recursos.

Solução de erro de status

AWS Service Catalog garante que um grupo de recursos seja criado para todos os produtos provisionados definidos como `TAINTED` do `ProvisionProduct`. Se o mecanismo de provisionamento do Terraform não retornar um `ResourceIdentifier`, ou se não AWS Service Catalog conseguir criar um grupo de recursos, o produto provisionado será definido no estado `ERROR`, forçando você a encerrar.

Gerenciar o arquivo do estado do produto Terraform Open Source

Cada produto provisionado do Terraform Open Source tem um arquivo de estado único. Há uma relação equivalente entre o produto provisionado e seu arquivo de estado. Os arquivos são armazenados em um bucket do Amazon S3 chamado `sc-terraform-engine-state-${AWS::AccountId}-${AWS::Region}`. O arquivo de estado é salvo sob `AccountID` ou a chave de objeto do `ProvisionedProductID`.

O acesso aos arquivos de estado é limitado ao `GetStateFile` AWS Lambda e modelos de lançamento do Amazon EC2. Os administradores doAWS Service Catalog não têm acesso direto aos arquivos de estado no Amazon S3. Os administradores devem acessar os arquivos usando o Amazon EC2. Por padrão, os administradores do AWS Service Catalog podem ver a lista de arquivos de estado, mas não podem ler ou escrever no conteúdo dos arquivos. Somente o mecanismo de provisionamento do Terraform pode ler ou escrever no conteúdo do arquivo.

Gerenciar tags no AWS Service Catalog

O AWS Service Catalog fornece tags para que você possa categorizar seus recursos. Existem dois tipos de tags: AutoTags TagOptions e.

AutoTags são tags que identificam informações sobre a origem de um recurso provisionado AWS Service Catalog e são automaticamente aplicadas por AWS Service Catalog aos recursos provisionados.

TagOptions são pares de valores-chave gerenciados AWS Service Catalog que servem como modelos para a criação AWS de tags.

Tópicos

AWS Service Catalog AutoTags

> **Note**
>
> AWS Service Catalognão oferece suporte AutoTags para produtos Terraform Open Source.

AutoTags são tags que identificam informações sobre a origem de um recurso provisionado AWS Service Catalog e são automaticamente aplicadas por AWS Service Catalog aos recursos provisionados.

AutoTags inclua etiquetas para os identificadores exclusivos de portfólio, produto, usuário, versão do produto e produto provisionado. Isso fornece um conjunto de tags que refletem a estrutura do AWS Service Catalog configurada pelos clientes no catálogo. AutoTags não contam para o limite de 50 tags do cliente.

> **Note**
>
> AWS Service Catalognão oferece suporte AutoTags para produtos Terraform Open Source.

AWS Service Catalog AutoTags pode ajudar a fornecer uma marcação consistente para seus recursos, o que é útil ao definir orçamentos para um portfólio, produto ou usuário. Você também pode usar o AutoTags para identificar recursos para operações pós-lançamento, como definir AWS Config regras. AutoTags seus recursos provisionados podem ser visualizados na seção Tags dos serviços downstream usados para provisionamento, como Amazon AWS CloudFormation EC2 e Amazon S3.

> **Note**
>
> AWS Service Catalognão é atualizado AutoTags depois que você se inscreve AutoTags nos recursos provisionados. Se você atualizar o produto provisionado para um produto diferente, artefato provisionado ou novo caminho de lançamento, o existente AutoTags ainda mostrará os valores originais.

AutoTag detalhes

- aws:servicecatalog:portfolioArn — o ARN do portfólio do qual o produto provisionado foi lançado.
- aws:servicecatalog:productArn — o ARN do produto do qual o produto provisionado foi lançado.
- aws:servicecatalog: - provisioningPrincipalArn O ARN do principal de provisionamento (usuário) que criou o produto provisionado.
- aws:servicecatalog: - O ARN do produto provisionedProductArn provisionado.
- aws:servicecatalog: provisioningArtifactIdentifier - O ID do artefato de provisionamento original (versão do produto).

AWS Service Catalog TagOption Biblioteca

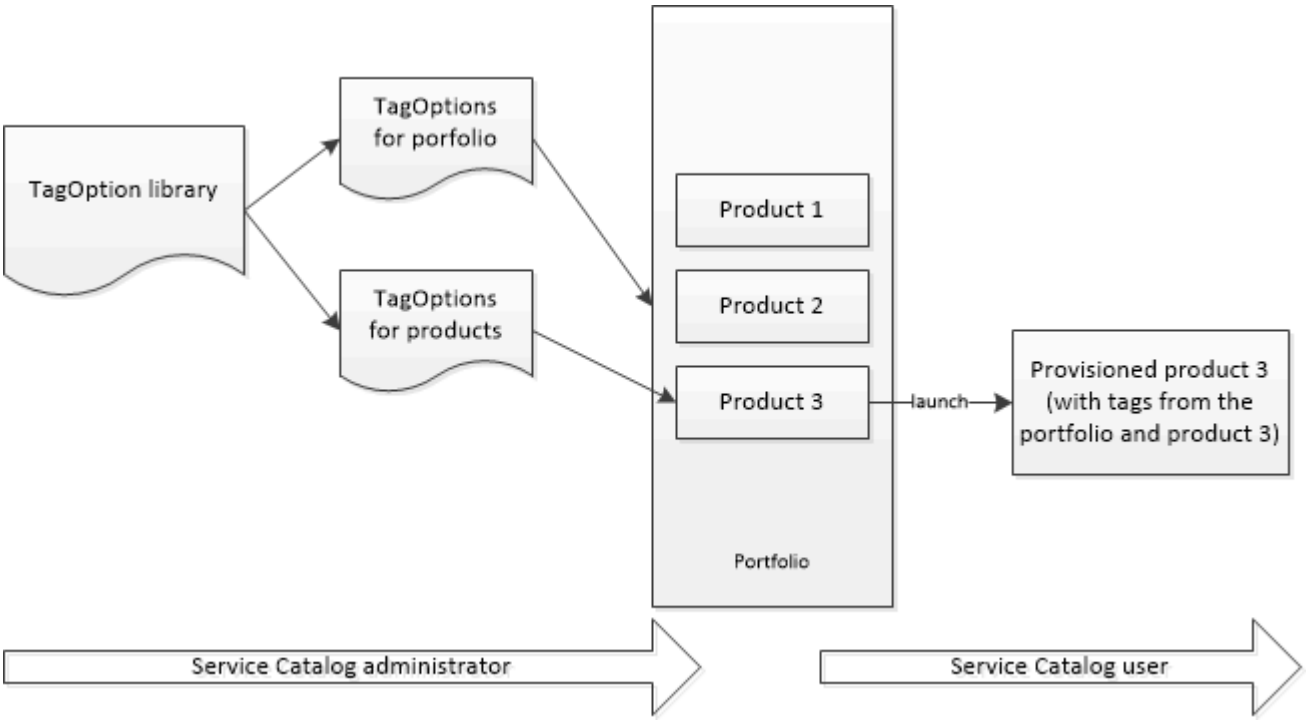
Para permitir que os administradores gerenciem facilmente as tags em produtos provisionados, AWS Service Catalog fornece uma biblioteca. TagOption A TagOption é um par de valores-chave gerenciado em. AWS Service Catalog Não é uma AWS tag, mas serve como um modelo para criar uma AWS tag com base na TagOption.

AWS Service Catalognão oferece suporte aos produtos TagOptions Terraform Open Source ou Terraform Cloud.

A TagOption biblioteca facilita a aplicação do seguinte:

- Uma taxonomia consistente
- Marcação adequada de recursos do AWS Service Catalog
- Opções definidas selecionáveis pelo usuário para tags permitidas

Os administradores podem se TagOptions associar a portfólios e produtos. Durante o lançamento de um produto (provisionamento), AWS Service Catalog agrega o portfólio e o produto TagOptions associados e os aplica ao produto provisionado, conforme mostrado no diagrama a seguir.



Com a TagOption biblioteca, você pode desativar TagOptions e manter suas associações a portfólios ou produtos e reativá-las quando precisar delas. Essa abordagem não apenas ajuda a manter a integridade da biblioteca, mas também permite gerenciar o TagOptions que pode ser usado de forma intermitente ou somente em circunstâncias especiais.

Você gerencia TagOptions com o AWS Service Catalog console ou a API da TagOption biblioteca. Para obter mais informações, consulte a Referência de APIs do Service Catalog.

Conteúdo

Lançamento de um produto com TagOptions

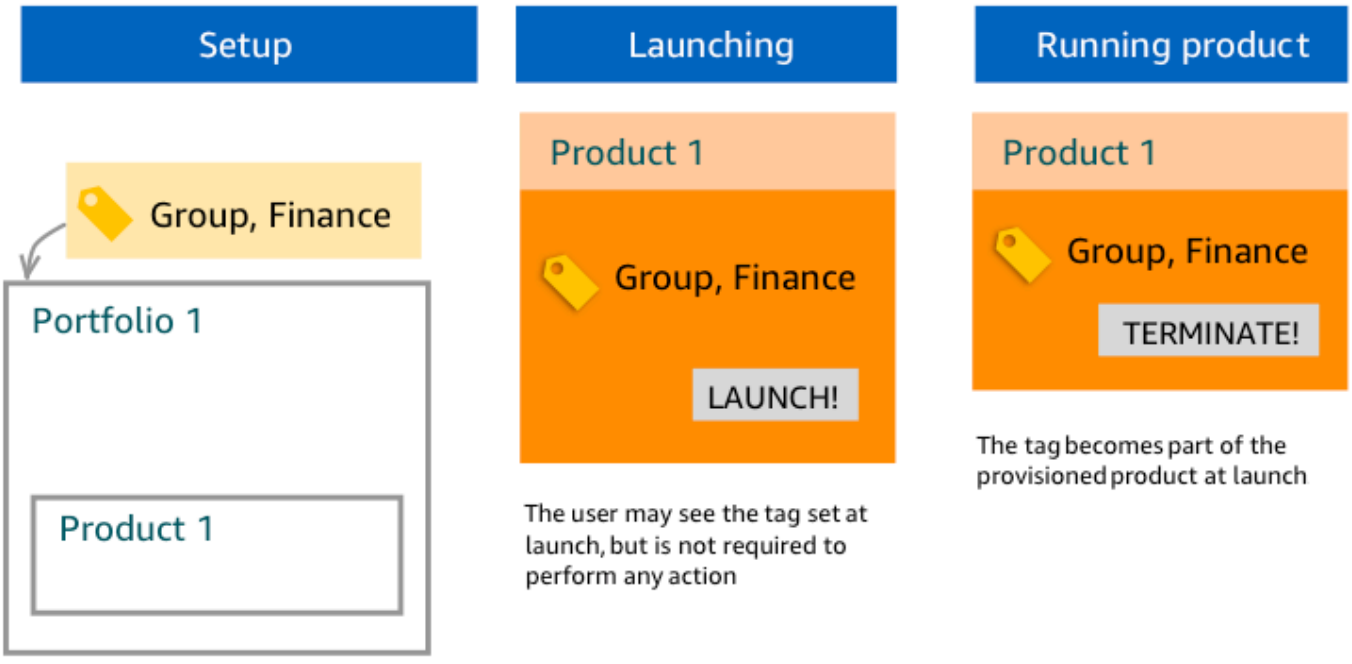
Quando um usuário lança um produto que tem TagOptions, AWS Service Catalog executa as seguintes ações em seu nome:

- Coleta tudo TagOptions para o produto e o portfólio de lançamento.
- Garante que somente TagOptions chaves exclusivas sejam usadas em uma tag no produto provisionado. Os usuários obtêm uma lista de valores de múltipla escolha para uma chave. Depois que o usuário escolhe um valor, ele se torna uma tag no produto provisionado.
- Permite que os usuários adicionem tags não conflitantes ao produto durante o provisionamento.

Os casos de uso a seguir demonstram como TagOptions funcionam durante o lançamento.

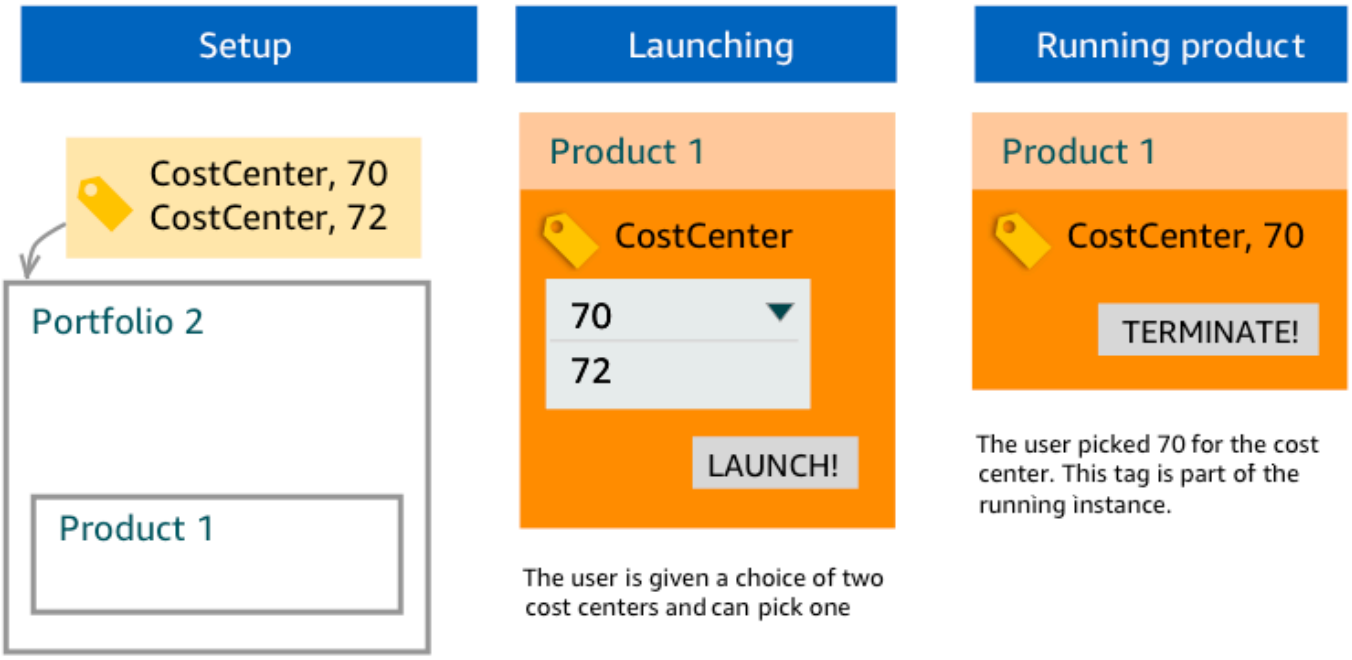
Exemplo 1: Uma TagOption chave exclusiva

Um administrador cria TagOption[Grupo=Finanças] e o associa ao Portfólio1, que tem o Produto1 sem nenhum. TagOptions Quando um usuário inicia o produto provisionado, o single TagOption se torna Tag [Group=Finance], da seguinte forma:



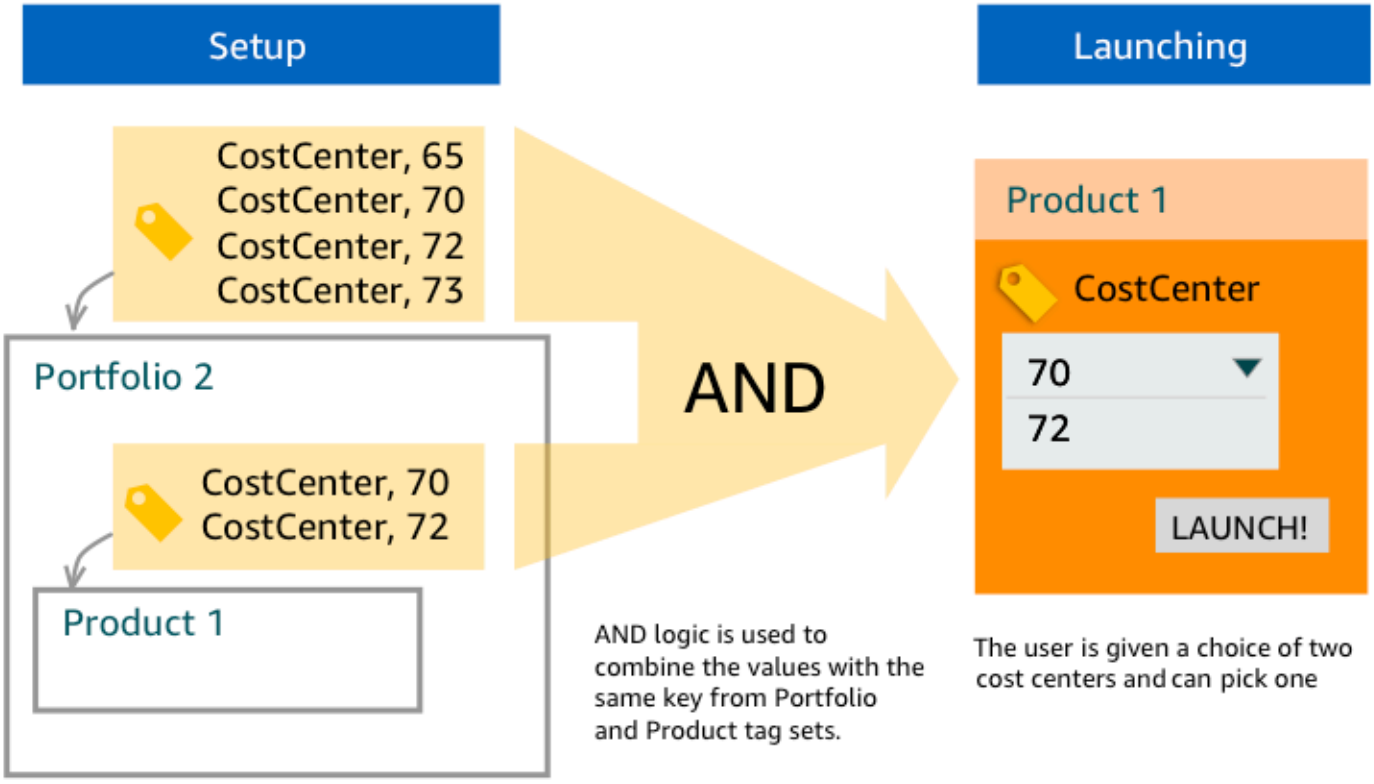
Exemplo 2: Um conjunto TagOptions com a mesma chave em um portfólio

Um administrador colocou duas TagOptions com a mesma chave em um portfólio, e não há nenhuma TagOptions com a mesma chave em nenhum produto desse portfólio. Durante o lançamento, o usuário deve selecionar um dos dois valores associados à chave. O produto provisionado é marcado com a chave e o valor selecionados pelo usuário.



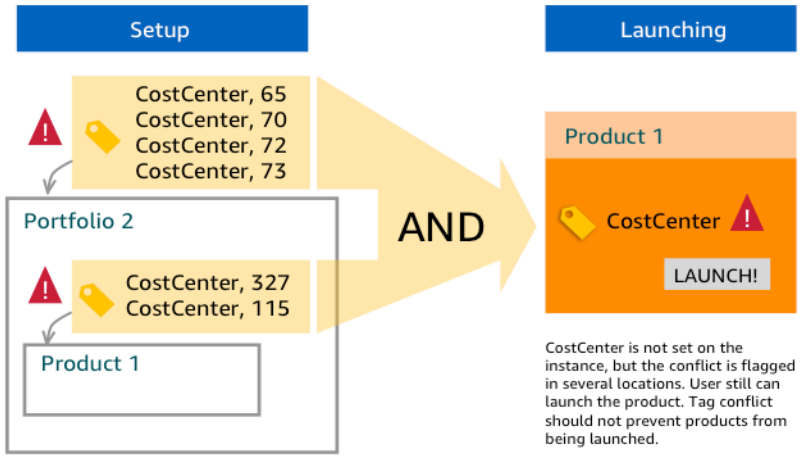
Exemplo 3: Um conjunto TagOptions com a mesma chave no portfólio e em um produto desse portfólio

Um administrador colocou vários TagOptions com a mesma chave em um portfólio, e também há vários TagOptions com a mesma chave no produto desse portfólio. AWS Service Catalogcria um conjunto de valores a partir da agregação (operação lógica AND) do TagOptions. Quando lança o produto, o usuário vê e seleciona a partir desse conjunto de valores. O produto provisionado é marcado com a chave e o valor selecionados pelo usuário.



Exemplo 4: Vários TagOptions com a mesma chave e valores conflitantes

Um administrador colocou vários TagOptions com a mesma chave em um portfólio, e também há vários TagOptions com a mesma chave no produto desse portfólio. AWS Service Catalogcria um conjunto de valores a partir da agregação (operação lógica AND) do TagOptions. Se a agregação não encontrar valores para a chave, o AWS Service Catalog criará uma tag com a mesma chave e um valor de `sc-tagconflict-`*`portfolioid`*`-`*`productid`*, onde *`portfolioid`* e *`productid`* são os ARNs do portfólio e do produto. Isso garante que o produto provisionado seja marcado com a chave correta e com um valor que o administrador pode localizar e corrigir.



Gerenciando TagOptions

Como administrador, você pode realizar as seguintes ações para gerenciar TagOptions na TagOptions biblioteca:

- Criar e excluir
- Ativar ou desativar
- Associar ou desassociar
- Edite

Para criar TagOptions no console

1. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/.
2. No menu de navegação à esquerda, escolha TagOptionsbiblioteca.
3. Em Criar novo TagOption, insira uma chave e um valor e escolha Adicionar.

   Depois que o novo TagOption é criado, ele é agrupado por par de valores-chave e classificado alfabeticamente na lista. TagOptions

   Para criar um TagOption usando a AWS Service Catalog API, consulte CreateTagOption.

Para excluir TagOptions no console

1. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/.

2. No menu de navegação à esquerda, escolha TagOptions biblioteca e, em seguida, escolha Ações.
3. Escolha Excluir e confirme a exclusão.

Para ativar ou desativar um ou mais TagOptions no console

1. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/.
2. No menu de navegação à esquerda, escolha TagOptions biblioteca e, em seguida, escolha Ações.
3. Para ativar, escolha o inativo TagOption que você deseja. Em seguida, escolha Ações e selecione Ativar no menu suspenso e confirme sua seleção.

   Para desativar, escolha o ativo que TagOption você deseja. Em seguida, escolha Ações e selecione Desativar no menu suspenso e confirme sua seleção.

Para associar ou desassociar um ou mais TagOptions de um portfólio no console

1. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/.
2. No menu de navegação à esquerda, selecione Portfólios e, em seguida, o portfólio que você deseja associar ou dissociar.
3. Escolha a TagOptionsguia e selecione uma ou mais TagOptions para associar ou desassociar do portfólio.
4. Escolha Ações. Em seguida, selecione Associar ou Desassociar e confirme sua seleção.

Para associar ou desassociar um ou mais TagOptions de um produto no console

1. Abra o console do AWS Service Catalog em: https://console.aws.amazon.com/servicecatalog/.
2. No menu de navegação à esquerda, em Administração, selecione Produtos. Em seguida, abra o produto que você deseja associar ou desassociar.
3. Escolha a TagOptionsguia e selecione uma ou mais TagOptions para associar ou desassociar do portfólio.
4. Escolha Ações. Em seguida, selecione Associar ou Desassociar e confirme sua seleção.

> **Note**
>
> Para TagOptions associar-se a um portfólio ou produto usando a AWS Service Catalog API, consulte AssociateTagOptionWithResource.
> Para remover (desassociar) TagOptions usando a AWS Service Catalog API, consulte DisassociateTagOptionFromResource.

Para editar valores para TagOptions no console

1. Abra o console do Service Catalog em https://console.aws.amazon.com/servicecatalog/.
2. No menu de navegação à esquerda, escolha TagOptionsbiblioteca.
3. Escolha um TagOption e abra o valor. (O valor tem um hiperlink.) Em seguida, escolha Editar.
4. No campo Valor, edite o valor e escolha Salvar alterações.

Usando TagOptions com políticas de AWS Organizations tag

Este tópico fornece uma breve visão geral das políticas de tags para AWS Organizations e TagOptions paraAWS Service Catalog. Também sugere como evitar conflitos de marcação ao usar os dois recursos simultaneamente.

TagOptions para AWS Service Catalog aplicar a produtos provisionados (CloudFormationpilhas), enquanto as políticas de tag AWS Organizations se aplicam a AWS contas e unidades organizacionais (OU) ou a uma raiz organizacional. Por exemplo, se você anexar uma política de tags a uma UO, a mesma política de tags se aplicará a todas as contas dessa UO. Se você usar os dois recursos de marcação simultaneamente, deverá configurá-los para que não entrem em conflito.

Políticas de tag

As políticas de tags permitem que você defina regras sobre como usar tags em recursos da AWS em suas contas em AWS Organizations. Você pode usar políticas de tags para criar e manter uma abordagem consistente para marcar recursos da AWS no nível da conta.

As políticas de tags fornecem uma maneira fácil de garantir que os usuários apliquem tags consistentes, auditem recursos marcados e mantenham a categorização adequada dos recursos. Você também pode definir como as chaves de tag devem ser capitalizadas e os valores que você deseja permitir. Por exemplo, você pode exigir que todas as instâncias do EC2 em uma conta

tenham uma chave de tag definida como **`CostCenter`** e valores para que essa tag seja **`Data Insights`** ou **`Marketing`**.

As políticas de tags permitem que você selecione opções para impor regras de marcação, evitar operações não compatíveis com tags e especificar os tipos de recursos aos quais a fiscalização se aplica. Se você não escolher uma opção de imposição, as políticas de tags permitem criar ou alterar as tags não compatíveis, mas as denunciam como não compatíveis no console AWS Organizations.

Para obter mais informações sobre como configurar a aplicação da marcação em nível de conta, consulte Políticas de tags em AWS Organizations.

TagOptions

TagOptions são um recurso de marcação que AWS Service Catalog se aplica aos produtos provisionados no nível da CloudFormation pilha se forem aplicados a um produto associado. AWS Service Catalogfornece uma TagOptions biblioteca na qual você pode definir os pares de valores-chave a serem associados aos seus AWS Service Catalog produtos. Ao lançar um AWS Service Catalog produto, você deve escolher TagOption valores para as TagOption chaves existentes associadas a esse portfólio ou produto para lançar esse produto. Como você define os TagOptions níveis de portfólio ou produto, você pode aplicar uma taxonomia consistente para marcação com portfólios compartilhados entre contas e regiões.

Para obter mais informações sobre como configurar TagOptions AWS Service Catalog, consulte AWS Service Catalog TagOption Biblioteca.

Evitando conflitos entre políticas de AWS Organizations tags e AWS Service Catalog TagOptions

Se você configurar políticas de tags AWS Organizations para contas em sua organização, recomendamos o seguinte:

- Compartilhe os requisitos de etiquetas de conformidade com administradores que também TagOptions gerenciam AWS Service Catalog portfólios e produtos.
- Compartilhe os requisitos de etiquetas de conformidade com os usuários finais que possam lançar produtos AWS Service Catalog e anexe etiquetas de usuário final opcionais aos lançamentos de seus produtos.

Suponha que você queira lançar um produto AWS Service Catalog que use a TagOption chave `city` e tenha uma política de tags que exija que as chaves de tag tenham valores de tag de cidades dos

EUA**`Atlanta`**, como**`San Francisco`**, ou**`Austin`**. `city` AWS Service Catalognão permite que você lance um produto sem ter selecionado TagOption valores para as TagOption chaves necessárias para um produto.

Nesse caso, se você tiver TagOption valores para a TagOption chave `city` que incluam cidades da América do Sul, como **`Rio de Janeiro`** ou**`Buenos Aires`**, não AWS Service Catalog lançará o produto. Em vez disso, você deve selecionar um TagOption valor que inclua uma cidade dos EUA durante o lançamento para estar em conformidade com a política de tags.

A tabela a seguir fornece cenários que descrevem como resolver os problemas de conflito de marcação que você pode encontrar ao usar políticas de tag e ao TagOptions mesmo tempo.

Cenário	Motivo	Solução
O produto não é lançado devido a tags não compatíve is se a aplicação de tags for verificada na política de tags.	Especificar TagOptions com chaves e valores que você não adicionou à lista permitida de tags compatíveis em sua política de tags. Adicionar tags personalizadas opcionais que não estão em conformidade com sua política de tags.	Se você configurar um esquema de capitalização específico em sua política de tags. A aplicação da capitalização de chaves de tag, certifique-se de que suas chaves de TagOptions tag e chaves de tag personalizadas opcionais sejam consistentes com o que você especificou em sua política de tags. Observe que quando a caixa de imposição de capitaliz ação da chave de tag está desmarcada em sua política de tags, isso faz com que todas as chaves de tag em minúsculas estejam em conformidade e garante que suas chaves de tag e chaves de TagOptions tag personalizadas opcionais

Cenário	Motivo	Solução
		sejam consistentes (como todas em minúsculas) com o que você exigiu em sua política de tags.
O produto falha ao iniciar devido à não conformidade com a capitalização da chave de tag.	Especificar a capitalização nas TagOptions chaves que é inconsistente com as regras de aplicação de maiúsculas e minúsculas da política de tags.	Configure corretamente suas políticas de tags. Se você não especificar a conformidade com a capitalização da chave de tag, a capitalização padrão da chave de tag será toda em minúsculas. Além disso, se você não especificar a conformidade com letras maiúsculas e minúsculas em sua política de tags, verifique se as chaves de TagOptions tag AWS Service Catalog estão todas em minúsculas para cumprir as regras de fiscalização. Se você usar uma política de tags que não tenha a conformidade com letras maiúsculas ativada, essa política de tags considera rá apenas todas as chaves de tag em minúsculas como compatíveis.

Cenário	Motivo	Solução
O produto falha no lançamento devido a valores de tag incompatíveis.	Selecionar um valor de TagOptions tag para o lançamento de um produto que não está na sua lista de permissões de conformidade com valores de tags.	Associe TagOptions aos seus produtos e portfólios que sejam consistentes com o que você exigiu na política de etiquetas Valores de etiquetas Conformidade com valores de etiquetas permitidos.

Motores externos para AWS Service Catalog

Em AWS Service Catalog, os motores externos são representados por meio de um tipo de `EXTERNAL` produto. O tipo de `EXTERNAL` produto permite a integração de mecanismos de provisionamento de terceiros, como o Terraform. Você pode usar mecanismos externos para estender os recursos do Service Catalog além dos AWS CloudFormation modelos nativos, permitindo o uso de outras ferramentas de infraestrutura como código (IaC).

O tipo de `EXTERNAL` produto permite gerenciar e implantar recursos usando a interface familiar do Service Catalog e, ao mesmo tempo, aproveitar os recursos e a sintaxe específicos da ferramenta de IaC escolhida.

Para habilitar tipos de `EXTERNAL` produtos no Service Catalog, você deve definir um conjunto de recursos padrão em sua conta. Esses recursos são conhecidos como mecanismo. O Service Catalog delega tarefas ao mecanismo em pontos específicos das operações de análise e provisionamento de artefatos.

Um artefato de provisionamento representa a versão específica de um produto no Service Catalog, permitindo que você gerencie e implante recursos consistentes.

Quando você chama DescribeProvisioningArtifactou AWS Service CatalogDescribeProvisioningParametersopera um artefato de provisionamento para um tipo de `EXTERNAL` produto, o Service Catalog invoca uma AWS Lambda função no mecanismo. Isso é necessário para extrair a lista de parâmetros do artefato de provisionamento fornecido e devolvê-los ao. AWS Service Catalog Esses parâmetros serão usados posteriormente como parte do processo de provisionamento.

Quando você `EXTERNAL` provisiona um artefato de provisionamento por meio de uma chamada ProvisionProduct, o Service Catalog primeiro executa algumas ações internamente e, em seguida, envia uma mensagem para uma fila do Amazon SQS no mecanismo. Em seguida, o mecanismo assume a função de lançamento fornecida (a função do IAM que você atribui a um produto como restrição de lançamento), provisiona os recursos com base no artefato de provisionamento fornecido e invoca a NotifyProvisionProductEngineWorkflowResultAPI para relatar sucesso ou falha.

As chamadas para UpdateProvisionedProducte TerminateProvisionedProductsão tratadas da mesma forma, com cada uma tendo uma fila e APIs de notificação distintas:

- NotifyProvisionProductEngineWorkflowResult

- NotifyUpdateProvisionedProductEngineWorkflowResult
- NotifyTerminateProvisionedProductEngineWorkflowResult.

Tópicos

Considerações

Limite de um mecanismo externo por conta de hub

Você só pode usar um mecanismo de `EXTERNAL` provisionamento por conta do hub do Service Catalog. O hub-and-spokemodelo Service Catalog permite que a conta hub crie produtos básicos e compartilhe o portfólio, enquanto as contas spoke importam portfólios e aproveitam os produtos.

Esse limite é porque só `EXTERNAL` pode ser roteado para um mecanismo em uma conta. Se um administrador quiser ter vários mecanismos externos, ele deverá configurar os mecanismos externos (junto com os portfólios e produtos) em diferentes contas do hub.

Mecanismos externos suportam apenas funções de lançamento com restrições de lançamento

`EXTERNAL`artefatos de provisionamento suportam somente o provisionamento com funções de lançamento que são especificadas usando restrições de lançamento. Uma restrição de lançamento especifica a função do IAM que o Service Catalog assume quando um usuário final lança, atualiza ou encerra um produto. Para obter mais informações sobre restrições de lançamento, consulte Restrições de AWS Service Catalog lançamento.

Análise de parâmetros

`EXTERNAL`os artefatos de provisionamento podem ser de qualquer formato. Isso significa que, ao criar um tipo de `EXTERNAL` produto, o mecanismo precisa extrair a lista de parâmetros do artefato

de provisionamento fornecido e devolvê-los ao Service Catalog. Isso é feito criando uma função Lambda em sua conta que pode aceitar o seguinte formato de solicitação, processar o artefato de provisionamento e retornar o seguinte formato de resposta.

> **Important**
>
> A função Lambda deve ser nomeada. `ServiceCatalogExternalParameterParser`

Sintaxe da solicitação:

```
{
    "artifact": {
        "path": "string",
        "type": "string"
    },
    "launchRoleArn": "string"
}
```

Campo	Tipo	Obrigatório	Descrição
artefato	objeto	Sim	Detalhes do artefato a ser analisado.
artefato/caminho	string	Sim	Local de onde o analisador baixa o artefato. Por exemplo, para`AWS_S3`, esse é o URI do Amazon S3.
artefato/tipo	string	Sim	Tipo de artefato. Valor permitido:`AWS_S3`.
Função de lançamento	string	Não	O Amazon Resource Name (ARN) da função de lançamento a ser assumida ao baixar o artefato. Se nenhuma função

Campo	Tipo	Obrigatório	Descrição
			de lançamento for fornecida, a função de execução do Lambda será usada.

Sintaxe da resposta:

```
{
    "parameters": [
        {
            "key": "string"
            "defaultValue": "string",
            "type": "string",
            "description": "string",
            "isNoEcho": boolean
        },
    ]
}
```

Campo	Tipo	Obrigatório	Descrição
parâmetros	list	Sim	A lista de parâmetros que o Service Catalog solicita que o usuário final forneça ao provisionar um produto ou atualizar um produto provisionado. Se nenhum parâmetro for definido no artefato, uma lista vazia será retornada.
chave	string	Sim	A chave de parâmetro.

Campo	Tipo	Obrigatório	Descrição
defaultValue	string	Não	O valor padrão do parâmetro se o usuário final não fornecer um valor.
tipo	string	Sim	O tipo esperado do valor do parâmetro para o motor. Por exemplo, uma string, booleano ou mapa. Os valores permitidos são específicos para cada motor. O Service Catalog passa cada valor de parâmetro para o mecanismo como uma string.
description	string	Não	Descrição do parâmetro. Recomenda-se que seja fácil de usar.
isNoEcho	boolean	não	Determina se o valor do parâmetro não é repetido nos registros . O valor padrão é falso (os valores dos parâmetros são repetidos).

Provisionamento

Para a ProvisionProductoperação, o Service Catalog delega o provisionamento real dos recursos ao mecanismo. O mecanismo é responsável pela interface com a solução de IaC de sua escolha

(como o Terraform) para provisionar recursos conforme definido no artefato. O mecanismo também é responsável por notificar o Service Catalog sobre o resultado.

O Service Catalog envia todas as solicitações de provisão para uma fila do Amazon SQS em sua conta chamada. `ServiceCatalogExternalProvisionOperationQueue`

Sintaxe da solicitação:

```
{
    "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	Obrigatório	Descrição
token	string	Sim	O token que identifica essa operação. O token deve ser devolvido ao Service Catalog para notificar os resultados da execução.
operação	string	Sim	Esse campo deve ser `PROVISION_PRODUCT` para essa operação.
provisionedProductId	string	Sim	ID do produto provisionado.
provisionedProductName	string	Sim	Nome do produto provisionado.
ID do produto	string	Sim	ID do produto.
provisioningArtifactId	string	Sim	ID do artefato de provisionamento.
recordId	string	Sim	ID do registro do Service Catalog para essa operação.
launchRoleArn	string	Sim	Nome de recurso da Amazon (ARN) para a função do IAM a ser usada para provisionar recursos.
artefato	objeto	Sim	Detalhes do artefato que define como

Campo	Tipo	Obrigatório	Descrição
			os recursos são provisionados.
artefato/caminho	string	Sim	Local de onde o motor baixa o artefato. Por exemplo, para`AWS_S3`, esse é o URI do Amazon S3.
artefato/tipo	string	Sim	Tipo de artefato. Valor permitido:`AWS_S3`.
identidade	string	Não	O campo não é usado atualmente.
parâmetros	list	Sim	Lista de pares de valores-chave de parâmetros que o usuário inseriu no Service Catalog como entradas para essa operação.
tags	list	Sim	Lista key-value-pairs do usuário inserido no Service Catalog como tags para aplicar aos recursos provision ados.

Notificação do resultado do fluxo de trabalho

Invoque a NotifyProvisionProductEngineWorkflowResult API com o objeto de resposta especificado na página de detalhes da API.

Atualizando

Para a UpdateProvisionedProductoperação, o Service Catalog delega a atualização real dos recursos ao mecanismo. O mecanismo é responsável pela interface com a solução de IaC de sua escolha (como o Terraform) para atualizar os recursos conforme definido no artefato. O mecanismo também é responsável por notificar o Service Catalog sobre o resultado.

O Service Catalog envia todas as solicitações de atualização para uma fila do Amazon SQS em sua conta chamada. `ServiceCatalogExternalUpdateOperationQueue`

Sintaxe da solicitação:

```
{
    "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	Obrigatório	Descrição
token	string	Sim	O token que identifica a essa operação. O token deve ser devolvido ao Service Catalog para notificar os resultados da execução.
operação	string	Sim	Esse campo deve ser `UPDATE_PROVISION_PRODUCT` para essa operação.
provisionedProductId	string	Sim	ID do produto provisionado.
provisionedProductName	string	Sim	Nome do produto provisionado.
ID do produto	string	Sim	ID do produto.
provisioningArtifactId	string	Sim	ID do artefato de provisionamento.
recordId	string	Sim	ID do registro do Service Catalog para essa operação.
launchRoleArn	string	Sim	Nome de recurso da Amazon (ARN) para a função do IAM a ser usada para provisionar recursos.

Campo	Tipo	Obrigatório	Descrição
artefato	objeto	Sim	Detalhes do artefato que define como os recursos são provisionados.
artefato/caminho	string	Sim	Local de onde o motor baixa o artefato. Por exemplo, para`AWS_S3`, esse é o URI do Amazon S3.
artefato/tipo	string	Sim	Tipo de artefato. Valor permitido:`AWS_S3`.
identidade	string	Não	O campo não é usado atualmente.
parâmetros	list	Sim	Lista de pares de valores-chave de parâmetros que o usuário inseriu no Service Catalog como entradas para essa operação.
tags	list	Sim	Lista key-value-pairs do usuário inserido no Service Catalog como tags para aplicar aos recursos provision ados.

Notificação do resultado do fluxo de trabalho

Invoque a NotifyUpdateProvisionedProductEngineWorkflowResultAPI com o objeto de resposta especificado na página de detalhes da API.

Encerrando

Para a TerminateProvisionedProductoperação, o Service Catalog delega o encerramento real dos recursos ao mecanismo. O mecanismo é responsável pela interface com a solução IaC de sua escolha (como o Terraform) para encerrar os recursos conforme definido no artefato. O mecanismo também é responsável por notificar o Service Catalog sobre o resultado.

O Service Catalog envia todas as solicitações de encerramento para uma fila do Amazon SQS em sua conta chamada. `ServiceCatalogExternalTerminateOperationQueue`

Sintaxe da solicitação:

```
{
    "token": "string",
    "operation": "string",
    "provisionedProductId": "string",
    "provisionedProductName": "string",
    "recordId": "string",
    "launchRoleArn": "string",
    "identity": {
        "principal": "string",
        "awsAccountId": "string",
        "organizationId": "string"
    }
}
```

Campo	Tipo	Obrigatório	Descrição
token	string	Sim	O token que identifica a essa operação. O token deve ser devolvido ao Service Catalog para notificar os resultados da execução.
operação	string	Sim	Esse campo deve ser `TERMINATE_PROVISIO`

Campo	Tipo	Obrigatório	Descrição
			N_PRODUCT para essa operação.
provisionedProductId	string	Sim	ID do produto provisionado.
provisionedProduct Name	string	Sim	Nome do produto provisionado.
recordId	string	Sim	ID do registro do Service Catalog para essa operação.
launchRoleArn	string	Sim	Nome de recurso da Amazon (ARN) para a função do IAM a ser usada para provision ar recursos.
identidade	string	Não	O campo não é usado atualmente.

Notificação do resultado do fluxo de trabalho

Invoque a NotifyTerminateProvisionedProductEngineWorkflowResultAPI com o objeto de resposta especificado na página de detalhes da API.

Tags

Para gerenciar tags por meio de Resource Groups, sua função inicial precisa das seguintes declarações de permissão adicionais:

```
{
    "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**
>
> A função de lançamento também precisa de permissões de marcação nos recursos específicos do artefato, como. `ec2:CreateTags`

Monitorar o AWS Service Catalog

Você pode monitorar seus AWS Service Catalog recursos usando a Amazon CloudWatch, que coleta e processa dados brutos AWS Service Catalog em métricas legíveis. Essas estatísticas são registradas por um período de duas semanas para que você possa acessar informações históricas e obter uma perspectiva melhor sobre o desempenho de seu serviço. Os dados de métricas do AWS Service Catalog são enviados automaticamente para o CloudWatch em períodos de 1 minuto. Para obter mais informações sobre CloudWatch, consulte o Guia CloudWatch do usuário da Amazon.

Para obter uma lista das métricas e dimensões disponíveis, consulte AWS Service Catalog CloudWatch Métricas.

O monitoramento é uma parte importante da manutenção da confiabilidade, da disponibilidade e do desempenho do AWS Service Catalog e de soluções da AWS. Você deve coletar dados de monitoramento de todas as partes de sua solução da AWS, para facilitar a depuração de uma falha multipontos, caso ocorra. Antes de começar a monitorar o AWS Service Catalog, crie um plano de monitoramento que inclua as respostas para as seguintes perguntas:

- Quais são seus objetivos de monitoramento?
- Quais recursos você vai monitorar?
- Com que frequência você vai monitorar esses recursos?
- Quais ferramentas de monitoramento você usará?
- Quem realizará o monitoramento das tarefas?
- Quem deve ser notificado quando algo der errado?

Ferramentas de monitoramento

A AWS fornece várias ferramentas que você pode usar para monitorar AWS Service Catalog. É possível configurar algumas dessas ferramentas para fazer o monitoramento em seu lugar, e, ao mesmo tempo, algumas das ferramentas exigem intervenção manual. Recomendamos que as tarefas de monitoramento sejam automatizadas ao máximo possível.

Ferramentas de monitoramento automatizadas

Você pode usar CloudWatch os alarmes da Amazon para monitorar AWS Service Catalog e relatar interrupções.

CloudWatch os alarmes observam uma única métrica em um período especificado por você e executam uma ou mais ações com base no valor da métrica em relação a um determinado limite em vários períodos. A ação é uma notificação enviada para um tópico do Amazon Simple Notification Service (Amazon SNS) ou para uma política do Amazon EC2 Auto Scaling. CloudWatch os alarmes não invocam ações simplesmente porque estão em um determinado estado; o estado deve ter sido alterado e mantido por um determinado número de períodos. Para saber como criar um alarme, consulte Criação de CloudWatch alarmes na Amazon. Para obter mais informações sobre como usar CloudWatch as métricas da Amazon comAWS Service Catalog, consulteAWS Service Catalog CloudWatch Métricas.

AWS Service Catalog CloudWatch Métricas

Você pode monitorar seus AWS Service Catalog recursos usando a Amazon CloudWatch, que coleta e processa dados brutos AWS Service Catalog em métricas legíveis. Essas estatísticas são registradas por um período de duas semanas para que você possa acessar informações históricas e obter uma perspectiva melhor sobre o desempenho de seu serviço. Os dados de métricas do AWS Service Catalog são enviados automaticamente para o CloudWatch em períodos de 1 minuto. Para obter mais informações sobre CloudWatch, consulte o Guia CloudWatch do usuário da Amazon.

Tópicos

- Habilitando CloudWatch métricas
- Métricas e dimensões disponíveis
- Visualizar métricas do AWS Service Catalog

Habilitando CloudWatch métricas

CloudWatch As métricas da Amazon são ativadas por padrão.

Métricas e dimensões disponíveis

As métricas e dimensões AWS Service Catalog enviadas para a Amazon CloudWatch estão listadas abaixo.

Métricas do AWS Service Catalog

O namespace `AWS/ServiceCatalog` inclui as métricas a seguir.

Métrica	Descrição
`ProvisionedProductLaunch`	O número de produtos provisionados iniciados para um determinado produto e artefato de provisionamento em um período especificado. Unidades: contagem Estatísticas válidas: mínimo, máximo, soma, média

Dimensões para métricas do AWS Service Catalog

AWS Service Catalogenvia as seguintes dimensões para a Amazon CloudWatch.

Dimensão	Descrição
`State`	Essa dimensão filtra os dados que você solicita para todos os produtos provisionados iniciados com esse estado especificado. Isso ajuda você a categorizar seus dados pelo estado de execução. Estado válido: SUCCEEDED, FAILED
`ProductId`	Essa dimensão filtra os dados que você solicita somente para o id do produto identificado. Isso ajuda a localizar um produto exato a partir do qual executar.
`ProvisioningArtifactId`	Essa dimensão filtra os dados que você solicita somente para o id do artefato de provisionamento. Isso ajuda a localizar uma versão exata dos produtos partir da qual executar.

Visualizar métricas do AWS Service Catalog

Você pode visualizar CloudWatch as métricas da Amazon no CloudWatch console da Amazon, que fornece uma exibição refinada e personalizável de seus recursos, bem como o número de tarefas em execução em um serviço.

Tópicos

Visualização de AWS Service Catalog métricas no Amazon CloudWatch Console

Você pode visualizar AWS Service Catalog as métricas no CloudWatch console da Amazon. O CloudWatch console da Amazon fornece uma visão detalhada das AWS Service Catalog métricas, e você pode personalizar as visualizações de acordo com suas necessidades. Para obter mais informações sobre a Amazon CloudWatch, consulte o Guia CloudWatch do usuário da Amazon.

Para visualizar métricas no CloudWatch console da Amazon

1. Abra o CloudWatch console da Amazon em https://console.aws.amazon.com/cloudwatch/.
2. Na seção Metrics (Métricas) do painel de navegação esquerdo, selecione Service Catalog (Catálogo de serviços).
3. Escolha as métricas a serem exibidas.

Registrar em log chamadas de API do AWS Service Catalog usando o AWS CloudTrail

AWS Service Catalogé integrado comAWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS serviço emAWS Service Catalog. CloudTrail captura todas as chamadas de API AWS Service Catalog como eventos. As chamadas capturadas incluem as aquelas do AWS Service Catalog console e chamadas de código para AWS Service Catalog operações API. Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para. AWS Service Catalog Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feitaAWS Service Catalog, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

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

AWS Service Cataloginformações em CloudTrail

CloudTrail é ativado em sua AWS conta quando você a cria. Quando a atividade ocorre emAWS Service Catalog, essa atividade é registrada em um CloudTrail evento junto com outros eventos AWS

de serviço no histórico de eventos. É possível visualizar, pesquisar e baixar os eventos recentes em sua conta da AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo de eventos em sua AWS conta, inclusive eventos para AWS Service Catalog, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na partição da AWS e entrega os arquivos de log no bucket do Amazon S3 que você especificou Além disso, você pode configurar outros AWS serviços para analisar e agir com base nos dados de eventos coletados nos CloudTrail registros. Para obter mais informações, consulte:

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

CloudTrail registra todas AWS Service Catalog as ações. Por exemplo, chamadas para o `CreatePortfolio` `CreateProduct` e `UpdateProvisionedProduct` as ações geram entradas nos arquivos de CloudTrail log.

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

- Se a solicitação foi feita com credenciais de usuário raiz ou usuário do IAM AWS Identity and Access Management
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da AWS.

Para obter mais informações, consulte Elemento userIdentity do CloudTrail .

Noções básicas sobre entradas de arquivos de log do AWS Service Catalog

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais

entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica. O exemplo a seguir mostra uma entrada de CloudTrail registro que demonstra a `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"
```

```
}
```

Preferências de marca do console

AWS Service Catalog permite que os administradores especifiquem as preferências de marca do console para contas. Os administradores podem usar a identidade visual do console para especificar o nome da empresa, a imagem do logotipo e uma cor primária e secundária (de destaque) para uma variedade de componentes do site. Essas preferências de marca são visíveis tanto para administradores quanto para usuários finais ao usar o console.

As preferências de marca do console aprimoram a aparência de uma conta e realizam o seguinte:

- Criam uma transição visual perfeita entre o console e os aplicativos internos
- Distinguem contas usadas por diferentes equipes internas dentro da mesma empresa
- Diferenciam contas em vários ambientes, como desenvolvimento, preparação ou produção

> **Note**
>
> Administradores especificam as preferências de marca do console para contas.

Como especificar as preferências de marca do console

1. No menu de navegação à esquerda, escolha Preferências.
2. Escolha Editar para as preferências de marca no modo claro ou no modo escuro.
3. Faça upload de um logotipo, insira o nome da marca e selecione a cor primária e a cor secundária.
4. Escolha Salvar.

Para obter uma lista das regiões em que AWS Service Catalog oferece suporte à marca do console, consulte o suporte da Região da AWS para a marca do console.

Suporte da Região da AWS para preferências de marca do console

AWS Service Catalog suporta as preferências de marca do console nas Regiões da AWS listadas na tabela abaixo.

Nome do Região da AWS	Identidade do Região da AWS	
Leste dos EUA (Norte da Virgínia)	us-east-1	
Leste dos EUA (Ohio)	us-east-2	
Oeste dos EUA (Norte da Califórnia)	us-west-1	
Oeste dos EUA (Oregon)	us-west-2	
África (Cidade do Cabo)	af-south-1	
Ásia-Pacífico (Hong Kong)	ap-east-1	
Ásia-Pacífico (Jacarta)	ap-southeast-3	
Ásia-Pacífico (Mumbai)	ap-south-1	
Ásia-Pacífico (Osaka)	ap-northeast-3	
Ásia-Pacífico (Seul)	ap-northeast-2	
Ásia-Pacífico (Singapura)	ap-southeast-1	
Ásia-Pacífico (Sydney)	ap-southeast-2	
Ásia-Pacífico (Tóquio)	ap-northeast-1	
Canadá (Central)	ca-central-1	
Europa (Frankfurt)	eu-central-1	
Europa (Irlanda)	eu-west-1	
Europa (Londres)	eu-west-2	
Europa (Milão)	eu-south-1	
Europa (Paris)	eu-west-3	
Europa (Estocolmo)	eu-north-1	

Nome do Região da AWS	Identidade do Região da AWS	
Oriente Médio (Barém)	me-south-1	
América do Sul (São Paulo)	sa-east-1	
AWS GovCloud (Leste dos EUA)	us-gov-east-1	
AWS GovCloud (Oeste dos EUA)	us-gov-west-1	

Histórico do documento

A tabela a seguir descreve as mudanças importantes na documentação do AWS Service Catalog. Para receber notificações sobre atualizações dessa documentação, você poderá se inscrever em um feed RSS.

- Versão da API: 12/11/2014
- Última atualização da documentação: 16 de maio de 2024

Alteração	Descrição	Data
Motores externos para AWS Service Catalog	AWS Service Catalog adiciona nova documentação para mecanismos externos. Os motores externos são representados por meio de um tipo de `EXTERNAL` produto. O tipo de `EXTERNAL` produto permite a integração de mecanismos de provision amento de terceiros, como o Terraform. Você pode usar mecanismos externos para estender os recursos do Service Catalog além dos AWS CloudFormation modelos nativos, permitindo o uso de outras ferramentas de infraestr utura como código (IaC). Para obter mais informações, consulte Mecanismos externos para AWS Service Catalog.	16 de maio de 2024
Atualização de segurança do IAM	AWS Service Catalog atualiza a `AWSServiceCatalogS yncServiceRolePoli`	7 de maio de 2024

	cy política para mudar `codestar-connections` para `codeconnections`. Para obter mais informações, consulte AWS Políticas gerenciadas para o AWS Service Catalog AppRegistry.	

Atualizações anteriores

A tabela a seguir descreve o histórico de lançamento da documentação AWS Service Catalog antes de 25 de abril de 2024.

Atributo	Descrição	Data de lançamento
AWS Service Catalog	Para saber mais sobre as mudanças da Hashicorp no licenciamento e na atualização do Terraform para o tipo de produto externo, consulte Atualizar os produtos existentes do Terraform Open Source e dos produtos provisionados para o tipo de produto External.	20 de outubro de 2023
AWS Service Catalog	Para saber mais sobre como compartilhar um portfólio AWS Organizations e permitir AWS Service Catalog a sincronização com ele AWS Organizations, consulte a AWSServiceCatalogOrgsDataSyncServiceRolePolicypolítica e a função AWSServic	14 de abril de 2023

Atributo	Descrição	Data de lançamento
	eRoleForServiceCatalogOrgsDataSyncvinculada ao serviço.	
AWS Service Catalog	Para saber mais sobre como gerenciar produtos conectados ao git e permitir AWS Service Catalog a sincronização de modelos em um repositório externo com seus AWS Service Catalog produtos, consulte a AWSServiceCatalogSyncServiceRolePolicypolítica e a função vinculada ao serviço. AWSServiceRoleForServiceCatalogSync	18 de novembro de 2022
AWS Service Catalog AppRegistry	Para saber como AppRegistry ajudar a armazenar seus AWS aplicativos, suas coleções de recursos associadas e grupos de atributos de aplicativos, consulte AWS Service Catalog AppRegistry.	15 de junho de 2022
AWS Service Management Connector	Para saber mais sobre conectores para o Jira Service Management e ServiceNow, consulte Conector de gerenciamento AWS de serviços.	9 de junho de 2022

Atributo	Descrição	Data de lançamento
Conector para Jira Service Management	Para saber mais sobre as atualizações do conector para Jira Service Management, consulte Service Management Connector da AWS para Jira Service Management.	25 de maio de 2021
Conector para ServiceNow	Para saber mais sobre as atualizações do Connector for ServiceNow, consulte AWS Service Management Connector for ServiceNow.	7 de abril de 2021
Conector para ServiceNow	Para saber mais sobre as atualizações do Connector for ServiceNow, consulte AWS Service Management Connector for ServiceNow.	24 de setembro de 2020
AWS Service Quotas	Para saber mais sobre como AWS Service Catalog funciona com Cotas AWS de Serviço, consulte Cotas de serviço AWS Service Catalog padrão.	24 de março de 2020
Biblioteca de conceitos básicos	Para saber mais sobre a biblioteca de modelos de produtos bem arquitetados oferecidos pela AWS Service Catalog, consulte Biblioteca de conceitos básicos	10 de março de 2020

Atributo	Descrição	Data de lançamento
Orientações sobre versões	Para saber mais sobre a orientações sobre versões do produto, consulte Orientações sobre versões.	17 de dezembro de 2019
Conector para Jira Service Desk	Para começar a usar o Conector para o Jira Service Desk, consulte Service Management Connector da AWS para o Jira Service Desk.	21 de novembro de 2019
Conector para ServiceNow	Para saber mais sobre as atualizações do Connector for ServiceNow, consulte AWS Service Management Connector for ServiceNow.	18 de novembro de 2019
Novo capítulo de segurança	Para saber mais sobre segurança em AWS Service Catalog, consulte Segurança em AWS Service Catalog.	31 de outubro de 2019
Alterar o proprietário do produto provisionado	Para saber mais sobre como alterar o proprietário de produtos provisionados, consulte Alterar o Proprietário do Produto Provisionado.	31 de outubro de 2019
Nova restrição de atualização do recurso	Para saber mais sobre como usar a restrição RESOURCE_UPDATE para atualizar tags em produtos provision ados, consulte Restrições de Atualização de Tag AWS Service Catalog.	17 de abril de 2019

Atributo	Descrição	Data de lançamento
Conector para ServiceNow	Para começar a usar o Conector para ServiceNow, consulte Conector de gerenciamento de AWS serviços para ServiceNow.	19 de março de 2019
Support for AWS CloudFormation StackSets	Para começar a usar AWS CloudFormation StackSets, consulte Usando AWS CloudFormation StackSets.	14 de novembro de 2018
Ações de autoatendimento	Para começar a usar ações de autoatendimento, consulte AWS CloudFormation Ações de atendimento.	17 de outubro de 2018
CloudWatch Métricas da Amazon	Para saber mais sobre CloudWatch as métricas da Amazon, consulte AWS Service CatalogAmazon CloudWatch.	26 de setembro de 2018
Support for TagOptions	Para gerenciar tags, consulte AWS Service Catalog TagOptionBiblioteca.	28 de junho de 2017
Importação de um portfólio	Para importar um portfólio compartilhado de outra AWS conta, consulte Importação de um portfólio.	16 de fevereiro de 2016
Atualizações em informações de permissões	Para conceder acesso à visualização do console do usuário final, consulte Acesso ao console para usuários finais.	16 de fevereiro de 2016

Atributo	Descrição	Data de lançamento
Lançamento inicial	Esta é a versão inicial do Guia do AWS Service Catalog Administrador.	9 de julho de 2015

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.