Panduan Administrator

AWS Service Catalog

AWS Service Catalog: Panduan Administrator

Table of Contents

Apa itu Service Catalog?

Service Catalog memungkinkan organisasi untuk membuat dan mengelola katalog layanan TI yang disetujui. AWS Layanan IT ini dapat mencakup segala sesuatu mulai dari citra mesin virtual, server, perangkat lunak, basis data, dan banyak lagi untuk menyelesaikan arsitektur aplikasi multi-tingkat.

Service Catalog memungkinkan organisasi untuk mengelola layanan TI yang umum digunakan secara terpusat, dan membantu organisasi mencapai tata kelola yang konsisten dan memenuhi persyaratan kepatuhan. Pengguna akhir dapat dengan cepat men-deploy hanya layanan IT yang disetujui yang mereka butuhkan, mengikuti batasan yang ditetapkan oleh organisasi Anda.

Service Catalog memberikan manfaat sebagai berikut:

- Standardisasi

  Urus dan kelola aset yang disetujui dengan membatasi tempat peluncuran produk, tipe instans yang dapat digunakan, dan banyak opsi konfigurasi lainnya. Hasilnya adalah lanskap standar untuk penyediaan produk untuk seluruh organisasi Anda.
- Penemuan dan peluncuran swalayan

  Pengguna menelusuri daftar produk (layanan atau aplikasi) yang dapat mereka akses, menemukan produk yang ingin mereka gunakan, dan meluncurkan semuanya sendiri sebagai produk yang disediakan.
- Kontrol akses butir halus

  Administrator merakit portofolio produk dari katalog mereka, menambahkan batasan dan tanda sumber daya untuk digunakan pada penyediaan, lalu memberikan akses ke portofolio melalui pengguna dan grup AWS Identity and Access Management (IAM).
- Ekstensibilitas dan kontrol versi

  Administrator dapat menambahkan produk ke sejumlah portofolio dan membatasinya tanpa membuat salinan lain. Memperbarui produk ke versi baru dapat menyebarkan pembaruan ke semua produk di setiap portofolio yang mereferensikannya.

Untuk informasi selengkapnya, lihat halaman detail Service Catalog.

Service Catalog API menyediakan kontrol terprogram atas semua tindakan pengguna akhir sebagai alternatif untuk menggunakan. AWS Management Console Untuk informasi selengkapnya, lihat Panduan Pengembang Service Catalog.

Video: Pengantar AWS Service Catalog

Video ini (7:27) menjelaskan cara membuat, mengatur, dan mengatur katalog produk yang dikurasi, dan berbagi AWS produk dengan tingkat izin. Akibatnya, pengguna akhir dapat dengan cepat menyediakan sumber daya TI yang disetujui tanpa akses langsung ke AWS layanan yang mendasarinya.

Pengantar AWS Service Catalog

Ikhtisar Service Catalog

Saat memulai Service Catalog, Anda akan mendapat manfaat dari memahami komponennya dan alur kerja awal untuk administrator dan pengguna akhir.

Pengguna

Service Catalog mendukung jenis pengguna berikut:

- Administrator katalog (administrator) – Kelola katalog produk (aplikasi dan layanan), mengaturnya ke dalam portofolio dan memberikan akses ke pengguna akhir. Administrator katalog mempersiapkan templat AWS CloudFormation, mengonfigurasi batasan, dan mengelola IAM role untuk produk untuk menyediakan manajemen sumber daya lanjutan.
- Pengguna akhir – Terima kredensial AWS dari departemen atau manajer IT mereka dan gunakan AWS Management Console untuk meluncurkan produk yang telah mereka berikan akses. Kadang-kadang disebut sebagai pengguna sederhana, pengguna akhir dapat diberikan izin yang berbeda tergantung pada kebutuhan operasional Anda. Misalnya, pengguna mungkin memiliki tingkat izin maksimum (untuk meluncurkan dan mengelola semua sumber daya yang diperlukan oleh produk yang mereka gunakan) atau hanya izin untuk menggunakan fitur layanan tertentu.

Produk

Produk adalah layanan IT yang ingin Anda sediakan untuk deployment di AWS. Sebuah produk terdiri dari satu atau beberapa sumber daya AWS, seperti instans EC2, volume penyimpanan, basis data, konfigurasi pemantauan, dan komponen jaringan, atau produk AWS Marketplace yang dikemas.

Sebuah produk dapat menjadi instans komputasi tunggal yang menjalankan Linux AWS, aplikasi web multi-tingkat yang dikonfigurasi sepenuhnya dan berjalan di lingkungannya sendiri, atau apa pun di antaranya.

Anda membuat produk dengan mengimpor templat AWS CloudFormation. Templat AWS CloudFormation menentukan sumber daya AWS yang diperlukan untuk produk, hubungan antara sumber daya, dan parameter yang dapat dipasang oleh pengguna akhir saat mereka meluncurkan produk untuk mengonfigurasi grup keamanan, membuat pasangan kunci, dan melakukan penyesuaian lainnya.

HashiCorp Dukungan Terraform Open Source dan Terraform Cloud

AWS Service Catalogmemungkinkan penyediaan layanan mandiri yang cepat dengan tata kelola untuk konfigurasi Terraform Open Source dan HashiCorp Terraform Cloud Anda di dalamnya. AWS Anda dapat menggunakan Service Catalog sebagai alat tunggal untuk mengatur, mengatur, dan mendistribusikan konfigurasi Terraform Anda dalam skala besar. AWS Anda dapat mengakses fitur utama Service Catalog, termasuk membuat katalog templat Terraform standar dan disetujui sebelumnya, kontrol akses, penyediaan hak istimewa, pembuatan versi, penandaan, dan berbagi ke ribuan akun. AWS Pengguna akhir Anda melihat daftar sederhana produk dan versi yang dapat mereka akses, dan kemudian dapat menyebarkan produk tersebut dalam satu tindakan.

Untuk mempelajari lebih lanjut dan menyelesaikan tutorial produk Terraform, tinjau. Memulai dengan produk Terraform

Produk yang Disediakan

AWS CloudFormationtumpukan membuatnya lebih mudah untuk mengelola siklus hidup produk Anda dengan memungkinkan Anda untuk menyediakan, menandai, memperbarui, dan menghentikan instance produk Anda sebagai satu unit. Tumpukan AWS CloudFormation menyertakan templat AWS CloudFormation, yang ditulis dalam format JSON ataupun YAML, dan koleksi sumber daya yang terkait. Produk yang disediakan adalah tumpukan. Ketika pengguna akhir meluncurkan produk, instance produk yang disediakan oleh Service Catalog adalah tumpukan dengan sumber daya yang diperlukan untuk menjalankan produk. Untuk informasi selengkapnya, lihat Panduan Pengguna AWS CloudFormation.

Portofolio

Portofolio adalah koleksi produk yang berisi informasi konfigurasi. Portofolio membantu mengelola siapa saja yang dapat menggunakan produk tertentu dan cara mereka menggunakannya. Dengan

Service Catalog, Anda dapat membuat portofolio khusus untuk setiap jenis pengguna di organisasi Anda dan secara selektif memberikan akses ke portofolio yang sesuai. Ketika Anda menambahkan versi produk baru ke portofolio, versi tersebut secara otomatis tersedia untuk semua pengguna saat ini.

Anda juga dapat berbagi portofolio Anda dengan akun AWS dan memungkinkan administrator akun untuk mendistribusikan portofolio Anda dengan batasan tambahan, seperti membatasi instans EC2 mana yang dapat dibuat pengguna. Melalui penggunaan portofolio, izin, berbagi, dan batasan, Anda dapat memastikan bahwa pengguna meluncurkan produk yang dikonfigurasi dengan benar untuk kebutuhan dan standar organisasi.

Versioning

Service Catalog memungkinkan Anda mengelola beberapa versi produk dalam katalog Anda. Pendekatan ini memungkinkan Anda untuk menambahkan versi baru templat dan sumber daya terkait berdasarkan pembaruan perangkat lunak atau perubahan konfigurasi.

Saat Anda membuat versi baru produk, pembaruan secara otomatis didistribusikan ke semua pengguna yang memiliki akses ke produk, memungkinkan pengguna untuk memilih versi produk mana yang akan digunakan. Pengguna dapat memperbarui instans berjalan produk ke versi baru dengan cepat dan mudah.

Izin

Pemberian akses pengguna ke portofolio memungkinkan pengguna untuk menelusuri portofolio dan meluncurkan produk di dalamnya. Anda menerapkan izin AWS Identity and Access Management(IAM) untuk mengontrol siapa yang dapat melihat dan mengubah katalog Anda. Izin IAM dapat ditetapkan untuk pengguna IAM, grup IAM, dan IAM role.

Saat pengguna meluncurkan produk yang memiliki peran IAM yang ditetapkan padanya, Service Catalog menggunakan peran tersebut untuk meluncurkan sumber daya cloud produk yang digunakan. AWS CloudFormation Dengan menetapkan IAM role ke setiap produk, Anda dapat menghindari pemberian izin kepada pengguna untuk melakukan operasi yang tidak disetujui dan memungkinkan mereka untuk menyediakan sumber daya menggunakan katalog.

Batasan

Batasan mengontrol cara Anda men-deploy sumber daya AWS tertentu untuk suatu produk. Anda dapat menggunakannya untuk menerapkan batasan pada produk untuk tata kelola atau

pengendalian biaya. Ada berbagai tipe batasan AWS Service Catalog: batasan peluncuran, batasan notifikasi, dan batasan templat.

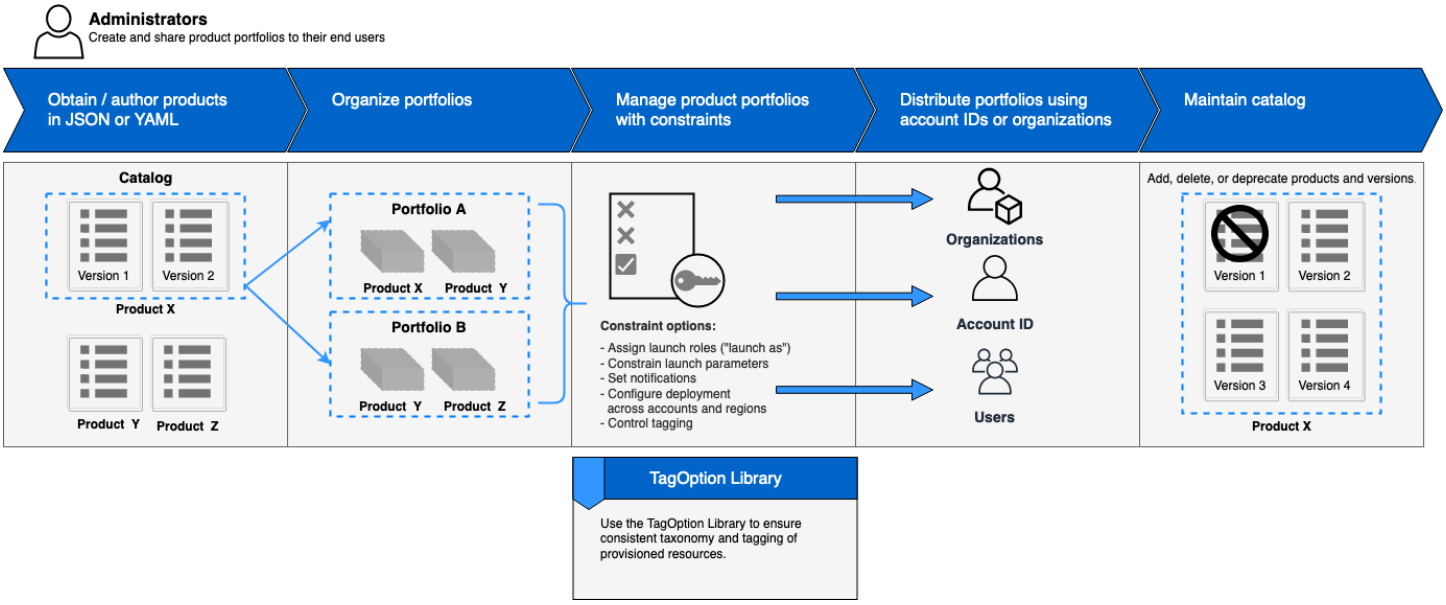
Dengan batasan peluncuran, Anda menentukan peran untuk produk di dalam portofolio. Gunakan peran ini untuk menyediakan sumber daya saat peluncuran, sehingga Anda dapat membatasi izin pengguna tanpa mempengaruhi kemampuan pengguna untuk menyediakan produk dari katalog.

Batasan notifikasi memungkinkan Anda mendapatkan notifikasi tentang peristiwa tumpukan menggunakan topik Amazon SNS.

Batasan templat membatasi parameter konfigurasi yang tersedia bagi pengguna saat meluncurkan produk (misalnya, tipe instans EC2 atau rentang alamat IP). Dengan batasan templat, Anda menggunakan kembali templat AWS CloudFormation umum untuk produk dan menerapkan batasan pada templat per produk atau per portofolio.

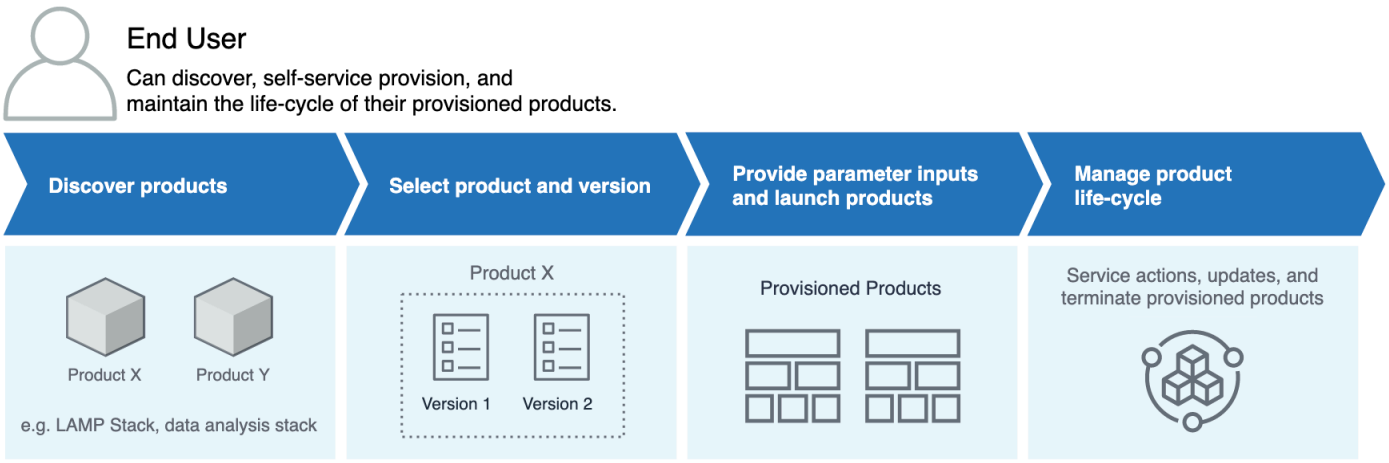
Alur Kerja Administrator Awal

Diagram ini menunjukkan alur kerja awal bagi administrator untuk membuat katalog.



Alur Kerja Pengguna Akhir Awal

Diagram ini menunjukkan alur kerja awal untuk pengguna akhir.



Service quotas default AWS Service Catalog

AWSAkun Anda memiliki kuota default berikut untukAWS Organizations, kendala, portofolio, produk, produk yang disediakan, regional, tindakan layanan, dan. TagOptions

Anda dapat menggunakan Service Quotas untuk mengelola kuota Anda atau meminta kenaikan kuota. Untuk informasi selengkapnya tentang Service Quotas, lihat Apa itu Service Quotas? dalam Panduan Pengguna Service Quotas. Untuk mempelajari cara meminta kenaikan kuota, lihat Meminta Kenaikan Kuota.

AWS Organizations

- Administrator yang didelegasikan AWS Service Catalog per organisasi: 50

Batasan kuota

- Batasan per produk per portofolio: 100

Kuota portofolio

- Pengguna, grup, dan peran per portofolio: 100
- Produk per portofolio: 150
- Tanda per portofolio: 20
- Akun bersama per portofolio: 5000

- Nilai tanda per kunci tanda: 25

Kuota produk

- Pengguna, grup, dan peran per produk: 200
- Versi produk per produk: 100
- Tanda per produk: 20
- Nilai tanda per kunci tanda: 25

Kuota produk yang disediakan

- Tanda per produk yang disediakan: 50

Kuota regional

- Portofolio: 100
- Produk: 350

Kuota tindakan layanan

- Tindakan layanan per wilayah: 200
- Asosiasi tindakan layanan per versi produk: 25

TagOptions kuota

- TagOptions per sumber daya: 25
- Nilai per TagOption: 25

Pengaturan AWS Service Catalog

Sebelum memulai AWS Service Catalog, selesaikan tugas berikut.

Topik

Mendaftar Akun AWS

Jika Anda tidak memiliki Akun AWS, selesaikan langkah-langkah berikut untuk membuatnya.

Untuk mendaftar Akun AWS

1. Buka https://portal.aws.amazon.com/billing/signup.
2. Ikuti petunjuk secara online.

   Anda akan diminta untuk menerima panggilan telepon dan memasukkan kode verifikasi pada keypad telepon sebagai bagian dari prosedur pendaftaran.

   Saat Anda mendaftar Akun AWS, Pengguna root akun AWS akan dibuat. Pengguna root memiliki akses ke semua Layanan AWS dan sumber daya dalam akun. Sebagai praktik terbaik keamanan, tetapkan akses administratif ke pengguna administratif, dan hanya gunakan pengguna root untuk melakukan tugas yang memerlukan akses pengguna root.

AWS akan mengirimkan email konfirmasi kepada Anda setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun saat ini dan mengelola akun dengan mengunjungi https://aws.amazon.com/ dan memilih Akun Saya.

Membuat pengguna administratif

Setelah mendaftar Akun AWS, amankan Pengguna root akun AWS, aktifkan AWS IAM Identity Center, dan buat sebuah pengguna administratif sehingga Anda tidak menggunakan pengguna root untuk tugas sehari-hari.

Mengamankan Pengguna root akun AWS Anda

1. Masuk ke AWS Management Console sebagai pemilik akun dengan memilih Pengguna root dan memasukkan alamat email Akun AWS Anda. Di halaman berikutnya, masukkan kata sandi Anda.

   Untuk bantuan masuk menggunakan pengguna root, lihat Masuk sebagai pengguna root dalam Panduan Pengguna AWS Sign-In.

2. Aktifkan autentikasi multi-faktor (MFA) untuk pengguna root Anda.

   Untuk petunjuknya, silakan lihat Mengaktifkan perangkat MFA virtual untuk pengguna root Akun AWS Anda (konsol) dalam Panduan Pengguna IAM.

Membuat pengguna administratif

1. Aktifkan Pusat Identitas IAM.

   Untuk mendapatkan petunjuk, silakan lihat Mengaktifkan AWS IAM Identity Center di Panduan Pengguna AWS IAM Identity Center.

2. Di Pusat Identitas IAM, berikan akses administratif ke sebuah pengguna administratif.

   Untuk mendapatkan tutorial tentang menggunakan Direktori Pusat Identitas IAM sebagai sumber identitas Anda, silakan lihat Mengonfigurasi akses pengguna dengan Direktori Pusat Identitas IAM default di Panduan Pengguna AWS IAM Identity Center.

Masuk sebagai pengguna administratif

- Untuk masuk dengan pengguna Pusat Identitas IAM, gunakan URL masuk yang dikirim ke alamat email Anda saat Anda membuat pengguna Pusat Identitas IAM.

  Untuk bantuan masuk menggunakan pengguna Pusat Identitas IAM, lihat Masuk ke portal akses AWS dalam Panduan Pengguna AWS Sign-In.

Untuk memberikan akses, tambahkan izin ke pengguna, grup, atau peran Anda:

- Pengguna dan grup di AWS IAM Identity Center:

  Buat rangkaian izin. Ikuti petunjuk dalam Buat set izin dalam Panduan Pengguna AWS IAM Identity Center.

- Pengguna yang dikelola di IAM melalui penyedia identitas:

  Buat peran untuk federasi identitas. Ikuti petunjuk dalam Membuat peran untuk penyedia identitas pihak ketiga (federasi) di Panduan Pengguna IAM.
- Pengguna IAM:
  - Buat peran yang dapat diambil pengguna Anda. Ikuti petunjuk dalam Membuat peran untuk pengguna IAM dalam Panduan Pengguna IAM.
  - (Tidak disarankan) Pasang kebijakan langsung ke pengguna atau tambahkan pengguna ke grup pengguna. Ikuti petunjuk di Menambahkan izin ke pengguna (konsol) dalam Panduan Pengguna IAM.

Berikan izin kepada administrator AWS Service Catalog

Sebagai administrator katalog, Anda memerlukan akses ke tampilan konsol administrator AWS Service Catalog dan izin IAM yang memungkinkan Anda untuk melakukan tugas-tugas seperti berikut:

- Membuat dan mengelola portofolio
- Membuat dan mengelola produk
- Menambahkan batasan templat untuk mengontrol opsi yang tersedia bagi pengguna akhir saat meluncurkan produk
- Menambahkan batasan peluncuran untuk menentukan IAM role yang diasumsikan oleh AWS Service Catalog ketika pengguna akhir meluncurkan produk
- Memberikan pengguna akhir akses ke produk Anda

Anda, atau administrator yang mengelola izin IAM Anda, harus melampirkan kebijakan untuk pengguna IAM, grup, atau IAM role yang diperlukan untuk menyelesaikan tutorial ini.

Memberikan izin kepada administrator katalog

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Manajemen akses, lalu pilih Pengguna. Jika Anda sudah membuat pengguna IAM yang ingin Anda gunakan sebagai administrator katalog, pilih nama pengguna, lalu pilih Tambahkan izin. Jika tidak, buat pengguna sebagai berikut:

   a. Pilih Tambahkan pengguna.

b. Untuk Nama pengguna, ketik **`ServiceCatalogAdmin`**.

c. Pilih Programmatic access (Akses terprogram) dan AWS Management Console access (akses).

d. Pilih Selanjutnya: Izin.

3. Pilih Lampirkan kebijakan yang sudah ada secara langsung.

4. Pilih Buat kebijakan, lalu lakukan hal berikut:

a. Pilih tab JSON.

b. Salin contoh kebijakan berikut, dan tempel di Dokumen Kebijakan:

```
{
    "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. Pilih Berikutnya: Tanda.

d. (Opsional) Pilih Tambahkan tag untuk mengaitkan pasangan kunci-nilai dengan sumber daya. Anda dapat menambahkan maksimal 50 tag.

> **Note**
>
> Tag adalah pasangan nilai kunci yang dapat Anda tambahkan ke sumber daya. Ini membantu mengidentifikasi, mengatur, dan mencari sumber daya. Untuk informasi selengkapnya, lihat Menandai AWS sumber daya di Panduan Referensi Umum AWS Referensi.

e. Pilih Berikutnya: Peninjauan.

f. Untuk Nama Kebijakan, ketik **`ServiceCatalogAdmin-AdditionalPermissions`**.

> **Important**
>
> Anda harus memberikan administrator izin Amazon S3 untuk mengakses template AWS Service Catalog yang disimpan di Amazon S3. Untuk informasi selengkapnya, lihat Contoh Kebijakan Pengguna di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

g. Pilih Buat Kebijakan.

5. Kembali ke jendela peramban dengan halaman izin dan pilih Segarkan.
6. Di bidang pencarian, ketik **`ServiceCatalog`** untuk memfilter daftar kebijakan.
7. Pilih kotak centang untuk **`ServiceCatalogAdmin-AdditionalPermissions`**kebijakan **`AWSServiceCatalogAdminFullAccess`**dan, lalu pilih Berikutnya: Tinjau.
8. Jika Anda memperbarui pengguna, pilih Tambahkan izin.

   Jika Anda membuat pengguna, pilih Buat pengguna. Anda dapat mengunduh atau menyalin kredensialnya lalu pilih Tutup.
9. Untuk masuk sebagai administrator katalog, gunakan URL khusus akun Anda. Untuk menemukan URL ini, pilih Dasbor di panel navigasi dan pilih Salin Tautan. Tempel tautan di peramban Anda, dan gunakan nama serta kata sandi dari pengguna IAM yang Anda buat atau perbarui dalam prosedur ini.

Berikan izin kepada pengguna AWS Service Catalog akhir

Sebelum pengguna akhir dapat menggunakan AWS Service Catalog, Anda harus memberikan akses ke tampilan konsol pengguna akhir AWS Service Catalog. Untuk memberikan akses, Anda melampirkan kebijakan ke pengguna IAM, grup, atau IAM role yang digunakan oleh pengguna akhir. Dalam prosedur berikut, kami melampirkan **`AWSServiceCatalogEndUserFullAccess`**kebijakan ke grup IAM.

Untuk memberikan izin kepada grup pengguna akhir

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Pada panel navigasi, pilih User groups (Grup pengguna).
3. Pilih Buat grup dan lakukan hal berikut:
    a. Untuk nama grup Pengguna, ketik**`Endusers`**.
    b. Di bidang pencarian, ketik **`AWSServiceCatalog`** untuk memfilter daftar kebijakan.
    c. Pilih kotak centang untuk **`AWSServiceCatalogEndUserFullAccess`**kebijakan tersebut. Anda juga memiliki opsi untuk memilih **`AWSServiceCatalogEndUserReadOnlyAccess`**sebagai gantinya.
    d. Pilih Buat group.
4. Di panel navigasi, pilih Pengguna.
5. Pilih Tambah pengguna dan lakukan hal berikut:
    a. Untuk Nama pengguna, ketik nama untuk pengguna.
    b. Pilih Kata Sandi - Akses Konsol AWS Manajemen.
    c. Pilih Selanjutnya: Izin.
    d. Pilih Tambahkan pengguna ke grup.
    e. Pilih kotak centang untuk grup Pengguna akhir dan pilih Selanjutnya: Tanda, lalu Selanjutnya: Tinjauan.
    f. Pada halaman Tinjauan, pilih Buat pengguna. Unduh atau salin kredensialnya, lalu pilih Tutup.

Instal dan konfigurasikan mesin penyediaan Terraform

Agar berhasil menggunakan produk TerraformAWS Service Catalog, Anda harus menginstal dan mengonfigurasi mesin penyediaan Terraform di akun yang sama tempat Anda akan mengelola produk Terraform. Untuk memulai, Anda dapat menggunakan mesin penyediaan Terraform yang disediakan olehAWS, yang menginstal dan mengonfigurasi kode dan infrastruktur yang diperlukan agar mesin penyediaan Terraform dapat digunakan. AWS Service Catalog Pengaturan satu kali ini memakan waktu sekitar 30 menit. AWS Service Catalogmenyediakan GitHub repositori dengan instruksi tentang menginstal dan mengonfigurasi mesin penyediaan Terraform.

Penentuan antrian

Saat Anda memanggil operasi penyediaan, AWS Service Catalog siapkan pesan payload untuk dikirim ke antrian yang relevan di mesin penyediaan. Dalam rangka membangun ARN untuk antrian, AWS Service Catalog membuat asumsi berikut:

- Mesin penyediaan terletak di akun pemilik produk
- Mesin penyediaan terletak di wilayah yang sama di mana panggilan dilakukan AWS Service Catalog
- Antrian mesin penyediaan mengikuti skema penamaan terdokumentasi yang dirinci di bawah ini

Misalnya, jika ProvisionProduct dipanggil `us-east-1` dari akun 1111111111 menggunakan produk yang dibuat oleh akun 0000000000000, asumsikan SQS ARN yang benar adalah. AWS Service Catalog `arn:aws:sqs:us-east-1:0000000000000:ServiceCatalogTerraformOSProvisionOperationQueue`

Logika yang sama berlaku untuk fungsi Lambda yang dipanggil oleh. `DescribeProvisioningParameters`

Menambahkan Deputi yang Bingung ke mesin penyediaan Terraform Anda

Kunci konteks Deputi yang bingung pada titik akhir untuk membatasi akses operasi **`lambda:Invoke`**

Fungsi Lambda parser parameter yang dibuat AWS Service Catalog oleh mesin -provided memiliki kebijakan akses yang memberikan izin `lambda:Invoke` lintas akun hanya kepada prinsipal layanan: 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"
    }
  ]
}
```

Ini harus menjadi satu-satunya izin yang diperlukan agar integrasi dengan berfungsi AWS Service Catalog dengan baik. Namun, Anda dapat membatasi ini lebih lanjut menggunakan kunci konteks [Deputi `aws:SourceAccount` Bingung](). Saat AWS Service Catalog mengirim pesan ke antrian ini, AWS Service Catalog isi kunci dengan ID akun penyediaan. Ini sangat membantu ketika Anda berniat untuk mendistribusikan produk melalui berbagi portofolio dan ingin memastikan bahwa hanya akun tertentu yang menggunakan mesin Anda.

Misalnya, Anda dapat membatasi mesin Anda untuk hanya mengizinkan permintaan yang berasal dari 000000000000 dan 111111111111 menggunakan kondisi yang ditunjukkan di bawah ini:

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

```
  ]
}
```

Kunci konteks Deputi yang bingung pada titik akhir untuk membatasi akses operasi **sqs:SendMessage**

Antrian operasi penyediaan Amazon SQS yang dibuat AWS Service Catalog oleh engine yang disediakan memiliki kebijakan akses yang memberikan izin `sqs:SendMessage` lintas akun (dan KMS terkait) hanya kepada prinsipal layanan: 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"
    }
  ]
}
```

Ini harus menjadi satu-satunya izin yang diperlukan agar integrasi dengan berfungsi AWS Service Catalog dengan baik. Namun, Anda dapat membatasi ini lebih lanjut menggunakan kunci konteks Deputi `aws:SourceAccount` Bingung. Saat AWS Service Catalog mengirim pesan ke antrian ini, AWS Service Catalog isi kunci dengan ID akun penyediaan. Ini sangat membantu ketika Anda berniat untuk mendistribusikan produk melalui berbagi portofolio dan ingin memastikan bahwa hanya akun tertentu yang menggunakan mesin Anda.

Misalnya, Anda dapat membatasi mesin Anda untuk hanya mengizinkan permintaan yang berasal dari 000000000000 dan 111111111111 menggunakan kondisi yang ditunjukkan di bawah ini:

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

Memulai

Anda dapat memulai AWS Service Catalog dengan menggunakan salah satu templat produk yang dirancang dengan baik di Perpustakaan Memulai atau dengan mengikuti langkah-langkah di salah satu tutorial memulai.

Dalam tutorial, Anda melakukan tugas sebagai administrator katalog dan pengguna akhir. Sebagai administrator katalog, Anda membuat portofolio dan kemudian produk. Sebagai pengguna akhir, Anda memverifikasi bahwa Anda dapat mengakses konsol pengguna akhir dan meluncurkan produk. Produk ini adalah salah satu dari yang berikut:

- Lingkungan pengembangan cloud yang berjalan di Amazon Linux dan didasarkan pada AWS CloudFormation template yang mendefinisikan AWS sumber daya yang dapat digunakan produk.
- Lingkungan open source yang berjalan pada mesin penyediaan Terraform dan didasarkan pada file konfigurasi tar.gz yang mendefinisikan AWS sumber daya yang dapat digunakan produk.

> **Note**
>
> Sebelum Anda mulai, pastikan bahwa Anda menyelesaikan item tindakan diPengaturan AWS Service Catalog.

Topik

Memulai Perpustakaan

AWS Service Catalog menyediakan Memulai Perpustakaan dari templat produk yang dirancang dengan baik sehingga Anda dapat memulai dengan cepat. Anda dapat menyalin salah satu produk dalam portofolio Memulai Perpustakaan kami ke akun Anda sendiri, lalu sesuaikan dengan kebutuhan Anda.

Topik

Prasyarat

Sebelum Anda menggunakan templat di Memulai Perpustakaan kami, pastikan Anda memiliki hal berikut:

- Izin yang diperlukan untuk menggunakan templat AWS CloudFormation. Untuk informasi selengkapnya, lihat Mengendalikan Akses dengan AWS Identity and Access Management.
- Izin administrator yang diperlukan untuk mengelola AWS Service Catalog. Untuk informasi selengkapnya, lihat the section called “Manajemen Identitas dan Akses”.

Pelajari Selengkapnya

Untuk informasi lebih lanjut tentang kerangka kerja yang dirancang dengan baik, lihat Well-Architected. AWS

Memulai dengan suatu AWS CloudFormation produk

Anda dapat memulai AWS Service Catalog dengan menggunakan salah satu template produk yang dirancang dengan baik di Perpustakaan Memulai atau dengan mengikuti langkah-langkah dalam tutorial memulai.

Dalam tutorial, Anda melakukan tugas sebagai administrator katalog dan pengguna akhir. Sebagai administrator katalog, Anda membuat porfolio dan kemudian produk. Sebagai pengguna akhir, Anda memverifikasi bahwa Anda dapat mengakses konsol pengguna akhir dan meluncurkan produk. Produk ini adalah lingkungan pengembangan cloud yang berjalan di Amazon Linux dan didasarkan pada AWS CloudFormation template yang mendefinisikan AWS sumber daya yang dapat digunakan produk.

> **Note**
>
> Sebelum Anda mulai, pastikan bahwa Anda menyelesaikan item tindakan diPengaturan AWS Service Catalog.

Topik

Langkah 1: Unduh AWS CloudFormation template

Anda dapat menggunakan AWS CloudFormation templat untuk mengonfigurasi dan menyediakan portofolio dan produk. Template ini adalah file teks yang dapat diformat dalam JSON atau YAMAL dan menjelaskan sumber daya yang ingin Anda sediakan. Untuk informasi selengkapnya, lihat Format templat dalam Panduan Pengguna AWS CloudFormation. Anda dapat menggunakan AWS CloudFormation editor atau editor teks pilihan Anda untuk membuat dan menyimpan templat. Dalam tutorial ini, kami menyediakan template sederhana, sehingga Anda dapat memulai. Template meluncurkan instance Linux tunggal yang dikonfigurasi untuk akses SSH.

> **Note**
>
> Menggunakan AWS CloudFormation template memerlukan izin khusus. Sebelum Anda mulai, pastikan Anda memiliki izin yang benar. Untuk informasi lebih lanjut, lihat prasyarat di. Memulai Perpustakaan

Unduhan templat

Contoh templat yang disediakan untuk tutorial ini, `development-environment.template`, tersedia di https://awsdocs.s3.amazonaws.com/servicecatalog/development-environment.template.

Gambaran Umum Templat

Teks dari templat sampel berikut:

```
{
```

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

Sumber Templat

Templat menyatakan sumber daya yang akan dibuat saat produk diluncurkan. Yang terdiri dari bagian-bagian berikut:

- AWSTemplateFormatVersion(opsional) - Versi Format AWS Template yang digunakan untuk membuat template ini. Versi format template terbaru adalah 2010-09-09 dan saat ini satu-satunya nilai yang valid.
- Deskripsi (opsional) — Deskripsi template.
- Parameter (opsional) — Parameter yang harus ditentukan pengguna Anda untuk meluncurkan produk. Untuk setiap parameter, templat menyertakan deskripsi dan batasan yang harus dipenuhi oleh nilai yang diketik. Untuk informasi lebih lanjut tentang batasan, lihat Menggunakan Batasan AWS Service Catalog.

  Parameter `KeyName` memungkinkan Anda menentukan nama pasangan kunci Amazon Elastic Compute Cloud (Amazon EC2) yang harus disediakan pengguna akhir ketika mereka menggunakan AWS Service Catalog untuk meluncurkan produk Anda. Anda akan membuat pasangan kunci pada langkah berikutnya.

- Metadata (opsional) — Objek yang memberikan informasi tambahan tentang template. Kunci AWS:CloudFormation: :Interface mendefinisikan bagaimana tampilan konsol pengguna akhir menampilkan parameter. Properti `ParameterGroups` menentukan metode pengelompokan parameter dan judul grup tersebut. Properti `ParameterLabels` menentukan nama parameter yang mudah diingat. Ketika pengguna menentukan parameter untuk meluncurkan produk yang berdasar pada templat ini, tampilan konsol pengguna akhir menampilkan parameter dengan label `Server size:` di judul `Instance configuration`, dan menampilkan parameter dengan label `Key pair:` dan `CIDR range:` di judul `Security configuration`.
- Pemetaan (opsional) - Pemetaan kunci dan nilai terkait yang dapat Anda gunakan untuk menentukan nilai parameter bersyarat, mirip dengan tabel pencarian. Anda dapat mencocokkan kunci ke nilai yang sesuai dengan menggunakan fungsi FindInMap intrinsik Fn:: di bagian Sumber Daya dan Output. Template di atas mencakup daftar AWS Wilayah dan Gambar Mesin Amazon (AMI) yang sesuai dengan masing-masing. AWS Service Catalogmenggunakan pemetaan ini untuk menentukan AMI mana yang akan digunakan berdasarkan AWS Wilayah yang dipilih pengguna di. AWS Management Console
- Sumber daya (wajib) - Tumpuk sumber daya dan propertinya. Anda dapat merujuk ke sumber daya di bagian Sumber Daya dan Keluaran dari template. Pada template di atas, kami menentukan instans EC2 yang menjalankan Amazon Linux dan grup keamanan yang memungkinkan akses SSH ke instance. Bagian Properties dari sumber daya instans EC2 menggunakan informasi yang diketik pengguna untuk mengonfigurasi jenis instans dan nama kunci untuk akses SSH.

  AWS CloudFormationmenggunakan AWS Region saat ini untuk memilih ID AMI dari pemetaan yang ditentukan sebelumnya dan menetapkan grup keamanan untuk itu. Grup keamanan dikonfigurasi untuk mengizinkan akses masuk pada port 22 dari rentang alamat IP CIDR yang ditentukan pengguna.
- Output (opsional) — Teks yang memberi tahu pengguna saat peluncuran produk selesai. Templat yang disediakan mendapatkan nama DNS publik dari instans yang diluncurkan dan menampilkannya kepada pengguna. Pengguna memerlukan nama DNS untuk terhubung ke instans menggunakan SSH.

  Untuk informasi selengkapnya tentang halaman anatomi Template, lihat Referensi template di Panduan AWS CloudFormation Pengguna.

Langkah 2: Buat key pair

Untuk memungkinkan pengguna akhir Anda meluncurkan produk yang didasarkan pada contoh templat untuk tutorial ini, Anda harus membuat pasangan kunci Amazon EC2. Pasangan kunci adalah kombinasi dari kunci publik yang digunakan untuk mengenkripsi data dan kunci privat yang digunakan untuk mendekripsi data. Untuk informasi selengkapnya tentang pasangan kunci, pastikan Anda masuk ke AWS konsol lalu tinjau Pasangan Kunci Amazon EC2 di Panduan Pengguna Amazon EC2 untuk Instans Linux.

Templat AWS CloudFormation untuk tutorial ini, `development-environment.template`, mencakup parameter `KeyName` berikut:

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

Pengguna akhir harus menentukan nama pasangan kunci ketika mereka menggunakan AWS Service Catalog untuk meluncurkan produk yang didasarkan pada templat.

Jika Anda sudah memiliki pasangan kunci di akun yang ingin Anda gunakan, Anda dapat langsung beralih ke Langkah 3: Buat portofolio. Jika tidak, selesaikan langkah-langkah berikut.

Untuk membuat pasangan kunci

1. Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2/.
2. Di panel navigasi, di Jaringan & Keamanan, pilih Pasangan Kunci.
3. Pada halaman Pasangan Kunci, pilih Buat Pasangan kunci.
4. Untuk Nama pasangan kunci, ketik nama yang mudah Anda ingat, lalu pilih Buat.
5. Saat konsol meminta Anda untuk menyimpan file kunci privat, simpan di tempat yang aman.

> **Important**
>
> Ini adalah satu-satunya kesempatan bagi Anda untuk menyelamatkan file kunci privat.

Langkah 3: Buat portofolio

Untuk menyediakan produk bagi pengguna, mulailah dengan membuat portofolio untuk produk tersebut.

Untuk membuat portofolio

1. Buka konsol Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Di panel navigasi kiri, pilih Portofolio, lalu pilih Buat portofolio.
3. Ketik nilai berikut:
   - Nama portofolio – **`Engineering Tools`**
   - Deskripsi portofolio - **`Sample portfolio that contains a single product.`**
   - Pemilik – **`IT (it@example.com)`**
4. Pilih Buat.

Langkah 4: Buat produk baru dalam portofolio

Setelah Anda membuat portofolio, Anda siap untuk membuat produk dalam portofolio. Untuk tutorial ini, Anda akan membuat produk yang disebut Linux Desktop, lingkungan pengembangan cloud yang berjalan di Amazon Linux, di dalam portofolio Engineering Tool.

Untuk membuat produk dalam portofolio

1. Jika Anda baru saja menyelesaikan langkah sebelumnya, halaman Portofolio telah ditampilkan. Jika tidak, buka https://console.aws.amazon.com/servicecatalog/.
2. Pilih dan buka portofolio Engineering Tool yang Anda buat di Langkah 2.
3. Pilih Unggah produk baru.
4. Pada halaman Buat produk di bagian Detail produk, masukkan yang berikut ini:
   - Nama Produk – **`Linux Desktop`**
   - Deskripsi Produk — **`Cloud development environment configured for engineering staff. Runs AWS Linux.`**
   - Pemilik – **`IT`**
   - Distributor – (kosong)

5. Pada halaman Detail versi, pilih Gunakan CloudFormation templat. Kemudian pilih Tentukan URL template Amazon S3 dan masukkan yang berikut ini:

   - Pilih templat – **`https://awsdocs.s3.amazonaws.com/servicecatalog/development-environment.template`**
   - Judul versi – **`v1.0`**
   - Deskripsi — **`Base Version`**

6. Di bagian Support details, masukkan yang berikut ini:

   - Kontak email – **`ITSupport@example.com`**
   - Tautan Support – **`https://wiki.example.com/IT/support`**
   - Deskripsi dukungan – **`Contact the IT department for issues deploying or connecting to this product.`**

7. Pilih Buat produk.

Langkah 5: Tambahkan batasan template untuk membatasi ukuran instance

Batasan menambahkan lapisan kontrol lain atas produk di tingkat portofolio. Batasan dapat mengontrol konteks peluncuran produk (batasan peluncuran), atau menambahkan aturan ke templat AWS CloudFormation (batasan templat). Untuk informasi selengkapnya, lihat Menggunakan Batasan AWS Service Catalog.

Tambahkan batasan template ke produk Desktop Linux yang mencegah pengguna memilih jenis instans besar pada waktu peluncuran. Templat pengembangan-lingkungan memungkinkan pengguna untuk memilih dari enam tipe instans; batasan ini membatasi tipe instans yang valid untuk dua tipe terkecil, `t2.micro` dan `t2.small`. Untuk informasi selengkapnya, lihat Instans T2 dalam Panduan Pengguna Amazon EC2 untuk Instans Linux.

Untuk menambahkan batasan templat ke produk Desktop Linux

1. Pada halaman Detail Portofolio, pilih Constraints, lalu pilih Create constraint.
2. Di halaman Create constraint, untuk Product, pilih Linux Desktop. Lalu, untuk Tipe batasan, pilih Templat.
3. Di bagian batasan emplate T, pilih Editor teks.
4. Tempelkan yang berikut ini ke editor teks:

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

5. Untuk deskripsi Constraint, masukkan. **`Small instance sizes`**
6. Pilih Buat.

Langkah 6: Tambahkan batasan peluncuran untuk menetapkan peran IAM

Kendala peluncuran menunjuk peran IAM yang AWS Service Catalog mengasumsikan ketika pengguna akhir meluncurkan produk.

Untuk langkah ini, Anda menambahkan batasan peluncuran ke produk Desktop Linux, sehingga AWS Service Catalog dapat menggunakan sumber daya IAM yang membentuk template produk. AWS CloudFormation

Peran IAM yang Anda tetapkan ke produk sebagai kendala peluncuran harus memiliki izin berikut

1. AWS CloudFormation
2. Layanan dalam templat AWS CloudFormation untuk produk
3. Baca akses ke AWS CloudFormation template dalam bucket Amazon S3 milik layanan.

Batasan peluncuran ini memungkinkan pengguna akhir untuk meluncurkan produk dan, setelah peluncuran, mengelolanya sebagai produk yang tersedia. Untuk informasi selengkapnya, lihat Batasan peluncuran AWS Service Catalog.

Tanpa kendala peluncuran, Anda perlu memberikan izin IAM tambahan kepada pengguna akhir Anda sebelum mereka dapat menggunakan produk Desktop Linux. Misalnya,

`ServiceCatalogEndUserAccess` kebijakan memberikan izin IAM minimum yang diperlukan untuk mengakses tampilan konsol pengguna AWS Service Catalog akhir.

Menggunakan batasan peluncuran memungkinkan Anda mengikuti praktik terbaik IAM untuk menjaga izin IAM pengguna akhir seminimal mungkin. Untuk informasi selengkapnya, lihat Pemberian hak istimewa terendah dalam Panduan Pengguna IAM.

Untuk menambahkan batasan peluncuran

1. Ikuti petunjuk untuk Membuat kebijakan baru di tab JSON di Panduan Pengguna IAM.
2. Rekatkan dokumen kebijakan JSON berikut:

   - `cloudformation`— Memungkinkan izin AWS Service Catalog penuh untuk membuat, membaca, memperbarui, menghapus, daftar, dan AWS CloudFormation tumpukan tag.
   - `ec2`— Memungkinkan izin AWS Service Catalog lengkap untuk mencantumkan, membaca, menulis, menyediakan, dan menandai sumber daya Amazon Elastic Compute Cloud (Amazon EC2) yang merupakan bagian dari produk. AWS Service Catalog Bergantung pada AWS sumber daya yang ingin Anda terapkan, izin ini mungkin berubah.
   - `ec2`— Membuat kebijakan terkelola baru untuk AWS akun Anda dan melampirkan kebijakan terkelola yang ditentukan ke peran IAM yang ditentukan.
   - `s3`— Memungkinkan akses ke ember Amazon S3 yang dimiliki oleh. AWS Service Catalog Untuk menyebarkan produk, AWS Service Catalog memerlukan akses ke artefak penyediaan.
   - `servicecatalog`— Memungkinkan AWS Service Catalog izin untuk membuat daftar, membaca, menulis, menandai, dan meluncurkan sumber daya atas nama pengguna akhir.
   - `sns`— Memungkinkan AWS Service Catalog izin untuk membuat daftar, membaca, menulis, dan menandai topik Amazon SNS untuk kendala peluncuran.

> **Note**
>
> Bergantung pada sumber daya dasar yang ingin Anda terapkan, Anda mungkin perlu memodifikasi contoh kebijakan 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. Pilih Berikutnya, Tag.
4. Pilih Berikutnya, Tinjau.
5. Di halaman Kebijakan tinjau, untuk Nama, masukkan**`linuxDesktopPolicy`**.
6. Pilih Buat kebijakan.
7. Di panel navigasi, silakan pilih Peran. Lalu pilih Buat peran dan lakukan hal berikut:

   a. Untuk Pilih entitas tepercaya, pilih AWSlayanan dan kemudian di bawah Kasus penggunaan untuk AWS layanan lain pilih Service Catalog. Pilih kasus penggunaan Service Catalog dan kemudian pilih Berikutnya.

   b. Cari linuxDesktopPolicykebijakan, lalu pilih kotak centang.

c. Pilih Berikutnya.

d. Untuk Nama Peran, ketik **`linuxDesktopLaunchRole`**.

e. Pilih Buat peran.

8. Buka konsol AWS Service Catalog di https://console.aws.amazon.com/servicecatalog.
9. Pilih portofolio Peralatan Teknik.
10. Pada halaman Detail portofolio, pilih tab Constraints, lalu pilih Create constraint.
11. Untuk Produk, Pilih Desktop Linux, dan untuk Tipe Batasan, pilih Luncurkan.
12. Pilih Pilih IAM role. Selanjutnya pilih linuxDesktopLaunchPeran, lalu pilih Buat.

Langkah 7: Berikan akses kepada pengguna akhir ke portofolio

Sekarang setelah Anda membuat portofolio dan menambahkan produk, Anda siap memberikan akses ke pengguna akhir.

Prasyarat

Jika Anda belum membuat grup IAM untuk pengguna akhir, lihat Berikan izin kepada pengguna AWS Service Catalog akhir.

Untuk menyediakan akses ke portofolio

1. Pada halaman detail portofolio, pilih tab Access.
2. Pilih Berikan akses.
3. Pada tab Grup, pilih kotak centang untuk grup IAM untuk pengguna akhir.
4. Pilih Tambahkan Akses.

Langkah 8: Uji pengalaman pengguna akhir

Untuk memverifikasi bahwa pengguna akhir dapat berhasil mengakses tampilan konsol pengguna akhir dan meluncurkan produk Anda, masuk ke AWS sebagai pengguna akhir dan lakukan tugas-tugas tersebut.

Untuk memverifikasi bahwa pengguna akhir dapat mengakses konsol pengguna akhir

1. Ikuti petunjuk untuk Masuk sebagai pengguna IAM di panduan Pengguna IAM.

2. Di bilah menu, pilih Wilayah AWS tempat Anda membuat portofolio `Engineering Tools`. Untuk tutorial ini, pilih wilayah us-east-1.
3. Buka AWS Service Catalog konsol di https://console.aws.amazon.com/servicecatalog/ untuk melihat:

   - Produk – Produk yang dapat digunakan oleh pengguna.
   - Produk yang tersedia – Produk yang tersedia yang telah diluncurkan oleh pengguna.

Untuk memverifikasi bahwa pengguna akhir dapat meluncurkan produk Desktop Linux

Perhatikan bahwa untuk tutorial ini, pilih wilayah us-east-1.

1. Di bagian konsol Produk, pilih Desktop Linux.
2. Pilih Luncurkan produk untuk memulai wizard yang mengonfigurasi produk Anda.
3. Pada halaman Peluncuran: Desktop Linux, masukkan **`Linux-Desktop`** untuk nama produk yang tersedia.
4. Pada halaman Parameter, masukkan hal berikut dan pilih Selanjutnya:

   - Ukuran server – Pilih **`t2.micro`**.
   - Pasangan kunci – Pilih pasangan kunci yang Anda buat di Langkah 2: Buat key pair.
   - Rentang CIDR – Masukkan rentang CIDR yang valid untuk alamat IP agar terhubung ke instans. Anda dapat menggunakan nilai default (0.0.0.0/0) untuk mengizinkan akses dari alamat IP, lalu alamat IP Anda, diikuti oleh **`/32`** guna membatasi akses hanya ke alamat IP Anda, atau sesuatu di antaranya.
5. Pilih Luncurkan produk untuk meluncurkan tumpukan. Konsol menampilkan halaman detail tumpukan untuk tumpukan Linux-Desktop. Status awal produk sedang berubah. Perlu beberapa menit bagi AWS Service Catalog untuk meluncurkan produk. Untuk melihat status saat ini, segarkan peramban Anda. Setelah produk diluncurkan, statusnya adalah Tersedia.

Memulai dengan produk Terraform

AWS Service Catalogmemungkinkan penyediaan layanan mandiri yang cepat dengan tata kelola untuk konfigurasi Terraform Anda HashiCorp di dalamnya. AWS Anda dapat menggunakan AWS Service Catalog sebagai alat tunggal untuk mengatur, mengatur, dan mendistribusikan konfigurasi Terraform Anda dalam skala besar. AWS AWS Service Catalogmendukung Terraform di beberapa fitur utama, termasuk membuat katalog templat Terraform standar dan disetujui sebelumnya, kontrol

akses, pembuatan versi, penandaan, dan berbagi ke akun lain. AWS DiAWS Service Catalog, pengguna akhir Anda melihat daftar sederhana produk dan versi yang dapat mereka akses, dan kemudian dapat menyebarkan produk tersebut dalam satu tindakan.

> **Note**
>
> Untuk melanjutkan dukungan HashiCorp teknologi, sebagai akibat dari perubahan lisensi baru-baru ini ke Terraform, AWS Service Catalog mengubah referensi Terraform Open Source sebelumnya menjadi Eksternal. Jenis produk Eksternal mencakup dukungan untuk Terraform Community Edition, yang sebelumnya dikenal sebagai Terraform Open Source. Untuk informasi dan petunjuk selengkapnya tentang memigrasi produk Terraform Open Source Anda yang ada dan produk yang disediakan ke jenis produk Eksternal, tinjau. Memperbarui produk Terraform Open Source yang ada dan produk yang disediakan ke jenis produk Eksternal

Langkah-langkah dalam tutorial berikut akan membantu Anda memulai dengan produk Terraform di. AWS Service Catalog

Sebagai administrator katalog, Anda bekerja di akun administrator pusat (akun hub). Baik produk Terrafrm Community Edition dan Terraform Cloud memerlukan mesin penyediaan Terraform, yang dapat Anda pelajari lebih lanjut di dan. Mesin penyediaan untuk Terraform Community Edition (Jenis produk eksternal) Mesin penyediaan untuk Terraform Cloud

Selama tutorial, Anda melakukan tugas-tugas berikut di akun administrator:

- Buat produk Terraform menggunakan jenis produk Terraform Cloud atau Eksternal. Service Catalog menggunakan jenis produk Eksternal untuk mendukung produk Terraform Community Edition.
- Kaitkan produk dengan portofolio
- Buat batasan peluncuran untuk memungkinkan pengguna akhir Anda menyediakan produk
- Tandai produk
- Bagikan portofolio dan produk Terraform dengan akun pengguna akhir (akun spoke)

Dalam tutorial, Anda berbagi portofolio menggunakan opsi berbagi organisasi dari akun hub admin, yang juga merupakan akun manajemen Organisasi. Untuk informasi selengkapnya tentang berbagi organisasi, lihatMembagi Portofolio.

AWSSumber daya yang terkandung dalam produk Terraform yang Anda buat dalam tutorial adalah bucket Amazon S3 sederhana.

> **Note**
>
> Sebelum Anda mulai, pastikan bahwa Anda menyelesaikan item tindakan diPengaturan AWS Service Catalog.

Topik

Memperbarui produk Terraform Open Source yang ada dan produk yang disediakan ke jenis produk Eksternal

Untuk melanjutkan dukungan HashiCorp teknologi, sebagai akibat dari perubahan lisensi baru-baru ini ke Terraform, AWS Service Catalog mengubah referensi Terraform Open Source sebelumnya menjadi Eksternal. Jenis produk Eksternal mencakup dukungan untuk Terraform Community Edition, yang sebelumnya dikenal sebagai Terraform Open Source. AWS Service Catalogtidak lagi mendukung Terraform Open Source sebagai jenis produk yang valid untuk produk baru atau produk yang disediakan. Anda hanya dapat memperbarui atau menghentikan sumber daya Sumber Terbuka Terraform yang ada, termasuk versi produk dan produk yang disediakan.

Jika Anda belum melakukannya, Anda harus mentransisikan semua produk Terraform Open Source yang ada dan produk yang disediakan ke produk Eksternal, dengan mengikuti petunjuk di bagian ini.

1. Perbarui Mesin Referensi Terraform Anda yang ada AWS Service Catalog untuk menyertakan dukungan untuk jenis produk Sumber Terbuka Eksternal dan Terraform. Untuk petunjuk tentang memperbarui Mesin Referensi Terraform Anda, tinjau Repositori kamiGitHub .
2. Buat ulang produk Terraform Open Source yang ada menggunakan jenis produk Eksternal yang baru.
3. Hapus semua produk yang ada yang menggunakan jenis produk Terraform Open Source.
4. Menyediakan kembali sumber daya yang tersisa untuk menggunakan jenis produk Eksternal yang baru.
5. Hentikan semua produk yang disediakan yang menggunakan jenis produk Terraform Open Source.

Setelah mentransisikan produk yang sudah ada, gunakan jenis produk Eksternal untuk setiap produk baru yang menggunakan file konfigurasi tar.gz.

AWS Service Catalogakan mendukung pelanggan melalui perubahan ini sesuai kebutuhan. Jika perubahan ini memerlukan upaya ekstensif untuk akun Anda, atau memengaruhi beban kerja produk penting, hubungi perwakilan akun Anda untuk meminta bantuan.

Prasyarat: Konfigurasikan mesin penyediaan Terraform Anda

Sebagai prasyarat untuk membuat produk Terraform diAWS Service Catalog, Anda harus menginstal dan mengonfigurasi mesin penyediaan di akun administrator Service Catalog (akun hub) Anda. Mesin penyediaan diperlukan untuk produk Terraform Community Edition (menggunakan jenis produk Eksternal) dan produk Terraform Cloud (menggunakan jenis produk Terraform Cloud).

> **Note**
>
> Konfigurasi mesin adalah pengaturan satu kali yang memakan waktu sekitar 30 menit.

Mesin penyediaan untuk Terraform Community Edition (Jenis produk eksternal)

AWS Service Catalogmenggunakan jenis produk Eksternal untuk mendukung produk Terraform Community Edition. Jenis produk Eksternal juga mendukung alat penyediaan lainnya, termasuk Pulumi, Ansible, Chef, dan lainnya berdasarkan konfigurasi mesin penyediaan.

Untuk AWS Service Catalog produk yang menggunakan jenis produk Eksternal dengan Edisi Komunitas HashiCorp Terraform, Anda harus menginstal dan mengonfigurasi mesin penyediaan Terraform di akun AWS Service Catalog administrator Anda (akun hub). AWSmengelola mesin ini dan sumber dayanya.

AWS Service Catalogmenyediakan GitHub repositori dengan instruksi tentang menginstal dan mengonfigurasi mesin penyediaan Terraform AWS yang disediakan. Repo mencakup informasi berikut:

- Alat instalasi yang dibutuhkan
- Membangun kode
- Menyebarkan ke akun AWS
- Informasi tambahan tentang penyediaan alur kerja, jaminan kualitas, dan batasan

Mesin penyediaan untuk Terraform Cloud

Untuk AWS Service Catalog produk yang menggunakan jenis produk Terraform Cloud dengan HashiCorp Terraform Cloud, Anda harus menginstal dan mengonfigurasi mesin penyediaan Terraform di akun administrator Anda (akun hub). AWS Service Catalog HashiCorp mengelola mesin ini di lingkungan terpencil.

HashiCorp menyediakan GitHub repositori dengan instruksi tentang mengonfigurasi mesin Terraform Cloud untuk. AWS Service Catalog Repo mencakup informasi berikut:

- Alat instalasi yang dibutuhkan
- Membangun kode
- Menyebarkan ke akun AWS
- Informasi tambahan tentang penyediaan alur kerja, jaminan kualitas, dan batasan

Langkah 1: Unduhan file konfigurasi Terraform

Anda dapat menggunakan file konfigurasi Terraform untuk membuat dan menyediakan produk HashiCorp Terraform. Konfigurasi ini adalah file teks biasa dan menjelaskan sumber daya yang ingin Anda sediakan. Anda dapat menggunakan editor teks pilihan Anda untuk membuat, memperbarui, dan menyimpan konfigurasi. Untuk pembuatan produk, Anda harus mengunggah konfigurasi Terraform sebagai file tar.gz. Dalam tutorial ini, AWS Service Catalog menyediakan file konfigurasi sederhana sehingga Anda dapat memulai. Konfigurasi membuat bucket Amazon S3.

Unduhan file konfigurasi

AWS Service Catalogmenyediakan contoh file simple-s3-bucket.tar.gzkonfigurasi untuk Anda gunakan dalam tutorial ini.

Ikhtisar file konfigurasi

Teks file konfigurasi sampel berikut:

```
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
}
```

Sumber Daya Konfigurasi

File konfigurasi mendeklarasikan sumber daya yang akan dibuat saat AWS Service Catalog menyediakan produk. Yang terdiri dari bagian-bagian berikut:

- Variabel (opsional) - Definisi nilai yang dapat ditetapkan oleh pengguna administrator (administrator akun hub) untuk menyesuaikan konfigurasi. Variabel menyediakan antarmuka yang konsisten untuk mengubah bagaimana konfigurasi tertentu berperilaku. Label setelah kata kunci variabel adalah nama untuk variabel, yang harus unik di antara semua variabel dalam modul yang sama. Nama ini digunakan untuk menetapkan nilai luar untuk variabel, dan untuk referensi nilai variabel dari dalam modul.
- Penyedia (opsional) — Penyedia layanan cloud untuk penyediaan sumber daya, yaitu. AWS AWS Service Cataloghanya mendukung AWS sebagai penyedia. Akibatnya, mesin penyediaan Terraform mengesampingkan penyedia lain yang terdaftar ke. AWS
- Sumber daya (wajib) — Sumber daya AWS infrastruktur untuk penyediaan. Untuk tutorial ini, file konfigurasi Terraform menentukan Amazon S3.

- Output (opsional) — Informasi atau nilai yang dikembalikan, mirip dengan nilai yang dikembalikan dalam bahasa pemrograman. Anda dapat menggunakan data output untuk mengonfigurasi alur kerja infrastruktur dengan alat otomatisasi.

Langkah 2: Buat produk Terraform

Setelah menginstal mesin penyediaan Terraform, Anda siap membuat produk Terraform di. HashiCorp AWS Service Catalog Dalam tutorial ini, Anda membuat produk Terraform yang berisi bucket Amazon S3 sederhana.

Untuk membuat produk Terraform

1. Buka AWS Service Catalog konsol di https://console.aws.amazon.com/servicecatalog/ dan masuk sebagai pengguna admin.
2. Arahkan ke bagian Administrasi, lalu pilih Daftar produk.
3. Pilih Buat produk.
4. Pada halaman Buat produk di bagian Detail produk, pilih jenis produk Eksternal atau Terraform Cloud. Service Catalog menggunakan jenis produk Eksternal untuk mendukung produk Terraform Community Edition.
5. Masukkan detail produk berikut:
   - Nama Produk – **`Simple S3 bucket`**
   - Deskripsi Produk — Produk Terraform yang berisi ember Amazon S3.
   - Pemilik – **`IT`**
   - Distributor – (kosong)
6. Pada panel Detail versi, pilih unggah file templat lalu pilih Pilih file. Pilih file yang Anda unduhLangkah 1: Unduhan file konfigurasi Terraform.
7. Masukkan yang berikut ini:
   - Nama versi - **`v1.0`**
   - Deskripsi versi - **`Base Version`**
8. Di bagian Support details, masukkan yang berikut ini lalu pilih Create product.
   - Kontak email – **`ITSupport@example.com`**
   - Tautan Support – **`https://wiki.example.com/IT/support`**

- Deskripsi dukungan – **`Contact the IT department for issues deploying or connecting to this product.`**

9. Pilih Buat produk.

Setelah berhasil membuat produk, AWS Service Catalog menampilkan spanduk konfirmasi di halaman produk.

Langkah 3: Buat AWS Service Catalog portofolio

Anda dapat membuat portofolio di akun AWS Service Catalog administrator Anda (akun hub) untuk memudahkan pengorganisasian produk dan distribusi ke akun pengguna akhir (akun spoke).

Untuk membuat portofolio

1. Buka AWS Service Catalog konsol di https://console.aws.amazon.com/servicecatalog/ dan masuk sebagai administrator.
2. Di panel navigasi kiri, pilih Portofolio, lalu pilih Buat portofolio.
3. Masukkan nilai berikut:
   - Nama portofolio – **`S3 bucket`**
   - Deskripsi portofolio - **`Sample portfolio for Terraform configurations.`**
   - Pemilik – **`IT (it@example.com)`**
4. Pilih Buat.

Langkah 4: Tambahkan produk ke portofolio

Setelah membuat portofolio, Anda dapat menambahkan produk HashiCorp Terraform yang Anda buat di Langkah 2.

Untuk menambahkan produk ke portofolio

1. Arahkan ke halaman daftar Produk.
2. Pilih produk Terraform bucket S3 Sederhana yang Anda buat di Langkah 2, lalu pilih Tindakan. Dari menu tarik-turun, pilih Tambahkan produk ke portofolio. AWS Service Catalogmenampilkan bucket Add Simple S3 ke panel portofolio.

3. Pilih portofolio bucket S3, lalu matikan Create launch constraint. Anda akan membuat kendala peluncuran nanti di tutorial.
4. Pilih Tambahkan produk ke portofolio.

Setelah berhasil menambahkan produk ke portofolio, AWS Service Catalog menampilkan banner konfirmasi pada halaman daftar Produk.

Langkah 5: Buat peran peluncuran

Pada langkah ini, Anda akan membuat peran IAM (peran peluncuran) yang menentukan izin yang AWS Service Catalog dapat diasumsikan oleh mesin penyediaan Terraform saat pengguna akhir meluncurkan produk Terraform. HashiCorp

Peran IAM (peran peluncuran) yang kemudian Anda tetapkan ke produk Terraform bucket Amazon S3 sederhana Anda sebagai batasan peluncuran harus memiliki izin berikut:

- Akses ke AWS sumber daya yang mendasari produk Terraform Anda. Dalam tutorial ini, ini termasuk akses ke operasi`s3:CreateBucket*`,`s3:DeleteBucket*`,`s3:Get*`,`s3:List*`, dan `s3:PutBucketTagging` Amazon S3.
- Baca akses ke template Amazon S3 dalam bucket Amazon AWS Service Catalog S3 milik
- Akses ke`CreateGroup`,, `ListGroupResourcesDeleteGroup`, dan operasi kelompok `Tag` sumber daya. Operasi ini memungkinkan AWS Service Catalog untuk mengelola kelompok sumber daya dan tag

Untuk membuat peran peluncuran di akun AWS Service Catalog administrator

1. Saat masuk ke akun AWS Service Catalog administrator, ikuti petunjuk untuk Membuat kebijakan baru di tab JSON di Panduan Pengguna IAM.
2. Buat kebijakan untuk produk Terraform bucket Amazon S3 sederhana Anda. Kebijakan ini harus dibuat sebelum Anda membuat peran peluncuran, dan terdiri dari izin berikut:

    - `s3`— Memungkinkan izin AWS Service Catalog penuh untuk mendaftar, membaca, menulis, menyediakan, dan menandai produk Amazon S3.
    - `s3`— Memungkinkan akses ke ember Amazon S3 yang dimiliki oleh. AWS Service Catalog Untuk menyebarkan produk, AWS Service Catalog memerlukan akses ke artefak penyediaan.
    - `resourcegroups`— Memungkinkan AWS Service Catalog untuk membuat, daftar, menghapus, dan menandaiAWS Resource Groups.

- `tag`— Memungkinkan izin AWS Service Catalog penandaan.

> **Note**
>
> Bergantung pada sumber daya dasar yang ingin Anda terapkan, Anda mungkin perlu mengubah contoh kebijakan JSON.

Rekatkan dokumen kebijakan JSON berikut:

```
{
    "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. Pilih Berikutnya, Tag.

   b. Pilih Berikutnya, Tinjau.

   c. Di halaman Kebijakan ulasan, untuk Nama, masukkan**`S3ResourceCreationAndArtifactAccessPolicy`**.

   d. Pilih Buat kebijakan.

4. Di panel navigasi, pilih Peran, lalu pilih Buat peran.

5. Untuk Pilih entitas tepercaya, pilih Kebijakan kepercayaan khusus, lalu masukkan kebijakan JSON berikut:

```
{
    "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. Pilih Berikutnya.
7. Dalam daftar Kebijakan, pilih yang baru saja `S3ResourceCreationAndArtifactAccessPolicy` Anda buat.
8. Pilih Berikutnya.
9. Untuk Nama peran, masukkan **`SCLaunch-S3product`**.

> **Important**
>
> Nama peran peluncuran harus dimulai dengan “SCLaunch” diikuti dengan nama peran yang diinginkan.

10. Pilih Buat peran.

> **Important**
>
> Setelah membuat peran peluncuran di akun AWS Service Catalog administrator Anda, Anda juga harus membuat peran peluncuran yang identik di akun pengguna AWS Service Catalog akhir. Peran di akun pengguna akhir harus memiliki nama yang sama dan menyertakan kebijakan yang sama dengan peran di akun administrator.

Untuk membuat peran peluncuran di akun pengguna AWS Service Catalog akhir

1. Masuk sebagai administrator ke akun pengguna akhir, lalu ikuti petunjuk untuk Membuat kebijakan baru di tab JSON di panduan Pengguna IAM.
2. Ulangi langkah 2-10 dari Untuk membuat peran peluncuran di akun AWS Service Catalog administrator di atas.

> **Note**
>
> Saat membuat peran peluncuran di akun pengguna AWS Service Catalog akhir, pastikan Anda menggunakan administrator yang sama **`AccountId`** dalam kebijakan kepercayaan khusus.

Sekarang setelah Anda membuat peran peluncuran di akun administrator dan pengguna akhir, Anda dapat menambahkan batasan peluncuran ke produk.

Langkah 6: Tambahkan batasan Peluncuran ke produk Terraform Anda

> **Important**
>
> Anda harus membuat batasan peluncuran untuk produk HashiCorp Terraform. Tanpa kendala peluncuran, pengguna akhir tidak dapat menyediakan produk.

Setelah membuat peran peluncuran di akun administrator Anda, Anda siap untuk mengaitkan peran peluncuran ke batasan peluncuran pada produk External atau Terraform Cloud Anda.

Batasan peluncuran ini memungkinkan pengguna akhir untuk meluncurkan produk dan, setelah peluncuran, mengelolanya sebagai produk yang tersedia. Untuk informasi selengkapnya, lihat Batasan peluncuran AWS Service Catalog.

Menggunakan batasan peluncuran memungkinkan Anda mengikuti praktik terbaik IAM untuk menjaga izin IAM pengguna akhir seminimal mungkin. Untuk informasi selengkapnya, lihat Pemberian hak istimewa terendah dalam Panduan Pengguna IAM.

Untuk menetapkan kendala peluncuran ke produk

1. Buka konsol AWS Service Catalog di https://console.aws.amazon.com/servicecatalog.

2. Di konsol navigasi kiri, pilih Portofolio.
3. Pilih portofolio bucket S3.
4. Pada halaman Detail portofolio, pilih tab Constraints, lalu pilih Create constraint.
5. Untuk Produk, pilih bucket S3 Simple. AWS Service Catalogsecara otomatis memilih jenis kendala Luncurkan.
6. Pilih Masukkan nama peran, lalu pilih Sclaunch-S3Product.
7. Pilih Buat.

> **Note**
>
> Nama peran yang diberikan harus muncul di akun yang menciptakan batasan peluncurannya dan di akun pengguna yang meluncurkan produk dengan batasan peluncuran ini.

Langkah 7: Berikan akses pengguna akhir

Setelah menerapkan batasan peluncuran ke produk HashiCorp Terraform Anda, Anda siap memberikan akses ke pengguna akhir di akun spoke.

Dalam tutorial ini, Anda memberikan akses ke pengguna akhir menggunakan berbagi Nama Utama. Nama Utama adalah nama untuk grup, peran, dan pengguna yang dapat ditentukan oleh administrator dalam portofolio, dan kemudian dibagikan dengan portofolio. Saat Anda membagikan portofolio, AWS Service Catalog verifikasi apakah Nama Utama tersebut sudah ada. Jika memang ada, AWS Service Catalog secara otomatis mengaitkan prinsip IAM yang cocok dengan portofolio bersama untuk memberikan akses ke pengguna akhir. Tinjau Berbagi Portofolio untuk informasi lebih lanjut.

Prasyarat

Jika Anda belum membuat grup IAM untuk pengguna akhir, lihatBerikan izin kepada pengguna AWS Service Catalog akhir.

Untuk menyediakan akses ke portofolio

1. Arahkan ke halaman Portofolio dan pilih portofolio bucket S3.
2. Pilih tab Access, lalu pilih Grant access.
3. Di panel Jenis akses, pilih Nama utama.

4. Di panel Nama utama, pilih Jenis nama utama, lalu masukkan Nama utama pengguna akhir yang diinginkan di akun spoke.
5. Pilih Berikan akses.

Langkah 8: Bagikan portofolio dengan pengguna akhir

AWS Service CatalogAdministrator dapat mendistribusikan portofolio dengan akun pengguna akhir menggunakan account-to-account berbagi atau AWS Organizations berbagi. Dalam tutorial ini, Anda berbagi portofolio Anda dengan organisasi dari akun administrator (akun hub), yang juga merupakan akun manajemen Organisasi.

Untuk berbagi portofolio dari akun admin hub

1. Buka konsol AWS Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Pada halaman Portofolio, pilih portofolio bucket S3. Di menu Tindakan, pilih Bagikan.
3. Pilih AWS Organizations, dan kemudian filter ke dalam struktur organisasi Anda.
4. Di panel AWSOrganisasi, pilih akun pengguna akhir (akun bicara).

   Anda juga dapat memilih node Root untuk berbagi portofolio dengan seluruh organisasi, Unit Organisasi induk (OU), atau OU anak dalam organisasi Anda berdasarkan struktur organisasi Anda. Untuk informasi lebih lanjut, tinjauMembagi Portofolio.
5. Di panel Setelan Bagikan, pilih Berbagi utama.
6. Pilih Bagikan.

Setelah berhasil membagikan portofolio dengan pengguna akhir, langkah selanjutnya adalah memverifikasi pengalaman pengguna akhir dan menyediakan produk Terraform.

Langkah 9: Uji pengalaman pengguna akhir

Untuk memverifikasi pengguna akhir berhasil mengakses tampilan konsol pengguna akhir dan meluncurkan **`Simple S3 bucket`** produk Anda, masuk AWS sebagai pengguna akhir dan lakukan tugas di bawah ini.

Untuk memverifikasi bahwa pengguna akhir dapat mengakses konsol pengguna akhir

- Buka AWS Service Catalog konsol di https://console.aws.amazon.com/servicecatalog/ untuk melihat:

- Produk – Produk yang dapat digunakan oleh pengguna.
- Produk yang tersedia – Produk yang tersedia yang telah diluncurkan oleh pengguna.

Untuk memverifikasi pengguna akhir dapat meluncurkan produk Terraform

1. Di bagian Produk konsol, pilih bucket S3 sederhana.
2. Pilih Luncurkan produk untuk memulai wizard yang mengonfigurasi produk Anda.
3. Pada halaman bucket Launch Simple S3, masukkan nama **`Amazon S3 product`** produk yang disediakan.
4. Pada halaman Parameter, masukkan hal berikut dan pilih Selanjutnya:
   - bucket_name - Berikan nama unik untuk bucket Amazon S3. Misalnya, **`terraform-s3-product`**.
5. Pilih Luncurkan produk. Konsol menampilkan halaman detail tumpukan untuk peluncuran produk Amazon S3. Status awal produk adalah Di bawah perubahan. Perlu beberapa menit bagi AWS Service Catalog untuk meluncurkan produk. Untuk melihat status saat ini, segarkan peramban Anda. Setelah peluncuran produk yang sukses, statusnya Tersedia.

   AWS Service Catalogmembuat bucket Amazon S3 baru bernama. **`terraform-s3-product`**

Langkah 10: Memantau operasi penyediaan Terraform

Jika ingin memantau operasi penyediaan, Anda dapat meninjau CloudWatch log Amazon dan alur kerja AWS Step Functions penyediaan apa pun.

Ada dua mesin status untuk alur kerja penyediaan:

- `ManageProvisionedProductStateMachine`— AWS Service Catalog memanggil mesin status ini saat menyediakan produk Terraform baru dan saat memperbarui produk yang disediakan Terraform yang ada.
- `TerminateProvisionedProductStateMachine`— AWS Service Catalog memanggil mesin status ini saat menghentikan produk yang disediakan Terraform yang ada.

Untuk menjalankan mesin negara pemantauan

1. Buka konsol AWS manajemen dan masuk sebagai administrator di akun hub admin tempat mesin penyediaan Terraform diinstal.
2. Buka AWS Step Functions.
3. Di panel navigasi kiri, pilih mesin State.
4. Pilih ManageProvisionedProductStateMachine.
5. Dalam daftar Eksekusi, masukkan ID produk yang disediakan untuk menemukan eksekusi Anda.

> **Note**
>
> AWS Service Catalogmembuat ID produk yang disediakan saat Anda menyediakan produk. ID produk yang disediakan diformat sebagai berikut:. **`pp-1111pwtn[ID number]`**

6. Pilih ID eksekusi.

Pada halaman Detail eksekusi yang dihasilkan, Anda dapat melihat semua langkah dalam alur kerja penyediaan. Anda juga dapat meninjau langkah-langkah yang gagal untuk mengidentifikasi penyebab kegagalan.

Keamanan di AWS Service Catalog

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. Model tanggung jawab bersama menjelaskan hal ini sebagai keamanan dari cloud dan keamanan di cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi keefektifan keamanan kami sebagai bagian dari program kepatuhan AWS.

  Untuk mempelajari tentang program kepatuhan yang berlaku AWS Service Catalog, lihat AWS Layanan dalam Lingkup berdasarkan Program Kepatuhan
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

Dokumentasi ini membantu Anda memahami cara menerapkan model tanggung jawab bersama saat menggunakan AWS Service Catalog. Topik berikut menunjukkan cara mengonfigurasi AWS Service Catalog untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga akan diperkenalkan ke AWS layanan lain yang membantu Anda memantau dan mengamankan AWS Service Catalog sumber daya Anda.

Topik

Perlindungan Data di AWS Service Catalog

Model tanggung jawab AWS bersama model berlaku untuk perlindungan data di AWS Service Catalog. Seperti yang dijelaskan dalam model AWS ini, bertanggung jawab untuk melindungi infrastruktur global yang menjalankan semua AWS Cloud. Anda bertanggung jawab untuk mempertahankan kendali atas konten yang di-host pada infrastruktur ini. Anda juga bertanggung jawab atas tugas-tugas konfigurasi dan manajemen keamanan untuk Layanan AWS yang Anda gunakan. Lihat informasi yang lebih lengkap tentang privasi data dalam Pertanyaan Umum Privasi Data. Lihat informasi tentang perlindungan data di Eropa di pos blog Model Tanggung Jawab Bersama dan GDPR AWS di Blog Keamanan AWS .

Untuk tujuan perlindungan data, kami menyarankan Anda melindungi Akun AWS kredensyal dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di Standar Pemrosesan Informasi Federal (FIPS) 140-2.

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti bidang Nama. Ini termasuk saat Anda bekerja dengan AWS Service Catalog atau lainnya Layanan AWS menggunakan konsol, API AWS CLI, atau AWS SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat

menganjurkan supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Melindungi Data dengan Enkripsi

Enkripsi diam

AWS Service Catalog menggunakan bucket Amazon S3 dan database Amazon DynamoDB yang dienkripsi saat istirahat menggunakan kunci yang dikelola Amazon. Untuk mempelajari selengkapnya, lihat informasi tentang enkripsi saat tidak aktif yang disediakan oleh Amazon S3 dan Amazon DynamoDB.

Enkripsi dalam perjalanan

AWS Service Catalog menggunakan Transport Layer Security (TLS) dan enkripsi informasi sisi klien dalam perjalanan antara penelepon dan. AWS

Anda dapat mengakses AWS Service Catalog API secara pribadi dari Amazon Virtual Private Cloud (Amazon VPC) dengan membuat titik akhir VPC. Dengan titik akhir VPC, perutean antara VPC dan AWS Service Catalog ditangani oleh AWS jaringan tanpa memerlukan gateway internet, gateway NAT, atau koneksi VPN.

Generasi terbaru dari titik akhir VPC yang digunakan oleh didukung oleh AWS Service Catalog AWS PrivateLink, sebuah AWS teknologi yang memungkinkan konektivitas pribadi antar AWS layanan menggunakan Antarmuka Jaringan Elastis dengan IP pribadi di VPC Anda.

Manajemen Identitas dan Akses di AWS Service Catalog

Akses ke AWS Service Catalog membutuhkan kredensyal. Kredensi tersebut harus memiliki izin untuk mengakses AWS sumber daya, seperti AWS Service Catalog portofolio atau produk. AWS Service Catalog terintegrasi dengan AWS Identity and Access Management (IAM) untuk memungkinkan Anda memberikan AWS Service Catalog administrator izin yang mereka butuhkan untuk membuat dan mengelola produk, dan untuk memberikan pengguna AWS Service Catalog akhir izin yang mereka butuhkan untuk meluncurkan produk dan mengelola produk yang disediakan. Kebijakan ini dibuat dan dikelola oleh AWS atau secara individual oleh administrator dan pengguna akhir. Untuk mengontrol akses, Anda melampirkan kebijakan ini ke pengguna, grup, dan peran yang Anda gunakan AWS Service Catalog.

Audiens

Izin yang Anda miliki dengan AWS Identity and Access Management (IAM) dapat bergantung pada peran yang Anda mainkan. AWS Service Catalog

Izin yang Anda miliki melalui AWS Identity and Access Management (IAM) juga dapat bergantung pada peran yang Anda mainkan. AWS Service Catalog

Administrator - Sebagai AWS Service Catalog administrator, Anda memerlukan akses penuh ke konsol administrator dan izin IAM yang memungkinkan Anda melakukan tugas-tugas seperti membuat dan mengelola portofolio dan produk, mengelola kendala, dan memberikan akses ke pengguna akhir.

Pengguna akhir - Sebelum pengguna akhir dapat menggunakan produk Anda, Anda harus memberi mereka izin yang memberi mereka akses ke konsol pengguna AWS Service Catalog akhir. Mereka juga dapat memiliki izin untuk meluncurkan produk dan mengelola produk yang disediakan.

Administrator IAM – Jika Anda adalah administrator IAM, Anda mungkin ingin mempelajari detail tentang cara Anda menulis kebijakan untuk mengelola akses ke AWS Service Catalog. Untuk melihat contoh kebijakan AWS Service Catalog berbasis identitas yang dapat Anda gunakan di IAM, lihat. the section called “AWS kebijakan terkelola”

Contoh kebijakan berbasis identitas untuk AWS Service Catalog

Topik

Akses konsol untuk pengguna akhir

`AWSServiceCatalogEndUserReadOnlyAccess`Kebijakan **`AWSServiceCatalogEndUserFullAccess`**dan kebijakan memberikan akses ke tampilan konsol pengguna AWS Service Catalog akhir. Saat pengguna yang memiliki salah satu kebijakan ini memilih AWS Service Catalog AWS Management Console, tampilan konsol pengguna akhir akan menampilkan produk yang diizinkan untuk diluncurkan.

Sebelum pengguna akhir berhasil meluncurkan produk tempat Anda memberi akses, Anda harus memberi mereka izin IAM tambahan agar mereka dapat menggunakan masing-masing AWS sumber

daya yang mendasarinya dalam templat produk. AWS Service Catalog AWS CloudFormation Sebagai contoh, jika templat produk termasuk Amazon Relational Database Service (Amazon RDS), Anda harus memberikan izin pada pengguna Amazon RDS untuk meluncurkan produk.

Untuk mempelajari cara mengaktifkan pengguna akhir meluncurkan produk sambil menerapkan izin akses paling sedikit ke sumber daya, lihat. AWS the section called “Menggunakan Batasan”

Jika Anda menerapkan **`AWSServiceCatalogEndUserReadOnlyAccess`**kebijakan, pengguna Anda memiliki akses ke konsol pengguna akhir, tetapi mereka tidak akan memiliki izin yang mereka perlukan untuk meluncurkan produk dan mengelola produk yang disediakan. Anda dapat memberikan izin ini secara langsung kepada pengguna akhir yang menggunakan IAM, tetapi jika Anda ingin membatasi akses yang dimiliki pengguna akhir ke AWS sumber daya, Anda harus melampirkan kebijakan tersebut ke peran peluncuran. Anda kemudian menggunakan AWS Service Catalog untuk menerapkan peran peluncuran ke kendala peluncuran untuk produk. Untuk informasi selengkapnya tentang menerapkan peran peluncuran, batasan peran peluncuran, dan peran peluncuran sampel, lihat Batasan Peluncuran AWS Service Catalog.

> **Note**
>
> Jika Anda memberikan izin IAM kepada pengguna untuk AWS Service Catalog administrator, tampilan konsol administrator akan ditampilkan sebagai gantinya. Jangan berikan izin ini kepada pengguna akhir kecuali jika Anda ingin mereka memiliki akses ke tampilan konsol administrator.

Akses produk untuk pengguna akhir

Sebelum pengguna akhir dapat menggunakan produk yang Anda beri akses, Anda harus memberi mereka izin IAM tambahan untuk memungkinkan mereka menggunakan setiap AWS sumber daya yang mendasarinya dalam templat produk. AWS CloudFormation Sebagai contoh, jika templat produk termasuk Amazon Relational Database Service (Amazon RDS), Anda harus memberikan izin pada pengguna Amazon RDS untuk meluncurkan produk.

Jika Anda menerapkan **`AWSServiceCatalogEndUserReadOnlyAccess`**kebijakan, pengguna Anda memiliki akses ke tampilan konsol pengguna akhir, tetapi mereka tidak akan memiliki izin yang mereka perlukan untuk meluncurkan produk dan mengelola produk yang disediakan. Anda dapat memberikan izin ini secara langsung kepada pengguna akhir di IAM, tetapi jika Anda ingin membatasi akses yang dimiliki pengguna akhir ke AWS sumber daya, Anda harus melampirkan

kebijakan tersebut ke peran peluncuran. Anda kemudian menggunakan AWS Service Catalog untuk menerapkan peran peluncuran ke kendala peluncuran untuk produk. Untuk informasi selengkapnya tentang menerapkan peran peluncuran, batasan peran peluncuran, dan peran peluncuran sampel, lihat Batasan Peluncuran AWS Service Catalog.

Cpntoh kebijakan untuk mengelola produk yang disediakan

Anda dapat membuat kebijakan kustom untuk membantu memenuhi persyaratan keamanan organisasi Anda. Contoh berikut menjelaskan cara menyesuaikan tingkat akses untuk setiap tindakan dengan dukungan untuk tingkat pengguna, peran, dan akun. Anda dapat memberikan akses pada pengguna untuk melihat, memperbarui, mengakhiri, dan mengelola produk yang disediakan yang dibuat hanya oleh pengguna tersebut atau dibuat oleh orang lain yang juga di bawah peran mereka atau akun tempat mereka masuk. Akses ini hierarkis - memberikan akses tingkat akun juga memberikan akses tingkat peran dan akses tingkat pengguna, selagi menambahkan akses tingkat peran juga memberikan akses tingkat pengguna tetapi tidak akses tingkat akun. Anda dapat menentukan ini dalam kebijakan JSON menggunakan blok `Condition` sebagai `accountLevel`, `roleLevel`, atau `userLevel`.

Contoh-contoh ini juga berlaku untuk tingkat akses untuk operasi penulisan AWS Service Catalog API: `UpdateProvisionedProduct` dan`TerminateProvisionedProduct`, dan operasi baca:`DescribeRecord`,`ScanProvisionedProducts`, dan`ListRecordHistory`. Operasi API `ScanProvisionedProducts` dan `ListRecordHistory` menggunakan `AccessLevelFilterKey` sebagai input, dan bahwa nilai-nilai kunci sesuai dengan tingkat blok `Condition` yang didiskusikan di sini (`accountLevel` setara dengan nilai “Akun” `AccessLevelFilterKey`, `roleLevel` dengan “Peran”, dan `userLevel` dengan “Pengguna”). Untuk informasi selengkapnya, lihat Panduan Pengembang Service Catalog.

Contoh-contoh

- Akses admin penuh ke produk yang disediakan
- Akses pengguna akhir ke produk yang disediakan
- Akses admin sebagian ke produk yang disediakan

Akses admin penuh ke produk yang disediakan

Kebijakan berikut memungkinkan akses baca dan tulis penuh ke produk dan catatan yang disediakan dalam katalog pada tingkat akun.

```
{
```

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

Kebijakan ini secara fungsional setara dengan kebijakan berikut:

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

Tidak menentukan `Condition` blok dalam kebijakan apa pun untuk AWS Service Catalog diperlakukan sama dengan menentukan akses`"servicecatalog:accountLevel"`. Perhatikan bahwa akses `accountLevel` termasuk akses `roleLevel` dan `userLevel`.

Akses pengguna akhir ke produk yang disediakan

Kebijakan berikut membatasi akses ke operasi baca dan tulis untuk hanya produk yang disediakan atau catatan terkait yang dibuat pengguna saat ini.

```
{
```

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

Akses admin sebagian ke produk yang disediakan

Dua kebijakan di bawah ini, jika keduanya diterapkan pada pengguna yang sama, memungkinkan terjadinya tipe "akses admin parsial" dengan menyediakan akses hanya baca penuh dan akses tulis terbatas. Ini berarti pengguna dapat melihat produk yang disediakan atau catatan terkait dalam akun katalog tetapi tidak dapat melakukan tindakan apa pun pada produk atau catatan yang disediakan yang tidak dimiliki oleh pengguna tersebut.

Kebijakan pertama memungkinkan akses pengguna ke operasi tulis pada produk yang disediakan yang dibuat pengguna saat ini, tetapi tidak pada produk yang disediakan yang dibuat oleh orang lain. Kebijakan kedua menambahkan akses penuh ke operasi baca pada produk yang disediakan yang dibuat oleh semua (pengguna, peran, atau akun).

```
{
    "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 kebijakan terkelola untuk AWS Service Catalog AppRegistry

AWS kebijakan terkelola: **AWSServiceCatalogAdminFullAccess**

Anda dapat melampirkan `AWSServiceCatalogAdminFullAccess` ke entitas IAM Anda. AppRegistry juga melampirkan kebijakan ini ke peran layanan yang memungkinkan AppRegistry untuk melakukan tindakan atas nama Anda.

Kebijakan ini memberikan izin *administratif* yang memungkinkan akses penuh ke tampilan konsol administrator dan memberikan izin untuk membuat dan mengelola produk dan portofolio.

Detail izin

Kebijakan ini mencakup izin berikut.

- `servicecatalog`— Memungkinkan kepala sekolah izin penuh ke tampilan konsol administrator dan kemampuan untuk membuat dan mengelola portofolio dan produk, mengelola kendala, memberikan akses ke pengguna akhir, dan melakukan tugas administratif lainnya di dalamnya. AWS Service Catalog
- `cloudformation`— Memungkinkan izin AWS Service Catalog penuh untuk daftar, membaca, menulis, dan menandai AWS CloudFormation tumpukan.
- `config`— Memungkinkan izin AWS Service Catalog terbatas untuk portofolio, produk, dan produk yang disediakan melalui. AWS Config
- `iam`— Memungkinkan prinsipal izin penuh untuk melihat dan membuat pengguna layanan, gropus, atau peran yang diperlukan untuk membuat dan mengelola produk dan portofolio.
- `ssm`— Memungkinkan AWS Service Catalog AWS Systems Manager untuk menggunakan daftar dan membaca dokumen Systems Manager di AWS akun saat ini dan AWS Wilayah.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStackEvents",
                "cloudformation:DescribeStacks",
                "cloudformation:SetStackPolicy",
```

```
                "cloudformation:UpdateStack",
                "cloudformation:CreateChangeSet",
                "cloudformation:DescribeChangeSet",
                "cloudformation:ExecuteChangeSet",
                "cloudformation:ListChangeSets",
                "cloudformation:DeleteChangeSet",
                "cloudformation:ListStackResources",
                "cloudformation:TagResource",
                "cloudformation:CreateStackSet",
                "cloudformation:CreateStackInstances",
                "cloudformation:UpdateStackSet",
                "cloudformation:UpdateStackInstances",
                "cloudformation:DeleteStackSet",
                "cloudformation:DeleteStackInstances",
                "cloudformation:DescribeStackSet",
                "cloudformation:DescribeStackInstance",
                "cloudformation:DescribeStackSetOperation",
                "cloudformation:ListStackInstances",
                "cloudformation:ListStackSetOperations",
                "cloudformation:ListStackSetOperationResults"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:stack/SC-*",
                "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
                "arn:aws:cloudformation:*:*:changeSet/SC-*",
                "arn:aws:cloudformation:*:*:stackset/SC-*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateUploadBucket",
                "cloudformation:GetTemplateSummary",
                "cloudformation:ValidateTemplate",
                "iam:GetGroup",
                "iam:GetRole",
                "iam:GetUser",
                "iam:ListGroups",
                "iam:ListRoles",
                "iam:ListUsers",
                "servicecatalog:Get*",
                "servicecatalog:Scan*",
                "servicecatalog:Search*",
                "servicecatalog:List*",
```

```
                "servicecatalog:TagResource",
                "servicecatalog:UntagResource",
                "servicecatalog:SyncResource",
                "ssm:DescribeDocument",
                "ssm:GetAutomationExecution",
                "ssm:ListDocuments",
                "ssm:ListDocumentVersions",
                "config:DescribeConfigurationRecorders",
                "config:DescribeConfigurationRecorderStatus"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "servicecatalog:Accept*",
                "servicecatalog:Associate*",
                "servicecatalog:Batch*",
                "servicecatalog:Copy*",
                "servicecatalog:Create*",
                "servicecatalog:Delete*",
                "servicecatalog:Describe*",
                "servicecatalog:Disable*",
                "servicecatalog:Disassociate*",
                "servicecatalog:Enable*",
                "servicecatalog:Execute*",
                "servicecatalog:Import*",
                "servicecatalog:Provision*",
                "servicecatalog:Put*",
                "servicecatalog:Reject*",
                "servicecatalog:Terminate*",
                "servicecatalog:Update*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "servicecatalog.amazonaws.com"
                }
            }
```

```
        },
     {
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": "arn:aws:iam::*:role/aws-service-role/
orgsdatasync.servicecatalog.amazonaws.com/AWSServiceRoleForServiceCatalogOrgsDataSync",
    "Condition": {
    "StringEquals": {
     "iam:AWSServiceName": "orgsdatasync.servicecatalog.amazonaws.com"
           }
        }
    }
```

AWS kebijakan terkelola: **`AWSServiceCatalogAdminReadOnlyAccess`**

Anda dapat melampirkan `AWSServiceCatalogAdminReadOnlyAccess` ke entitas IAM Anda. AppRegistry juga melampirkan kebijakan ini ke peran layanan yang memungkinkan AppRegistry untuk melakukan tindakan atas nama Anda.

Kebijakan ini memberikan izin *`hanya-baca`* yang memungkinkan akses penuh ke tampilan konsol administrator. Kebijakan ini tidak memberikan akses untuk membuat atau mengelola produk dan portofolio.

Detail izin

Kebijakan ini mencakup izin berikut.

- `servicecatalog`— Mengizinkan izin hanya-baca kepala sekolah ke tampilan konsol administrator.
- `cloudformation`— Memungkinkan izin AWS Service Catalog terbatas untuk daftar dan membaca AWS CloudFormation tumpukan.
- `config`— Memungkinkan izin AWS Service Catalog terbatas untuk portofolio, produk, dan produk yang disediakan melalui. AWS Config
- `iam`— Memungkinkan izin terbatas prinsipal untuk melihat pengguna layanan, grup, atau peran yang diperlukan untuk membuat dan mengelola produk dan portofolio.
- `ssm`— Memungkinkan AWS Service Catalog AWS Systems Manager untuk menggunakan daftar dan membaca dokumen Systems Manager di AWS akun saat ini dan AWS Wilayah.

```
{
```

```
"Version": "2012-10-17",
"Statement": [
 {
  "Effect": "Allow",
  "Action": [
   "cloudformation:DescribeStackEvents",
   "cloudformation:DescribeStacks",
   "cloudformation:DescribeChangeSet",
   "cloudformation:ListChangeSets",
   "cloudformation:ListStackResources",
   "cloudformation:DescribeStackSet",
   "cloudformation:DescribeStackInstance",
   "cloudformation:DescribeStackSetOperation",
   "cloudformation:ListStackInstances",
   "cloudformation:ListStackSetOperations",
   "cloudformation:ListStackSetOperationResults"
  ],
  "Resource": [
   "arn:aws:cloudformation:*:*:stack/SC-*",
   "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
   "arn:aws:cloudformation:*:*:changeSet/SC-*",
   "arn:aws:cloudformation:*:*:stackset/SC-*"
  ]
 },
 {
  "Effect": "Allow",
  "Action": [
   "cloudformation:GetTemplateSummary",
   "iam:GetGroup",
   "iam:GetRole",
   "iam:GetUser",
   "iam:ListGroups",
   "iam:ListRoles",
   "iam:ListUsers",
   "servicecatalog:Get*",
   "servicecatalog:List*",
   "servicecatalog:Describe*",
   "servicecatalog:ScanProvisionedProducts",
   "servicecatalog:Search*",
   "ssm:DescribeDocument",
   "ssm:GetAutomationExecution",
   "ssm:ListDocuments",
   "ssm:ListDocumentVersions",
   "config:DescribeConfigurationRecorders",
```

```
    "config:DescribeConfigurationRecorderStatus"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS kebijakan terkelola: **AWSServiceCatalogEndUserFullAccess**

Anda dapat melampirkan `AWSServiceCatalogEndUserFullAccess` ke entitas IAM Anda. AppRegistry juga melampirkan kebijakan ini ke peran layanan yang memungkinkan AppRegistry untuk melakukan tindakan atas nama Anda.

Kebijakan ini memberikan izin *`kontributor`* yang memungkinkan akses penuh ke tampilan konsol pengguna akhir dan memberikan izin untuk meluncurkan produk dan mengelola produk yang disediakan.

Detail izin

Kebijakan ini mencakup izin berikut.

- `servicecatalog`— Memungkinkan kepala sekolah izin penuh ke tampilan konsol pengguna akhir dan kemampuan untuk meluncurkan produk dan mengelola produk yang disediakan.
- `cloudformation`— Memungkinkan izin AWS Service Catalog penuh untuk daftar, membaca, menulis, dan menandai AWS CloudFormation tumpukan.
- `config`— Memungkinkan izin AWS Service Catalog terbatas untuk membuat daftar dan membaca detail tentang portofolio, produk, dan produk yang disediakan melalui. AWS Config
- `ssm`— Memungkinkan AWS Service Catalog untuk menggunakan AWS Systems Manager untuk membaca dokumen Systems Manager di AWS akun saat ini dan AWS Wilayah.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "cloudformation:CreateStack",
    "cloudformation:DeleteStack",
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStacks",
```

```
    "cloudformation:SetStackPolicy",
    "cloudformation:ValidateTemplate",
    "cloudformation:UpdateStack",
    "cloudformation:CreateChangeSet",
    "cloudformation:DescribeChangeSet",
    "cloudformation:ExecuteChangeSet",
    "cloudformation:ListChangeSets",
    "cloudformation:DeleteChangeSet",
    "cloudformation:TagResource",
    "cloudformation:CreateStackSet",
    "cloudformation:CreateStackInstances",
    "cloudformation:UpdateStackSet",
    "cloudformation:UpdateStackInstances",
    "cloudformation:DeleteStackSet",
    "cloudformation:DeleteStackInstances",
    "cloudformation:DescribeStackSet",
    "cloudformation:DescribeStackInstance",
    "cloudformation:DescribeStackSetOperation",
    "cloudformation:ListStackInstances",
    "cloudformation:ListStackResources",
    "cloudformation:ListStackSetOperations",
    "cloudformation:ListStackSetOperationResults"
   ],
   "Resource": [
    "arn:aws:cloudformation:*:*:stack/SC-*",
    "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
    "arn:aws:cloudformation:*:*:changeSet/SC-*",
    "arn:aws:cloudformation:*:*:stackset/SC-*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "cloudformation:GetTemplateSummary",
    "servicecatalog:DescribeProduct",
    "servicecatalog:DescribeProductView",
    "servicecatalog:DescribeProvisioningParameters",
    "servicecatalog:ListLaunchPaths",
    "servicecatalog:ProvisionProduct",
    "servicecatalog:SearchProducts",
    "ssm:DescribeDocument",
    "ssm:GetAutomationExecution",
    "config:DescribeConfigurationRecorders",
    "config:DescribeConfigurationRecorderStatus"
```

```
    ],
    "Resource": "*"
   },
   {
    "Effect": "Allow",
    "Action": [
     "servicecatalog:DescribeProvisionedProduct",
     "servicecatalog:DescribeRecord",
     "servicecatalog:ListRecordHistory",
     "servicecatalog:ListStackInstancesForProvisionedProduct",
     "servicecatalog:ScanProvisionedProducts",
     "servicecatalog:TerminateProvisionedProduct",
     "servicecatalog:UpdateProvisionedProduct",
     "servicecatalog:SearchProvisionedProducts",
     "servicecatalog:CreateProvisionedProductPlan",
     "servicecatalog:DescribeProvisionedProductPlan",
     "servicecatalog:ExecuteProvisionedProductPlan",
     "servicecatalog:DeleteProvisionedProductPlan",
     "servicecatalog:ListProvisionedProductPlans",
     "servicecatalog:ListServiceActionsForProvisioningArtifact",
     "servicecatalog:ExecuteProvisionedProductServiceAction",
     "servicecatalog:DescribeServiceActionExecutionParameters"
    ],
    "Resource": "*",
    "Condition": {
     "StringEquals": {
      "servicecatalog:userLevel": "self"
     }
    }
   }
  ]
}
```

AWS kebijakan terkelola: **AWSServiceCatalogEndUserReadOnlyAccess**

Anda dapat melampirkan `AWSServiceCatalogEndUserReadOnlyAccess` ke entitas IAM Anda. AppRegistry juga melampirkan kebijakan ini ke peran layanan yang memungkinkan AppRegistry untuk melakukan tindakan atas nama Anda.

Kebijakan ini memberikan izin *`hanya-baca`* yang memungkinkan akses hanya-baca ke tampilan konsol pengguna akhir. Kebijakan ini tidak memberikan izin untuk meluncurkan produk atau mengelola produk yang disediakan.

Detail izin

Kebijakan ini mencakup izin berikut.

- `servicecatalog`— Mengizinkan izin hanya-baca utama ke tampilan konsol pengguna akhir.
- `cloudformation`— Memungkinkan izin AWS Service Catalog terbatas untuk daftar dan membaca AWS CloudFormation tumpukan.
- `config`— Memungkinkan izin AWS Service Catalog terbatas untuk membuat daftar dan membaca detail tentang portofolio, produk, dan produk yang disediakan melalui. AWS Config
- `ssm`— Memungkinkan AWS Service Catalog untuk menggunakan AWS Systems Manager untuk membaca dokumen Systems Manager di AWS akun saat ini dan AWS Wilayah.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "cloudformation:DescribeStackEvents",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeChangeSet",
    "cloudformation:ListChangeSets",
    "cloudformation:DescribeStackSet",
    "cloudformation:DescribeStackInstance",
    "cloudformation:DescribeStackSetOperation",
    "cloudformation:ListStackInstances",
    "cloudformation:ListStackResources",
    "cloudformation:ListStackSetOperations",
    "cloudformation:ListStackSetOperationResults"
   ],
   "Resource": [
    "arn:aws:cloudformation:*:*:stack/SC-*",
    "arn:aws:cloudformation:*:*:stack/StackSet-SC-*",
    "arn:aws:cloudformation:*:*:changeSet/SC-*",
    "arn:aws:cloudformation:*:*:stackset/SC-*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "cloudformation:GetTemplateSummary",
```

```
    "servicecatalog:DescribeProduct",
    "servicecatalog:DescribeProductView",
    "servicecatalog:DescribeProvisioningParameters",
    "servicecatalog:ListLaunchPaths",
    "servicecatalog:SearchProducts",
    "ssm:DescribeDocument",
    "ssm:GetAutomationExecution",
    "config:DescribeConfigurationRecorders",
    "config:DescribeConfigurationRecorderStatus"
   ],
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "servicecatalog:DescribeProvisionedProduct",
    "servicecatalog:DescribeRecord",
    "servicecatalog:ListRecordHistory",
    "servicecatalog:ListStackInstancesForProvisionedProduct",
    "servicecatalog:ScanProvisionedProducts",
    "servicecatalog:SearchProvisionedProducts",
    "servicecatalog:DescribeProvisionedProductPlan",
    "servicecatalog:ListProvisionedProductPlans",
    "servicecatalog:ListServiceActionsForProvisioningArtifact",
    "servicecatalog:DescribeServiceActionExecutionParameters"
   ],
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "servicecatalog:userLevel": "self"
    }
   }
  }
 ]
}
```

AWS kebijakan terkelola: **AWSServiceCatalogSyncServiceRolePolicy**

AWS Service Catalog melampirkan kebijakan ini ke peran `AWSServiceRoleForServiceCatalogSync` terkait layanan (SLR), yang memungkinkan AWS Service Catalog untuk menyinkronkan templat di repositori eksternal ke produk. AWS Service Catalog

Kebijakan ini memberikan izin yang memungkinkan akses terbatas ke AWS Service Catalog tindakan (misalnya, panggilan API), dan tindakan AWS layanan lain yang AWS Service Catalog bergantung padanya.

Kebijakan ini mencakup izin berikut.

- `servicecatalog`— Memungkinkan peran sinkronisasi AWS Service Catalog artefak akses terbatas ke API AWS Service Catalog publik.
- `codestar-connections`— Memungkinkan peran sinkronisasi AWS Service Catalog artefak akses terbatas ke API CodeConnections publik.
- `cloudformation`— Memungkinkan peran sinkronisasi AWS Service Catalog artefak akses terbatas ke API AWS CloudFormation publik.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "ArtifactSynctoServiceCatalog",
   "Effect": "Allow",
   "Action": [
    "servicecatalog:ListProvisioningArtifacts",
    "servicecatalog:DescribeProductAsAdmin",
    "servicecatalog:DeleteProvisioningArtifact",
    "servicecatalog:ListServiceActionsForProvisioningArtifact",
    "servicecatalog:CreateProvisioningArtifact",
    "servicecatalog:UpdateProvisioningArtifact"
   ],
   "Resource": "*"
  },
  {
   "Sid": "AccessArtifactRepositories",
   "Effect": "Allow",
   "Action": [
    "codestar-connections:UseConnection"
   ],
   "Resource": "arn:aws:codestar-connections:*:*:connection/*"
  },
  {
   "Sid": "ValidateTemplate",
   "Effect": "Allow",
```

```
    "Action": [
     "cloudformation:ValidateTemplate"
    ],
    "Resource": "*"
   }
  ]
}
```

AWS Service Catalog menggunakan detail izin di atas untuk peran `AWSServiceRoleForServiceCatalogSync` terkait layanan yang dibuat saat pengguna membuat atau memperbarui AWS Service Catalog produk yang digunakan. CodeConnections Anda dapat mengubah kebijakan ini menggunakan AWS CLI, AWS API, atau melalui konsol. AWS Service Catalog Untuk informasi selengkapnya tentang cara membuat, mengedit, dan menghapus peran terkait layanan, lihat Menggunakan peran terkait layanan (SLR) untuk. AWS Service Catalog

Izin yang disertakan dalam peran `AWSServiceRoleForServiceCatalogSync` terkait layanan memungkinkan AWS Service Catalog untuk melakukan tindakan berikut atas nama pelanggan.

- `servicecatalog:ListProvisioningArtifacts`— Memungkinkan peran sinkronisasi AWS Service Catalog artefak untuk mencantumkan artefak penyediaan untuk AWS Service Catalog produk tertentu yang disinkronkan ke file template dalam repositori.
- `servicecatalog:DescribeProductAsAdmin`— Memungkinkan peran sinkronisasi AWS Service Catalog artefak untuk menggunakan `DescribeProductAsAdmin` API untuk mendapatkan detail untuk AWS Service Catalog produk dan artefak yang disediakan terkait yang disinkronkan ke file template dalam repositori. Peran sinkronisasi artefak menggunakan output dari panggilan ini untuk memverifikasi batas kuota layanan produk untuk penyediaan artefak.
- `servicecatalog:DeleteProvisioningArtifact`— Memungkinkan peran sinkronisasi AWS Service Catalog artefak untuk menghapus artefak yang disediakan.
- `servicecatalog:ListServiceActionsForProvisioningArtifact`— Memungkinkan peran sinkronisasi AWS Service Catalog artefak untuk menentukan apakah Tindakan Layanan dikaitkan dengan artefak penyediaan dan memastikan bahwa artefak penyediaan tidak dihapus jika Tindakan Layanan dikaitkan.
- `servicecatalog:DescribeProvisioningArtifact`— Memungkinkan peran sinkronisasi AWS Service Catalog artefak untuk mengambil detail dari `DescribeProvisioningArtifact` API, termasuk ID komit, yang disediakan dalam output. `SourceRevisionInfo`

- `servicecatalog:CreateProvisioningArtifact`— Memungkinkan peran sinkronisasi AWS Service Catalog artefak untuk membuat artefak baru yang disediakan jika perubahan terdeteksi (misalnya, git-push dilakukan) ke file template sumber di repositori eksternal.
- `servicecatalog:UpdateProvisioningArtifact`— Memungkinkan peran sinkronisasi AWS Service Catalog artefak untuk memperbarui artefak yang disediakan untuk produk yang terhubung atau disinkronkan.
- `codestar-connections:UseConnection`— Memungkinkan peran sinkronisasi AWS Service Catalog artefak untuk menggunakan koneksi yang ada untuk memperbarui dan menyinkronkan produk.
- `cloudformation:ValidateTemplate`— Memungkinkan peran sinkronisasi AWS Service Catalog artefak akses terbatas AWS CloudFormation untuk memvalidasi format template untuk template yang digunakan dalam repositori eksternal dan memverifikasi apakah AWS CloudFormation dapat mendukung template.

AWS kebijakan terkelola: **`AWSServiceCatalogOrgsDataSyncServiceRolePolicy`**

AWS Service Catalog melampirkan kebijakan ini ke peran `AWSServiceRoleForServiceCatalogOrgsDataSync` terkait layanan (SLR), yang memungkinkan AWS Service Catalog untuk disinkronkan. AWS Organizations

Kebijakan ini memberikan izin yang memungkinkan akses terbatas ke AWS Service Catalog tindakan (misalnya, panggilan API), dan tindakan AWS layanan lain yang AWS Service Catalog bergantung padanya.

Kebijakan ini mencakup izin berikut.

- `organizations`— Memungkinkan peran sinkronisasi AWS Service Catalog data terbatas akses ke API AWS Organizations publik.

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

```
            "Action": [
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListChildren",
                "organizations:ListParents",
                "organizations:ListAWSServiceAccessForOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Service Catalog menggunakan detail izin di atas untuk peran `AWSServiceRoleForServiceCatalogOrgsDataSync` terkait layanan yang dibuat saat pengguna mengaktifkan akses portofolio AWS Organizations bersama atau membuat pembagian portofolio. Anda dapat mengubah kebijakan ini menggunakan AWS CLI, AWS API, atau melalui konsol. AWS Service Catalog Untuk informasi selengkapnya tentang cara membuat, mengedit, dan menghapus peran terkait layanan, lihat Menggunakan peran terkait layanan (SLR) untuk. AWS Service Catalog

Izin yang disertakan dalam peran `AWSServiceRoleForServiceCatalogOrgsDataSync` terkait layanan memungkinkan AWS Service Catalog untuk melakukan tindakan berikut atas nama pelanggan.

- `organizations:DescribeAccount`— Memungkinkan peran AWS Service Catalog Organizations Data Sync untuk mengambil informasi AWS Organizations terkait tentang akun yang ditentukan.
- `organizations:DescribeOrganization`— Memungkinkan peran AWS Service Catalog Organizations Data Sync untuk mengambil informasi tentang organisasi yang menjadi milik akun pengguna.
- `organizations:ListAccounts`— Memungkinkan peran AWS Service Catalog Organizations Data Sync untuk mencantumkan akun di organisasi pengguna.
- `organizations:ListChildren`— Memungkinkan peran AWS Service Catalog Organizations Data Sync untuk mencantumkan semua unit organisasi (UO) atau akun yang terkandung dalam OU atau root induk yang ditentukan.
- `organizations:ListParents`— Memungkinkan peran AWS Service Catalog Organizations Data Sync untuk mencantumkan root atau OU yang berfungsi sebagai induk langsung dari OU atau akun anak yang ditentukan.

- `organizations:ListAWSServiceAccessForOrganization`— Memungkinkan peran AWS Service Catalog Organizations Data Sync untuk mengambil daftar AWS layanan yang diaktifkan pengguna untuk mengintegrasikan dengan organisasi mereka.

Kebijakan yang tidak lagi digunakan

Kebijakan terkelola berikut tidak lagi digunakan:

- ServiceCatalogAdminFullAccess— Gunakan AWSServiceCatalogAdminFullAccesssebagai gantinya.
- ServiceCatalogAdminReadOnlyAccess— Gunakan AWSServiceCatalogAdminReadOnlyAccesssebagai gantinya.
- ServiceCatalogEndUserFullAccess— Gunakan AWSServiceCatalogEndUserFullAccesssebagai gantinya.
- ServiceCatalogEndUserAccess— Gunakan AWSServiceCatalogEndUserReadOnlyAccesssebagai gantinya.

Gunakan prosedur berikut untuk memastikan bahwa administrator dan pengguna akhir diberikan izin untuk menggunakan kebijakan saat ini.

Untuk bermigrasi dari kebijakan usang ke kebijakan saat ini, lihat Menambahkan dan menghapus izin identitas IAM di Panduan Pengguna.AWS Identity and Access Management

AppRegistry pembaruan kebijakan AWS terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola AppRegistry sejak layanan ini mulai melacak perubahan ini. Untuk peringatan otomatis tentang perubahan pada halaman ini, berlangganan umpan RSS di halaman Riwayat AppRegistry dokumen.

Perubahan	Deskripsi	Tanggal
AWSServiceCatalogAdminFullAccess— Perbarui kebijakan terkelola	AWS Service Catalog memperbarui `AWSServiceCatalogAdminFullAccess` kebijakan untuk menyertakan izin yang diperlukan AWS Service	April 14, 2023

Perubahan	Deskripsi	Tanggal
	Catalog administrator untuk membuat peran `AWSServiceRoleForServiceCatalogOrgsDataSync` terkait layanan (SLR) di akun mereka.	
AWSServiceCatalogOrgsDataSyncServiceRolePolicy— Kebijakan terkelola baru	AWS Service Catalog menambahkan`AWSServiceCatalogOrgsDataSyncServiceRolePolicy` , yang dilampirkan ke peran `AWSServiceRoleForServiceCatalogOrgsDataSync` terkait layanan (SLR), memungkinkan AWS Service Catalog untuk disinkronkan dengan. AWS Organizations Kebijakan ini memungkinkan akses terbatas ke AWS Service Catalog tindakan (misalnya, panggilan API), dan tindakan AWS layanan lain yang AWS Service Catalog bergantung padanya.	April 14, 2023

Perubahan	Deskripsi	Tanggal
AWSServiceCatalogAdminFullAccess— Perbarui kebijakan terkelola	AWS Service Catalog memperbarui `AWSServiceCatalogAdminFullAccess` kebijakan untuk menyertakan semua izin untuk AWS Service Catalog Administrator dan membuat kompatibilitas dengannya AppRegistry.	Januari 12, 2023
AWSServiceCatalogSyncServiceRolePolicy— Kebijakan terkelola baru	AWS Service Catalog menambahkan `AWSServiceCatalogSyncServiceRolePolicy` kebijakan, yang dilampirkan ke peran `AWSServiceRoleForServiceCatalogSync` terkait layanan (SLR). Kebijakan ini memungkinkan AWS Service Catalog untuk menyinkronkan templat di repositori eksternal ke AWS Service Catalog produk.	18 November 2022

Perubahan	Deskripsi	Tanggal
AWSServiceRoleForServiceCatalogSync— Peran terkait layanan baru	AWS Service Catalog menambahkan peran `AWSServiceRoleForServiceCatalogSync` terkait layanan (SLR). Peran ini diperlukan AWS Service Catalog untuk menggunakan CodeConnections dan membuat, memperbarui, dan menjelaskan Artefak AWS Service Catalog Penyediaan untuk suatu produk.	18 November 2022

Perubahan	Deskripsi	Tanggal
AWSServiceCatalogAdminFullAccess— Kebijakan terkelola yang diperbarui	AWS Service Catalog memperbarui `AWSServiceCatalogAdminFullAccess` kebijakan untuk menyertakan semua izin yang diperlukan untuk AWS Service Catalog Administrator. Kebijakan mengidentifikasi tindakan spesifik yang dapat dilakukan administrator terhadap semua AWS Service Catalog sumber daya, seperti membuat, mendeskripsikan, menghapus, dan lainnya. Selain itu, kebijakan diubah untuk mendukung fitur yang baru diluncurkan, Attribute Based Access Control (ABAC) untuk AWS Service Catalog. ABAC memungkinkan Anda menggunakan `AWSServiceCatalogAdminFullAccess` kebijakan sebagai templat untuk mengizinkan atau menolak tindakan pada AWS Service Catalog sumber daya berdasarkan tag. Untuk informasi lebih lanjut tentang ABAC, lihat Untuk AWS apa ABAC. AWS Identity and Access Management	30 September 2022

Perubahan	Deskripsi	Tanggal
AppRegistry mulai melacak perubahan	AppRegistry mulai melacak perubahan untuk kebijakan yang AWS dikelola.	15 September 2022

Menggunakan peran terkait layanan untuk AWS Service Catalog

AWS Service Catalog menggunakan AWS Identity and Access Management peran terkait layanan (IAM). Peran terkait layanan adalah jenis unik peran IAM yang ditautkan langsung ke. AWS Service Catalog Peran terkait layanan telah ditentukan sebelumnya oleh AWS Service Catalog dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan AWS Service Catalog lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. AWS Service Catalog mendefinisikan izin peran terkait layanan, dan kecuali ditentukan lain, hanya AWS Service Catalog dapat mengambil perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, serta bahwa kebijakan izin tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi AWS Service Catalog sumber daya Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, lihat Layanan AWS yang Bekerja bersama IAM dan mencari layanan yang memiliki Ya dalam Peran Terkait Layanan. Pilih Ya dengan sebuah tautan untuk melihat dokumentasi peran terkait layanan untuk layanan tersebut.

Izin peran terkait layanan untuk **`AWSServiceRoleForServiceCatalogSync`**

AWS Service Catalog dapat menggunakan peran terkait layanan bernama **`AWSServiceRoleForServiceCatalogSync`**— Peran terkait layanan ini diperlukan AWS Service Catalog untuk menggunakan CodeConnections dan membuat, memperbarui, dan menjelaskan Artefak AWS Service Catalog Penyediaan untuk suatu produk.

Peran tertaut layanan `AWSServiceRoleForServiceCatalogSync` memercayai layanan berikut untuk mengambil peran tersebut:

- `sync.servicecatalog.amazonaws.com`

Kebijakan izin peran bernama AWSServiceCatalogSyncServiceRolePolicymemungkinkan AWS Service Catalog untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan: `Connection` pada `CodeConnections`
- Tindakan: `Create, Update, and Describe` aktif `ProvisioningArtifact` untuk suatu AWS Service Catalog produk

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran tertaut layanan dalam Panduan Pengguna IAM.

Membuat peran **`AWSServiceRoleForServiceCatalogSync`** terkait layanan

Anda tidak perlu membuat peran `AWSServiceRoleForServiceCatalogSync` terkait layanan secara manual. AWS Service Catalog membuat peran terkait layanan untuk Anda secara otomatis saat Anda membuat CodeConnections di AWS Management Console, the AWS CLI, atau API. AWS

> **Important**
>
> Peran tertaut layanan ini dapat muncul di akun Anda jika Anda menyelesaikan tindakan di layanan lain yang menggunakan fitur yang disupport oleh peran ini. Juga, jika Anda menggunakan AWS Service Catalog layanan sebelum 18 November 2022, ketika mulai mendukung peran terkait layanan, maka AWS Service Catalog buat `AWSServiceRoleForServiceCatalogSync` peran tersebut di akun Anda. Untuk mempelajari lebih lanjut, lihat Peran baru muncul di akun IAM saya.

Jika Anda menghapus peran yang terhubung dengan layanan ini, lalu ingin membuatnya lagi, Anda dapat menggunakan proses yang sama untuk membuat ulang peran tersebut di akun Anda. Ketika Anda membangun CodeConnections, AWS Service Catalog ciptakan peran terkait layanan untuk Anda lagi.

Anda juga dapat menggunakan konsol IAM untuk membuat peran terkait layanan dengan kasus penggunaan Produk yang disinkronkan AWS Service Catalog . Di AWS CLI atau AWS API, buat peran terkait layanan dengan nama `sync.servicecatalog.amazonaws.com` layanan. Untuk informasi selengkapnya, lihat Membuat peran tertaut layanan dalam Panduan Pengguna IAM. Jika Anda menghapus peran tertaut layanan ini, Anda dapat mengulang proses yang sama untuk membuat peran tersebut lagi.

Izin peran terkait layanan untuk **AWSServiceRoleForServiceCatalogOrgsDataSync**

AWS Service Catalog dapat menggunakan peran terkait layanan bernama **AWSServiceRoleForServiceCatalogOrgsDataSync**— Peran terkait layanan ini diperlukan agar AWS Service Catalog organisasi tetap sinkron. AWS Organizations

Peran tertaut layanan `AWSServiceRoleForServiceCatalogOrgsDataSync` memercayai layanan berikut untuk mengambil peran tersebut:

- `orgsdatasync.servicecatalog.amazonaws.com`

Peran `AWSServiceRoleForServiceCatalogOrgsDataSync` terkait layanan mengharuskan Anda menggunakan kebijakan kepercayaan berikut selain kebijakan `AWSServiceCatalogOrgsDataSyncServiceRolePolicy` terkelola:

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

Kebijakan izin peran bernama AWSServiceCatalogOrgsDataSyncServiceRolePolicymemungkinkan AWS Service Catalog untuk menyelesaikan tindakan berikut pada sumber daya yang ditentukan:

- Tindakan:`DescribeAccount`,`DescribeOrganization`, dan `ListAWSServiceAccessForOrganization` seterusnya `Organizations accounts`
- Tindakan:`ListAccounts`,`ListChildren`, dan `ListParent` seterusnya `Organizations accounts`

Anda harus mengonfigurasi izin untuk mengizinkan entitas IAM (seperti pengguna, grup, atau peran) untuk membuat, mengedit, atau menghapus peran terkait layanan. Untuk informasi selengkapnya, lihat Izin peran tertaut layanan dalam Panduan Pengguna IAM.

Membuat peran **`AWSServiceRoleForServiceCatalogOrgsDataSync`** terkait layanan

Anda tidak perlu membuat peran `AWSServiceRoleForServiceCatalogOrgsDataSync` terkait layanan secara manual. AWS Service Catalog mempertimbangkan tindakan Anda mengaktifkan Berbagi dengan AWS Organizations atau Membagi Portofolio sebagai izin AWS Service Catalog untuk membuat SLR di latar belakang atas nama Anda.

AWS Service Catalog membuat peran terkait layanan untuk Anda secara otomatis saat Anda meminta `EnableAWSOrganizationsAccess` atau `CreatePortfolioShare` di AWS Management Console, API AWS CLI, atau API. AWS

> **Important**
>
> Peran tertaut layanan ini dapat muncul di akun Anda jika Anda menyelesaikan tindakan di layanan lain yang menggunakan fitur yang disupport oleh peran ini. Untuk mempelajari lebih lanjut, lihat Peran baru muncul di akun IAM saya.

Jika Anda menghapus peran yang terhubung dengan layanan ini, lalu ingin membuatnya lagi, Anda dapat menggunakan proses yang sama untuk membuat ulang peran tersebut di akun Anda. Saat Anda meminta `EnableAWSOrganizationsAccess` atau`CreatePortfolioShare`, AWS Service Catalog buat peran terkait layanan untuk Anda lagi.

Mengedit peran terkait layanan untuk AWS Service Catalog

AWS Service Catalog tidak memungkinkan Anda untuk mengedit `AWSServiceRoleForServiceCatalogSync` atau peran `AWSServiceRoleForServiceCatalogOrgsDataSync` terkait layanan. Setelah membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin merujuk peran tersebut. Namun, Anda dapat mengedit deskripsi peran ini menggunakan IAM. Untuk informasi lebih lanjut, lihat Mengedit peran terkait layanan dalam Panduan Pengguna IAM.

Menghapus peran terkait layanan untuk AWS Service Catalog

Anda dapat menggunakan konsol IAM, AWS CLI, atau API untuk menghapus `AWSServiceRoleForServiceCatalogSync` atau AWS SLR secara manual.

`AWSServiceRoleForServiceCatalogOrgsDataSync` Untuk melakukan ini, Anda harus terlebih dahulu menghapus semua sumber daya yang menggunakan peran terkait layanan (misalnya, AWS Service Catalog produk apa pun yang disinkronkan ke repositori eksternal), dan kemudian peran terkait layanan dapat dihapus secara manual.

Wilayah yang didukung untuk peran yang terhubung dengan layanan AWS Service Catalog

AWS Service Catalog mendukung penggunaan peran terkait layanan di semua wilayah tempat layanan tersedia. Untuk informasi selengkapnya, silakan lihat Wilayah AWS dan titik akhir.

Nama wilayah	Identitas wilayah	Support di AWS Service Catalog
AS Timur (Virginia Utara)	us-east-1	Ya
US East (Ohio)	us-east-2	Ya
US West (N. California)	us-west-1	Ya
US West (Oregon)	us-west-2	Ya
Afrika (Cape Town)	af-south-1	Ya
Asia Pasifik (Hong Kong)	ap-east-1	Ya
Asia Pasifik (Jakarta)	ap-southeast-3	Ya
Asia Pacific (Mumbai)	ap-south-1	Ya
Asia Pacific (Osaka)	ap-northeast-3	Ya
Asia Pacific (Seoul)	ap-northeast-2	Ya
Asia Pacific (Singapore)	ap-southeast-1	Ya
Asia Pacific (Sydney)	ap-southeast-2	Ya
Asia Pacific (Tokyo)	ap-northeast-1	Ya
Canada (Central)	ca-sentral-1	Ya

Nama wilayah	Identitas wilayah	Support di AWS Service Catalog
Eropa (Frankfurt)	eu-central-1	Ya
Eropa (Irlandia)	eu-west-1	Ya
Eropa (London)	eu-west-2	Ya
Eropa (Milan)	eu-south-1	Ya
Europe (Paris)	eu-west-3	Ya
Eropa (Stockholm)	eu-north-1	Ya
Timur Tengah (Bahrain)	me-south-1	Ya
South America (São Paulo)	sa-east-1	Ya
AWS GovCloud (AS-Timur)	us-gov-east-1	Tidak
AWS GovCloud (AS-Barat)	us-gov-west-1	Tidak

Memecahkan masalah AWS Service Catalog identitas dan akses

Gunakan informasi berikut untuk membantu Anda mendiagnosis dan memperbaiki masalah umum yang mungkin Anda temui saat bekerja dengan AWS Service Catalog dan IAM.

Topik

- Saya tidak berwenang untuk melakukan tindakan di AWS Service Catalog
- Saya tidak berwenang untuk melakukan iam:PassRole
- Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses AWS Service Catalog sumber daya saya

Saya tidak berwenang untuk melakukan tindakan di AWS Service Catalog

Jika AWS Management Console memberitahu Anda bahwa Anda tidak berwenang untuk melakukan tindakan, maka Anda harus menghubungi administrator Anda untuk bantuan. Administrator Anda

adalah orang yang memberi Anda kredensial masuk. Contoh kesalahan berikut terjadi ketika pengguna mateojackson mencoba menggunakan konsol untuk melihat detail tentang my-example-widget sumber daya fiksi tetapi tidak memiliki izin fiksi. `aws:GetWidget`

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

Dalam hal ini, Mateo meminta administratornya untuk memperbarui kebijakannya untuk mengizinkan dia mengakses sumber daya `my-example-widget` menggunakan tindakan `aws:GetWidget`.

Saya tidak berwenang untuk melakukan **`iam:PassRole`**

Jika Anda menerima kesalahan bahwa Anda tidak terotorisasi untuk melakukan tindakan `iam:PassRole`, Anda harus menghubungi administrator untuk mendapatkan bantuan. Administrator Anda adalah orang yang memberikan Anda nama pengguna dan kata sandi Anda. Minta orang tersebut untuk memperbarui kebijakan Anda agar Anda dapat memberikan peran ke AWS Service Catalog.

Beberapa AWS layanan memungkinkan Anda untuk meneruskan peran yang ada ke layanan tersebut, alih-alih membuat peran layanan baru atau peran terkait layanan. Untuk melakukannya, Anda harus memiliki izin untuk meneruskan peran ke layanan.

Contoh kesalahan berikut terjadi ketika pengguna bernama marymajor mencoba menggunakan konsol untuk melakukan tindakan di. AWS Service Catalog Namun, tindakan ini mengharuskan layanan memiliki izin yang diberikan oleh peran layanan. Mary tidak memiliki izin untuk meneruskan peran tersebut ke layanan.

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

Dalam hal ini, Mary meminta administratornya untuk memperbarui kebijakannya untuk memungkinkannya melakukan PassRole tindakan iam:.

Saya ingin mengizinkan orang di luar AWS akun saya untuk mengakses AWS Service Catalog sumber daya saya

Anda dapat membuat peran yang dapat digunakan pengguna di akun lain atau pengguna di luar organisasi Anda untuk mengakses sumber daya Anda. Anda dapat menentukan siapa saja yang

dipercaya untuk mengambil peran tersebut. Untuk layanan yang mendukung kebijakan berbasis sumber daya atau daftar kontrol akses (ACL), Anda dapat menggunakan kebijakan tersebut untuk memberi pengguna akses ke sumber daya Anda.

Untuk mempelajari selengkapnya, periksa hal berikut:

- Untuk mempelajari apakah AWS Service Catalog mendukung fitur ini, lihat AWS Identity and Access ManagementAWS Service Catalog di Panduan AWS Service Catalog Administrator.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda di seluruh AWS akun yang Anda miliki, lihat Menyediakan akses ke pengguna IAM di AWS akun lain yang Anda miliki di Panduan Pengguna IAM.
- Untuk mempelajari cara menyediakan akses ke sumber daya Anda ke AWS akun pihak ketiga, lihat Menyediakan akses ke AWS akun yang dimiliki oleh pihak ketiga di Panduan Pengguna IAM.
- Untuk mempelajari cara memberikan akses melalui federasi identitas, lihat Memberikan akses kepada pengguna eksternal yang sah (federasi identitas) dalam Panduan Pengguna IAM.
- Untuk mempelajari perbedaan antara penggunaan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat Perbedaan antara peran IAM dan kebijakan berbasis sumber daya di Panduan Pengguna IAM.

Mengontrol Akses

AWS Service Catalog portofolio memberi administrator Anda tingkat kontrol akses untuk grup pengguna akhir Anda. Ketika Anda menambahkan pengguna ke portofolio, mereka dapat menelusuri dan meluncurkan salah satu produk dalam portofolio. Untuk informasi selengkapnya, lihat the section called “Mengelola Portofolio”.

Batasan

Batasan mengontrol aturan yang diterapkan ke pengguna akhir Anda saat meluncurkan produk dari portofolio tertentu. Anda menggunakannya untuk menerapkan batasan produk untuk tata kelola atau pengendalian biaya. Untuk informasi selengkapnya tentang batasan, lihat the section called “Menggunakan Batasan”.

AWS Service Catalog kendala peluncuran memberi Anda kontrol lebih besar atas izin yang dibutuhkan oleh pengguna akhir. Ketika administrator Anda membuat batasan peluncuran untuk produk dalam portofolio, batasan peluncuran mengaitkan ARN peran yang digunakan ketika pengguna akhir Anda meluncurkan produk dari portofolio tersebut. Dengan menggunakan pola ini,

Anda dapat mengontrol akses ke pembuatan AWS sumber daya. Untuk informasi selengkapnya, lihat the section called “Batasan Peluncuran”.

Logging dan Monitoring di AWS Service Catalog

AWS Service Catalog terintegrasi dengan AWS CloudTrail, layanan yang menangkap semua panggilan AWS Service Catalog API dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Untuk informasi selengkapnya, lihat Mencatat Panggilan AWS Service Catalog API dengan CloudTrail.

Anda juga dapat menggunakan batasan notifikasi untuk menyiapkan notifikasi Amazon SNS tentang peristiwa tumpukan. Untuk informasi selengkapnya, lihat the section called “Batasan Notifikasi”.

Validasi Kepatuhan untuk AWS Service Catalog

Auditor pihak ketiga menilai keamanan dan kepatuhan AWS Service Catalog sebagai bagian dari beberapa program AWS kepatuhan, termasuk yang berikut:

- Kontrol Sistem dan Organisasi (SOC)
- Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS)
- Program Manajemen Risiko dan Otorisasi Federal (FedRAMP)
- Undang-Undang Akuntabilitas dan Portabilitas Asuransi Kesehatan (HIPAA)

Untuk daftar AWS layanan dalam lingkup program kepatuhan tertentu, lihat AWS Services in Scope by Compliance Program. Untuk informasi umum, lihat Program AWS Kepatuhan Program AWS .

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat Mengunduh Laporan di AWS Artefak.

Tanggung jawab kepatuhan Anda saat menggunakan AWS Service Catalog tergantung pada sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya ini untuk membantu kepatuhan:

- Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar yang berfokus pada keamanan dan kepatuhan. AWS

- Arsitektur untuk Whitepaper Keamanan dan Kepatuhan HIPAA — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan untuk membuat aplikasi yang sesuai dengan HIPAA. AWS
- AWS Sumber Daya Kepatuhan - Kumpulan buku kerja dan panduan ini dapat berlaku untuk industri dan lokasi Anda.
- AWS Config AWS Layanan ini menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- AWS Security Hub— AWS Layanan ini memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS yang membantu Anda memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik.

Ketahanan di AWS Service Catalog

Infrastruktur AWS global dibangun di sekitar AWS Wilayah dan Zona Ketersediaan. AWS Wilayah menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang dan mengoperasikan aplikasi dan basis data yang melakukan secara otomatis pinda saat gagal/failover di antara zona-zona tanpa terputus. Availability Zone memiliki ketersediaan yang lebih baik, toleransi kesalahan, dan dapat diskalakan dibandingkan satu atau beberapa infrastruktur pusat data tradisional.

Untuk informasi selengkapnya tentang AWS Wilayah dan Availability Zone, lihat Infrastruktur AWS Global.

Selain infrastruktur AWS global, AWS Service Catalog menawarkan tindakan AWS Service Catalog swalayan. Dengan tindakan layanan mandiri, pelanggan dapat mengurangi perawatan administratif dan pelatihan pengguna akhir sambil mengikuti langkah-langkah kepatuhan dan keamanan. Dengan tindakan layanan mandiri, sebagai administrator, Anda dapat mengaktifkan pengguna akhir untuk melakukan tugas-tugas operasional seperti pencadangan dan pemulihan, memecahkan masalah, menjalankan perintah yang disetujui, dan meminta izin di AWS Service Catalog. Untuk mempelajari selengkapnya, lihat the section called “Menggunakan Tindakan Layanan”.

Keamanan Infrastruktur di AWS Service Catalog

Sebagai layanan terkelola, AWS Service Catalog dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat

Keamanan AWS Cloud. Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat Perlindungan Infrastruktur dalam Kerangka Kerja yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses AWS Service Catalog melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Selain itu, permintaan harus ditandatangani dengan menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan pengguna utama IAM. Atau Anda dapat menggunakan AWS Security Token Service (AWS STS) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

Dengan AWS Service Catalog, Anda dapat mengontrol Wilayah tempat data disimpan. Portofolio dan produk hanya tersedia di Wilayah tempat Anda telah membuatnya tersedia. Anda dapat menggunakan API `CopyProduct` untuk menyalin produk ke Wilayah lainnya.

Praktik Terbaik Keamanan untuk AWS Service Catalog

AWS Service Catalog menyediakan sejumlah fitur keamanan untuk dipertimbangkan saat Anda mengembangkan dan menerapkan kebijakan keamanan Anda sendiri. Praktik terbaik berikut adalah pedoman umum dan tidak mewakili solusi keamanan yang lengkap. Karena praktik terbaik ini mungkin tidak sesuai atau cukup untuk lingkungan Anda, anggap praktik terbaik tersebut sebagai pertimbangan yang membantu dan bukan sebagai rekomendasi.

Anda dapat menentukan aturan yang membatasi nilai parameter yang dimasukkan pengguna saat meluncurkan produk. Aturan-aturan ini disebut batasan templat karena aturan ini membatasi cara templat AWS CloudFormation untuk produk di-deploy. Anda menggunakan editor sederhana untuk membuat batasan templat, dan Anda menerapkannya pada produk individu.

AWS Service Catalog menerapkan kendala saat menyediakan produk baru atau memperbarui produk yang sudah digunakan. Ini selalu menerapkan batasan yang paling ketat di antara semua batasan yang diterapkan pada portofolio dan produk. Sebagai contoh, pertimbangkan skenario saat produk memungkinkan semua instans Amazon EC2 diluncurkan dan portofolio memiliki dua batasan:

satu yang memungkinkan semua instans EC2 tipe non-GPU yang akan diluncurkan dan satu yang memungkinkan hanya t1.micro dan m1.small EC2 yang akan diluncurkan. Untuk contoh ini, AWS Service Catalog terapkan kendala kedua yang lebih ketat (t1.micro dan m1.small).

Anda dapat membatasi akses yang dimiliki pengguna akhir ke AWS sumber daya saat Anda melampirkan kebijakan IAM ke peran peluncuran. Anda kemudian menggunakan AWS Service Catalog untuk membuat batasan peluncuran untuk menggunakan peran saat meluncurkan produk.

Untuk mempelajari selengkapnya tentang kebijakan terkelola AWS Service Catalog, lihat Kebijakan AWS Terkelola untuk AWS Service Catalog.

Mengelola Katalog

AWS Service Catalog menyediakan antarmuka untuk mengelola portofolio, produk, dan batasan dari konsol administrator.

> **Note**
>
> Untuk melakukan tugas apa pun di bagian ini, Anda harus memiliki izin administrator untuk AWS Service Catalog. Untuk informasi selengkapnya, lihat Manajemen Identitas dan Akses di AWS Service Catalog.

Tugas

- Mengelola Portofolio
- Mengelola Produk
- Menggunakan Batasan AWS Service Catalog
- Tindakan Layanan AWS Service Catalog
- Menambahkan Produk AWS Marketplace untuk Portofolio Anda
- Menggunakan AWS CloudFormation StackSets
- Mengelola Anggaran

Mengelola Portofolio

Anda membuat, melihat, dan memperbarui portofolio pada halaman Portofolio di konsol administrator AWS Service Catalog.

Tugas

- Membuat, Melihat, dan Menghapus Portofolio
- Melihat Detail Portofolio
- Membuat dan Menghapus Portofolio
- Menambahkan produk
- Menambahkan Batasan
- Memberikan Akses ke Pengguna
- Membagi Portofolio

- Membagikan dan Mengimpor Portofolio

Membuat, Melihat, dan Menghapus Portofolio

Halaman Portofolio menampilkan daftar portofolio yang telah Anda buat di wilayah saat ini. Gunakan halaman ini untuk membuat portofolio baru, lihat detail portofolio, atau hapus portofolio dari akun Anda.

Untuk melihat halaman Portofolio

1. Buka konsol Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Pilih wilayah yang berbeda seperlunya.
3. Jika Anda baru saja menggunakan AWS Service Catalog, Anda dapat melihat halaman awal AWS Service Catalog. Pilih Memulai untuk membuat portofolio. Ikuti instruksi untuk membuat portofolio pertama Anda, lalu lanjutkan ke halaman Portofolio.

Saat menggunakan AWS Service Catalog, Anda dapat kembali ke halaman Portofolio setiap saat; pilih Service Catalog di bilah navigasi lalu pilih Portofolio.

Melihat Detail Portofolio

Di konsol administrator AWS Service Catalog, halaman Detail Portofolio mencantumkan pengaturan untuk portofolio. Gunakan halaman ini untuk mengelola produk dalam portofolio, memberikan pengguna akses ke produk, dan menerapkan TagOptions dan kendala.

Untuk melihat halaman Detail Portofolio

1. Buka konsol Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Pilih portofolio yang ingin Anda kelola.

Membuat dan Menghapus Portofolio

Gunakan halaman Portofolio untuk membuat dan menghapus portofolio.

Untuk membuat portofolio baru

1. Di menu navigasi kiri, pilih Portofolio.
2. Pilih Buat portofolio.

3. Pada halaman Buat portofolio, masukkan informasi yang diminta.
4. Pilih Buat. AWS Service Catalog membuat portofolio dan menampilkan detail portofolio.

Untuk menghapus portofolio

> **Note**
>
> Anda hanya dapat menghapus portofolio lokal. Anda dapat menghapus portofolio yang diimpor (bersama), tetapi Anda tidak dapat menghapus portofolio yang diimpor.

Sebelum Anda dapat menghapus portofolio, Anda harus menghapus semua produk, kendala, grup, peran, pengguna, saham, dan. TagOptions Untuk melakukannya, buka portofolio untuk menampilkan detail Portofolio. Kemudian pilih tab untuk menghapusnya.

> **Note**
>
> Untuk menghindari kesalahan, hapus kendala dari portofolio sebelum Anda menghapus produk apa pun.

1. Di menu navigasi kiri, pilih Portofolio.
2. Pilih portofolio yang ingin Anda hapus.
3. Pilih Hapus. Anda hanya dapat menghapus portofolio lokal. Jika Anda mencoba menghapus portofolio yang diimpor (bersama), menu Tindakan tidak tersedia.
4. Di jendela konfirmasi, pilih Hapus.

Menambahkan produk

Anda dapat menambahkan produk ke portofolio dengan mengunggah produk baru langsung ke portofolio yang ada atau dengan mengaitkan produk yang ada dari katalog Anda ke portofolio.

> **Note**
>
> Saat Anda membuat AWS Service Catalog produk, Anda dapat mengunggah AWS CloudFormation templat atau file konfigurasi Terraform. AWS CloudFormationTemplate disimpan dalam bucket Amazon Simple Storage Service (Amazon S3), dan nama bucket

dimulai dengan "cf-templates-.” Anda juga harus memiliki izin untuk mengambil objek dari bucket tambahan saat menyediakan produk. Untuk informasi selengkapnya, lihat Membuat produk.

Menambahkan produk baru

Anda menambahkan produk baru langsung dari halaman rincian Portofolio. Ketika Anda membuat produk dari halaman ini, AWS Service Catalog menambahkannya ke portofolio yang saat ini dipilih.

Untuk menambahkan produk baru

1. Arahkan ke halaman Portofolio, lalu pilih nama portofolio yang ingin Anda tambahkan produk.
2. Pada halaman detail Portofolio, perluas bagian Produk, lalu pilih Unggah produk baru.
3. Untuk Masukkan detail produk, masukkan perintah berikut:

   - Nama Produk – Nama dari produk tersebut.
   - Deskripsi produk (opsional) — Deskripsi produk. Deskripsi ini ditampilkan dalam daftar produk untuk membantu Anda memilih produk yang benar.
   - Deskripsi – Deskripsi lengkap. Deskripsi ini ditampilkan dalam daftar produk untuk membantu Anda memilih produk yang benar.
   - Pemilik atau Distributor — Nama atau alamat email pemilik. Informasi kontak untuk distributor adalah opsional.
   - Vendor (opsional) – Nama penerbit aplikasi. Bidang ini memungkinkan Anda mengurutkan daftar produk agar lebih mudah menemukan produk.
4. Di halaman Detail versi, masukkan informasi berikut:

   - Pilih template — Untuk AWS CloudFormation produk, pilih file template Anda sendiri, AWS CloudFormation template dari drive lokal atau URL yang menunjuk ke template yang disimpan di Amazon S3, template Stack AWS CloudFormation ARN yang ada, atau file template yang disimpan dalam repositori eksternal.

     Untuk produk Teraform, pilih file template Anda sendiri, file konfigurasi tar.gz dari drive lokal atau URL yang menunjuk ke template yang disimpan di Amazon S3, atau file konfigurasi tar.gz yang disimpan di repositori eksternal.
   - Nama versi (opsional) - Nama versi produk (misalnya, “v1", “v2beta”). Spasi tidak diperbolehkan.

- Deskripsi (opsional) – Deskripsi versi produk mencakup perbedaan versi ini dari versi sebelumnya.

5. Untuk Masukkan detail dukungan, masukkan hal-hal berikut:

   - Kontak email (opsional) – Alamat email untuk melaporkan masalah dengan produk.
   - Support Link (opsional) — URL ke situs tempat pengguna dapat menemukan informasi dukungan atau tiket file. URL harus dimulai dengan `http://` atau `https://`. Administrator bertanggung jawab untuk menjaga keakuratan dan akses informasi dukungan.
   - Deskripsi Support (opsional) - Deskripsi tentang bagaimana Anda harus menggunakan kontak Email dan tautan Support.

6. Pilih Buat produk.

Menambahkan produk yang sudah ada

Anda dapat menambahkan produk yang ada ke portofolio dari tiga tempat: daftar Portofolio, halaman rincian Portofolio, atau halaman daftar Produk.

Untuk menambahkan produk yang sudah ada ke portofolio

1. Arahkan ke halaman Portofolio.
2. Pilih portofolio. Kemudian pilih Tindakan - Tambahkan produk ke portofolio.
3. Pilih produk, lalu pilih Tambahkan produk ke portofolio.

Menghapus produk dari portofolio

Ketika Anda tidak lagi ingin menggunakan produk, hapus dari portofolio. Produk ini masih tersedia dalam katalog Anda dari halaman Produk, dan Anda masih dapat menambahkannya ke portofolio lain. Anda dapat menghapus beberapa produk dari portofolio pada satu waktu.

Untuk menghapus produk dari portofolio

1. Arahkan ke halaman Portofolio, lalu pilih portofolio yang berisi produk. Halaman detail Portofolio terbuka.
2. Perluas bagian Produk.
3. Pilih satu atau beberapa produk, lalu pilih Hapus.
4. Konfirmasikan pilihan Anda.

Menambahkan Batasan

Anda harus menambahkan batasan untuk mengontrol cara pengguna terlibat dengan produk. Untuk informasi selengkapnya tentang tipe kebijakan batasan yang mendukung AWS Service Catalog, lihat Menggunakan Batasan AWS Service Catalog.

Anda menambahkan batasan untuk produk setelah ditempatkan dalam portofolio.

Untuk menambahkan batasan pada produk

1. Buka konsol Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Pilih Portofolio dan pilih portofolio.
3. Di halaman detail portofolio, perluas bagian Create constraint dan pilih Add constraints.
4. Untuk Produk, pilih produk yang akan diterapkan batasan.
5. Untuk Tipe batasan, pilih salah satu opsi berikut:

   Peluncuran - Memungkinkan Anda menetapkan peran IAM ke produk yang digunakan untuk menyediakan sumber daya. AWS Untuk informasi selengkapnya, lihat Batasan Peluncuran AWS Service Catalog.

   Pemberitahuan - Memungkinkan Anda mengalirkan pemberitahuan produk ke topik Amazon SNS. Untuk informasi selengkapnya, lihat Batasan Notifikasi AWS Service Catalog.

   Template - Memungkinkan Anda membatasi opsi yang tersedia bagi pengguna akhir saat mereka meluncurkan produk. Template terdiri dari file teks berformat JSON yang berisi satu atau beberapa aturan. Aturan ditambahkan ke templat AWS CloudFormation yang digunakan oleh produk. Untuk informasi selengkapnya, lihat Aturan Batasan Templat.

   Stack Set - Memungkinkan Anda mengonfigurasi penyebaran produk di seluruh akun dan wilayah yang digunakan AWS CloudFormation StackSets. Untuk informasi selengkapnya, lihat Batasan Set Tumpukan AWS Service Catalog.

   Perbarui Tanda — Mengizinkan Anda untuk memperbarui tanda setelah produk telah disediakan. Untuk informasi selengkapnya, lihat AWS Service CatalogBatasan Pembaruan Tag.
6. Pilih Lanjutkan dan masukkan informasi yang diperlukan.

Untuk mengedit batasan

1. Masuklah ke AWS Management Console dan buka konsol administrator AWS Service Catalog di https://console.aws.amazon.com/catalog/.
2. Pilih Portofolio dan pilih portofolio.
3. Di halaman detail Portofolio, perluas bagian Buat batasan dan pilih kendala untuk diedit.
4. Pilih Mengedit batasan.
5. Edit kendala sesuai kebutuhan, dan pilih Simpan.

Memberikan Akses ke Pengguna

Berikan pengguna akses ke portofolio melalui grup atau peran. Cara terbaik untuk menyediakan akses portofolio bagi banyak pengguna adalah menempatkan pengguna dalam grup IAM dan memberikan akses ke grup tersebut. Dengan begitu, Anda cukup menambahkan dan menghapus pengguna dari grup untuk mengelola akses portofolio. Untuk informasi selengkapnya, lihat Pengguna dan grup IAM dalam Panduan Pengguna IAM.

Selain akses ke portofolio, pengguna juga harus memiliki akses ke konsol pengguna AWS Service Catalog akhir. Anda memberikan akses ke konsol tersebut dengan menerapkan izin di IAM. Untuk informasi selengkapnya, lihat Manajemen Identitas dan Akses di AWS Service Catalog.

Jika Anda ingin berbagi portofolio dan Prinsipnya dengan akun lain, Anda dapat mengaitkan Nama Utama (grup, peran, atau pengguna) dengan Portofolio. Nama Utama dibagikan dengan Portofolio dan digunakan di akun penerima untuk memberikan akses ke pengguna akhir.

Untuk memberikan akses portofolio ke pengguna atau grup

1. Buka konsol Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Dari panel navigasi, pilih Administrasi, lalu pilih Portofolio.
3. Pilih portofolio yang ingin Anda berikan kepada grup, peran, atau akses pengguna. AWS Service Catalogmengarahkan ke halaman rincian Portofolio.
4. Pada halaman Detail Portofolio, pilih tab Access.
5. Di bawah akses Portofolio, pilih Akses hibah.
6. Untuk Type, pilih Principal Name, lalu pilih group/, role/, atau user/, Type. Anda dapat menambahkan hingga 9 nama utama.
7. Pilih Akses Hibah untuk mengaitkan prinsipal dengan portofolio saat ini.

Untuk menghapus akses ke portofolio

1. Pada halaman Detail portofolio, pilih grup, peran, atau nama pengguna.
2. Pilih Hapus akses.

Membagi Portofolio

Untuk mengaktifkan AWS Service Catalog administrator AWS akun lain untuk mendistribusikan produk Anda ke pengguna akhir, bagikan AWS Service Catalog portofolio Anda dengan mereka menggunakan account-to-account berbagi atauAWS Organizations.

Ketika Anda berbagi portofolio menggunakan account-to-account berbagi atau Organizations, Anda berbagi referensi portofolio tersebut. Produk dan batasan dalam portofolio impor tetap sinkron dengan perubahan yang Anda buat ke Portofolio bersama, portofolio asli yang Anda bagikan.

Penerima tidak dapat mengubah produk atau kendala, tetapi dapat menambahkan AWS Identity and Access Management akses untuk pengguna akhir.

> **Note**
>
> Anda tidak dapat berbagi sumber daya bersama. Termasuk portofolio yang berisi produk bersama.

ccount-to-account Berbagi

Untuk menyelesaikan langkah-langkah ini, Anda harus mendapatkan ID akun dari AWS akun target. Anda dapat menemukan ID di halaman Akun saya di AWS Management Console dari akun target.

Untuk berbagi portofolio dengan AWS akun

1. Buka konsol Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Di menu navigasi kiri, pilih Portofolio dan kemudian pilih portofolio yang ingin Anda bagikan. Di menu Tindakan, pilih Bagikan.
3. Di Masukkan ID akun masukkan ID AWS akun akun yang Anda bagikan. (Opsional) Pilih TagOption Berbagi. Lalu, pilih Bagikan.
4. Kirim URL ke administrator AWS Service Catalog akun target. URL membuka halaman Portofolio impor dengan ARN dari portofolio bersama yang disediakan secara otomatis.

Mengimpor portofolio

Jika AWS Service Catalog administrator untuk AWS akun lain berbagi portofolio dengan Anda, impor portofolio itu ke akun Anda sehingga Anda dapat mendistribusikan produknya ke pengguna akhir Anda.

Anda tidak perlu mengimpor portofolio jika portofolio dibagikanAWS Organizations.

Untuk mengimpor portofolio, Anda harus mendapatkan ID portofolio dari administrator.

Untuk melihat semua portofolio yang diimpor, buka AWS Service Catalog konsol di https://console.aws.amazon.com/servicecatalog/. Pada halaman Portofolio, pilih tab Imported. Tinjau tabel Portofolio Impor.

Berbagi dengan AWS Organizations

Anda dapat berbagi portofolio AWS Service Catalog menggunakan AWS Organizations.

Pertama, Anda harus memutuskan apakah Anda berbagi dari akun manajemen atau akun administrator yang didelegasikan. Jika Anda tidak ingin berbagi dari akun manajemen Anda, daftarkan akun admin yang didelegasikan yang dapat Anda gunakan untuk berbagi. Untuk informasi selengkapnya, lihat Daftarkan administrator yang didelegasikan di Panduan Pengguna AWS CloudFormation.

Selanjutnya, Anda harus memutuskan siapa yang akan dibagikan. Anda dapat berbagi ke entitas berikut:

- Akun organisasi.
- Unit organisasi (OU)
- Organisasi itu sendiri. (Entitas tersebut dibagikan dengan setiap akun dalam organisasi.)

Berbagi dari akun manajemen

Anda dapat berbagi portofolio dengan organisasi ketika Anda menggunakan struktur organisasi atau memasukkan ID simpul organisasi.

Untuk berbagi portofolio dengan organisasi dengan menggunakan struktur organisasi

1. Buka konsol AWS Service Catalog di https://console.aws.amazon.com/servicecatalog/.

2. Pada halaman Portofolio, pilih portofolio yang ingin Anda bagikan. Di menu Tindakan, pilih Bagikan.
3. Pilih AWS Organizationsdan filter ke dalam struktur organisasi Anda.

   Anda dapat memilih simpul Root untuk berbagi portofolio dengan seluruh organisasi Anda, Unit Organisasi (OU) induk, OU turunan, atau akun AWS dalam organisasi Anda.

   Berbagi ke OU induk membagikan portofolio ke semua akun dan OU turunan dalam OU induk tersebut.

   Anda dapat memilih Lihat AWS akun hanya untuk melihat daftar semua AWS akun di organisasi Anda.

Untuk berbagi portofolio dengan organisasi dengan memasukkan ID node organisasi

1. Buka konsol AWS Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Pada halaman Portofolio, pilih portofolio yang ingin Anda bagikan. Di menu Tindakan, pilih Bagikan.
3. Pilih Simpul Organisasi.

   Pilih apakah Anda ingin berbagi dengan seluruh organisasi, AWS akun dalam organisasi Anda, atau OU.

   Masukkan ID node organisasi yang Anda pilih, yang dapat Anda temukan di dalam AWS Organizations konsol di https://console.aws.amazon.com/organizations/.

Berbagi dari akun administrator yang didelegasikan

Akun manajemen organisasi yang dapat mendaftar dan membatalkan pendaftaran akun lain sebagai administrator yang didelegasikan untuk organisasi.

Administrator yang didelegasikan dapat berbagi sumber daya AWS Service Catalog dalam organisasi mereka dengan cara yang sama seperti akun manajemen. Mereka berwenang untuk membuat, menghapus, dan berbagi portofolio.

Untuk mendaftar atau membatalkan pendaftaran administrator yang didelegasikan, Anda harus menggunakan API atau CLI dari akun manajemen. Untuk informasi selengkapnya, lihat RegisterDelegatedAdministratordan DeregisterDelegatedAdministratordi Referensi AWS Organizations API.

> **Note**
>
> Sebelum Anda dapat menunjuk delegasi, administrator harus menelepon. `EnableAWSOrganizationsAccess`

Prosedur untuk membagi portofolio dari akun administrator yang didelegasikan sama dengan yang dibagikan dari akun manajemen, seperti yang terlihat di atas di the section called “Berbagi dari akun manajemen”.

Jika anggota membatalkan pendaftaran sebagai administrator yang didelegasikan, berikut ini terjadi:

- Pembagian portofolio yang dibuat dari akun tersebut akan dihapus.
- Mereka tidak bisa lagi membuat pembagian portofolio baru.

> **Note**
>
> Jika portofolio dan pembagian yang dibuat oleh administrator yang didelegasikan tidak dihapus setelah administrator didelegasikan membatalkan pendaftarannya, daftar dan batalkan pendaftarannya kembali administrator yang didelegasikan. Tindakan ini menghapus portofolio dan pembagian yang dibuat oleh akun tersebut.

Memindahkan akun dalam organisasi Anda

Jika Anda memindahkan akun dalam organisasi Anda, AWS Service Catalog portofolio yang dibagikan dengan akun tersebut mungkin berubah.

Akun hanya memiliki akses ke portofolio yang dibagikan dengan organisasi tujuan atau unit organisasi mereka.

Berbagi TagOptions saat berbagi portofolio

Sebagai administrator, Anda dapat membuat share untuk disertakan TagOptions. TagOptions adalah pasangan nilai kunci yang memungkinkan administrator untuk:

- Mendefinisikan dan menerapkan taksonomi untuk tanda.
- Tentukan opsi tanda dan kaitkan ke produk dan portofolio.

- Bagikan opsi tanda yang terkait dengan portofolio dan produk dengan akun lain.

Bila Anda menambahkan atau menghapus opsi tanda di akun utama, perubahan akan muncul secara otomatis di akun penerima. Di akun penerima, ketika pengguna akhir menyediakan produk TagOptions, mereka harus memilih nilai untuk tag yang menjadi tag pada produk yang disediakan.

Di akun penerima, administrator dapat mengaitkan lokal tambahan TagOptions ke portofolio impor mereka untuk menegakkan aturan penandaan yang khusus untuk akun tersebut.

> **Note**
>
> Untuk berbagi portofolio, Anda memerlukan ID AWS akun konsumen. Temukan ID AWS akun di Akun Saya di konsol.

> **Note**
>
> Jika a TagOption memiliki nilai tunggal, AWS secara otomatis memberlakukan nilai tersebut selama proses penyediaan.

Untuk berbagi TagOptions saat berbagi portofolio

1. Di menu navigasi kiri, pilih Portofolio.
2. Pada Portofolio lokal, pilih dan buka portfolio.
3. Pilih Pembagian dari daftar di atas lalu pilih tombol Pembagian.
4. Pilih untuk berbagi dengan AWS akun atau organisasi lain.
5. Masukkan 12 digit nomor ID akun, pilih Aktifkan, lalu pilih Pembagian.

   Akun yang Anda bagikan ditampilkan di bagian Akun yang dibagikan dengan. Ini menunjukkan TagOptions apakah diaktifkan.

Anda juga dapat memperbarui bagian portofolio untuk disertakan TagOptions. Semua TagOptions yang termasuk dalam portofolio dan produk sekarang dibagikan ke akun ini.

Untuk memperbarui bagian portofolio untuk disertakan TagOptions

1. Di menu navigasi kiri, pilih Portofolio.

2. Pada Portofolio lokal, pilih dan buka portfolio.
3. Pilih Pembagian dari daftar di atas.
4. Pada Akun yang dibagikan dengan, pilih ID akun, lalu pilih Tindakan.
5. Pilih Perbarui berhenti berbagi atau Berhenti Berbagi.

   Saat Anda memilih Perbarui unshare, pilih Aktifkan untuk memulai berbagi. TagOptions Akun yang Anda bagikan ditampilkan di bagian Akun yang dibagikan dengan.

   Ketika Anda memilih Berhenti Berbagi, konfirmasi Anda tidak lagi ingin berbagi akun.

Berbagi Nama Utama saat berbagi portofolio

Sebagai administrator, Anda dapat membuat bagian Portofolio yang menyertakan Nama Utama. Nama Utama adalah nama untuk grup, peran, dan pengguna yang dapat ditentukan oleh administrator dalam Portofolio, dan kemudian dibagikan dengan portofolio. Saat Anda membagikan portofolio, AWS Service Catalog verifikasi apakah Nama Utama tersebut sudah ada. Jika memang ada, AWS Service Catalog secara otomatis mengaitkan Prinsipal IAM yang cocok dengan Portofolio bersama untuk memberikan akses ke pengguna.

> **Note**
>
> Ketika Anda mengaitkan prinsipal dengan portofolio, jalur eskalasi hak istimewa potensial dapat terjadi ketika portofolio tersebut kemudian dibagikan dengan akun lain. Untuk pengguna di akun penerima yang bukan AWS Service Catalog Admin, tetapi masih memiliki kemampuan untuk membuat Prinsipal (Pengguna/Peran), pengguna tersebut dapat membuat Principal IAM yang cocok dengan asosiasi nama utama untuk portofolio. Meskipun pengguna ini mungkin tidak tahu nama utama mana yang terkaitAWS Service Catalog, mereka mungkin dapat menebak pengguna. Jika jalur eskalasi potensial ini menjadi perhatian, maka AWS Service Catalog rekomendasikan untuk menggunakan `PrincipalType` as`IAM`. Dengan konfigurasi ini, `PrincipalARN` harus sudah ada di akun penerima sebelum dapat dikaitkan.

Saat Anda menambahkan atau menghapus Nama Utama di akun utama, AWS Service Catalog secara otomatis menerapkan perubahan tersebut di akun penerima. Pengguna di akun penerima kemudian dapat melakukan tugas berdasarkan peran mereka:

- Pengguna akhir dapat menyediakan, memperbarui, dan menghentikan produk portofolio.

- Administrator dapat mengaitkan Prinsipal IAM tambahan ke portofolio impor mereka untuk memberikan akses ke pengguna akhir khusus untuk akun tersebut.

> **Note**
>
> Berbagi Nama Utama hanya tersedia untukAWS Organizations.

Untuk berbagi Nama Utama saat berbagi portofolio

1. Di menu navigasi kiri, pilih Portofolio.
2. Di Portofolio lokal, pilih portofolio yang ingin Anda bagikan.
3. Di menu Tindakan, pilih Bagikan.
4. Pilih organisasi diAWS Organizations.
5. Pilih seluruh akar organisasi, unit organisasi (OU), atau anggota organisasi.
6. Di pengaturan Bagikan, aktifkan opsi Berbagi utama.

Anda juga dapat memperbarui pembagian portofolio untuk menyertakan berbagi Nama Utama. Ini membagikan semua Nama Utama yang termasuk dalam portofolio tersebut dengan akun penerima.

Untuk memperbarui pembagian portofolio untuk mengaktifkan atau menonaktifkan Nama Utama

1. Di menu navigasi kiri, pilih Portofolio.
2. Dalam portofolio lokal, pilih portofolio yang ingin Anda perbarui.
3. Pilih tab Bagikan.
4. Pilih berbagi yang ingin Anda perbarui, lalu pilih Bagikan.
5. Pilih Perbarui berbagi, lalu pilih Aktifkan untuk memulai berbagi Principal. AWS Service Catalogkemudian membagikan Nama Utama di akun penerima.

Nonaktifkan berbagi Principal jika Anda ingin berhenti membagikan Nama Utama dengan akun penerima.

Menggunakan wildcard saat berbagi Nama Utama

AWS Service Catalogmendukung pemberian akses portofolio ke nama kepala sekolah IAM (pengguna, grup atau peran) dengan wildcard, seperti '*' atau '?'. Menggunakan pola wildcard

memungkinkan Anda untuk mencakup beberapa nama utama IAM sekaligus. Jalur ARN dan nama utama memungkinkan karakter wildcard tak terbatas.

Contoh ARN wildcard yang dapat diterima:

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

Contoh ARN wildcard yang tidak dapat diterima:

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

Dalam format ARN Principal IAM **arn:partition:iam:::resource-type/resource-path/resource-name** (), nilai yang valid termasuk user/, group/, atau role/. “?” dan “*” hanya diperbolehkan setelah tipe sumber daya di segmen resource-id. Anda dapat menggunakan karakter khusus di mana saja dalam resource-id.

Karakter “*” juga cocok dengan karakter “/”, memungkinkan jalur dibentuk dalam resource-id. Sebagai contoh:

arn:aws:iam:::role/*/ResourceName_?cocok dengan keduanya **arn:aws:iam:::role/pathA/pathB/ResourceName_1** dan**arn:aws:iam:::role/pathA/ResourceName_1**.

Membagikan dan Mengimpor Portofolio

Untuk membuat AWS Service Catalog produk Anda tersedia bagi pengguna yang tidak ada dalam AndaAkun AWS, seperti pengguna yang berasal dari organisasi lain atau orang lain Akun AWS di organisasi Anda, Anda membagikan portofolio Anda dengan mereka. Anda dapat berbagi dalam beberapa cara, termasuk account-to-account berbagi, berbagi organisasi, dan menerapkan katalog menggunakan kumpulan tumpukan.

Sebelum Anda berbagi produk dan portofolio ke akun lain, Anda harus memutuskan apakah ingin berbagi referensi katalog atau men-deploy salinan katalog ke setiap akun penerima. Perhatikan bahwa jika Anda men-deploy salinan, Anda harus men-deploy ulang jika ada pembaruan yang ingin disebarkan ke akun penerima.

Anda dapat menggunakan set tumpukan untuk men-deploy katalog Anda ke banyak akun pada saat yang sama. Jika Anda ingin berbagi referensi (versi impor portofolio Anda yang tetap sinkron

dengan aslinya), Anda dapat menggunakan account-to-account berbagi atau Anda dapat berbagi menggunakanAWS Organizations.

Untuk menggunakan kumpulan tumpukan untuk menerapkan salinan katalog Anda, lihat Cara menyiapkan katalog multi-wilayah, multi-akun produk standar perusahaan. AWS Service Catalog

Ketika Anda berbagi portofolio menggunakan account-to-account berbagi atauAWS Organizations, Anda mengizinkan AWS Service Catalog administrator AWS akun lain untuk mengimpor portofolio Anda ke akun mereka dan mendistribusikan produk ke pengguna akhir di akun itu.

Portofolio impor ini bukan salinan independen. Produk dan batasan dalam portofolio impor tetap sinkron dengan perubahan yang Anda buat ke Portofolio bersama, portofolio asli yang Anda bagikan. Administrator penerima, administrator dengan siapa Anda berbagi portofolio, tidak dapat mengubah produk atau batasan, tetapi dapat menambahkan akses (IAM) AWS Identity and Access Management untuk pengguna akhir. Untuk informasi selengkapnya, lihat Memberikan Akses ke Pengguna.

Administrator penerima dapat mendistribusikan produk ke pengguna akhir yang termasuk dalam AWS akun mereka dengan cara berikut:

- Dengan menambahkan pengguna, grup, dan peran ke portofolio yang diimpor.
- Dengan menambahkan produk dari portofolio yang diimpor ke portofolio lokal, portofolio terpisah yang dibuat oleh administrator penerima dan milik AWS akun mereka. Administrator penerima kemudian menambahkan pengguna, grup, dan peran ke portofolio lokal tersebut. Setiap kendala yang awalnya diterapkan pada produk dalam portofolio bersama juga ada dalam portofolio lokal. Administrator penerima portofolio lokal dapat menambahkan batasan tambahan, tetapi tidak dapat menghapus batasan yang awalnya diimpor dari portofolio bersama.

Ketika Anda menambahkan produk atau batasan untuk portofolio bersama atau menghapus produk atau batasan dari portofolio tersebut, perubahan menyebar ke semua instans portofolio yang diimpor. Misalnya, jika Anda menghapus produk dari portofolio bersama, produk tersebut juga dihapus dari portofolio yang diimpor. Produk tersebut juga dihapus dari semua portofolio lokal yang ditambahkan ke produk impor. Jika pengguna akhir meluncurkan produk sebelum Anda menghapusnya, produk yang disediakan pengguna akhir terus berjalan, namun produk menjadi tidak tersedia untuk peluncuran di masa mendatang.

Jika Anda menerapkan batasan peluncuran untuk produk dalam portofolio bersama, hal itu menyebar ke semua instans produk yang diimpor. Untuk mengganti batasan peluncuran ini, administrator penerima menambahkan produk ke portofolio lokal lalu menerapkan batasan peluncuran yang berbeda untuk itu. Batasan peluncuran yang berlaku menetapkan peran peluncuran untuk produk.

Peran peluncuran adalah peran IAM yang AWS Service Catalog digunakan untuk menyediakan AWS sumber daya (seperti instans Amazon EC2 atau database Amazon RDS) saat pengguna akhir meluncurkan produk. Sebagai administrator, Anda dapat memilih untuk menunjuk peran peluncuran tertentu ARN atau nama peran lokal. Jika Anda menggunakan peran ARN, peran akan digunakan meskipun pengguna akhir milik AWS akun yang berbeda dari yang memiliki peran peluncuran. Jika Anda menggunakan nama peran lokal, peran IAM dengan nama itu di akun pengguna akhir akan digunakan.

Untuk informasi selengkapnya tentang batasan peluncuran dan peran peluncuran, lihat Batasan Peluncuran AWS Service Catalog. Akun AWS yang memiliki kesediaan peran peluncuran sumber daya AWS, dan akun ini menimbulkan biaya penggunaan untuk sumber daya tersebut. Untuk informasi selengkapnya, lihat Harga AWS Service Catalog.

Video ini menunjukkan kepada Anda cara berbagi portofolio di seluruh akun di. AWS Service Catalog

Bagikan (https://www.youtube.com/embed/BVSohYOppjk%22%3EShare) Portofolio di Seluruh Akun di. AWS Service Catalog

> **Note**
>
> Anda tidak dapat membagi kembali produk dari portofolio yang telah diimpor atau dibagi.

> **Note**
>
> Portofolio impor harus terjadi di wilayah yang sama antara manajemen dan akun dependen.

Hubungan antara Portofolio Bersama dan yang Diimpor

Tabel ini merangkum hubungan antara portofolio yang diimpor dan portofolio bersama, dan tindakan yang administrator yang mengimpor portofolio dapat serta tidak dapat dilakukan dengan portofolio tersebut dan produk di dalamnya.

Elemen Portofolio Bersama	Hubungan dengan Portofolio yang Diimpor	Administrator penerima dapat melakukan	Administrator penerima tidak dapat melakukan
Produk dan versi produk	Diwarisi. Jika pembuat portofolio menambahkan produk ke atau menghapus produk dari portofolio bersama, perubahan akan menyebar ke portofolio yang diimpor.	Tambahkan produk yang diimpor ke portofolio lokal. Produk tetap sinkron dengan portofolio bersama.	Unggah atau tambahkan produk ke portofolio yang diimpor atau hapus produk dari portofolio yang diimpor.
Batasan peluncuran	Diwarisi. Jika pembuat portofolio menambahkan batasan peluncuran ke atau menghapus batasan peluncuran dari produk bersama, perubahan akan menyebar ke semua instance produk yang diimpor. Jika administrator penerima menambahkan produk yang diimpor ke portofolio lokal mereka, batasan peluncuran yang diimpor tidak akan	Dalam portofolio lokal, administrator dapat menerapkan batasan peluncuran yang memengaruhi peluncuran produk secara lokal.	Tambahkan batasan peluncuran atau hapus batasan peluncuran dari portofolio yang diimpor.

Elemen Portofolio Bersama	Hubungan dengan Portofolio yang Diimpor	Administrator penerima dapat melakukan	Administrator penerima tidak dapat melakukan
	dibawa ke portofolio bersama.		
Batasan templat	Diwarisi. Jika pembuat portofolio menambahkan batasan templat untuk atau menghapus batasan templat dari produk bersama, perubahan akan menyebar ke semua instans produk yang diimpor. Jika administrator penerima menambahkan produk impor ke portofolio lokal, batasan template yang diimpor tidak akan dibawa ke portofolio lokal.	Dalam portofolio lokal, administrator dapat menambahkan batasan template yang membatasi produk lokal.	Hapus batasan templat yang diimpor.
Pengguna, grup, dan peran	Tidak diwariskan.	Tambahkan pengguna, grup, dan peran yang ada di AWS akun administrator.	Tidak berlaku.

Mengelola Produk

Anda dapat membuat produk, memperbarui produk dengan membuat versi baru berdasarkan template yang diperbarui, dan mengelompokkan produk bersama ke dalam portofolio untuk mendistribusikannya kepada pengguna.

Versi baru produk disebarkan ke semua pengguna yang memiliki akses ke produk melalui portofolio. Saat Anda mendistribusikan pembaruan, pengguna akhir dapat memperbarui produk yang sudah disediakan.

Tugas

- Melihat Halaman Produk
- Membuat Produk
- Menambahkan produk ke portofolio
- Memperbarui produk
- Menyinkronkan produk ke file template dari GitHub, GitHub Enterprise, atau Bitbucket
- Menghapus produk
- Mengelola Versi

Melihat Halaman Produk

Anda mengelola produk dari halaman daftar Produk di konsol AWS Service Catalog administrator.

Untuk melihat halaman daftar Produk

1. Buka konsol Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Pilih Daftar Produk.

Membuat Produk

Anda membuat produk dari halaman Produk di dalam konsol administrator AWS Service Catalog.

> **Note**
>
> Membuat produk Terraform memerlukan konfigurasi tambahan, termasuk mesin penyediaan Terraform dan peran peluncuran. Untuk informasi lebih lanjut, tinjauMemulai dengan produk Terraform.

Untuk membuat produk AWS Service Catalog baru

1. Arahkan ke halaman daftar Produk.
2. Pilih Buat produk, dan pilih Buat produk.
3. Detail produk - Memungkinkan Anda memilih jenis produk yang ingin Anda buat. AWS Service CatalogmendukungAWS CloudFormation, Terraform Cloud, dan jenis produk Eksternal (mendukung Terraform Community Edition). Detail produk juga berisi metadata yang muncul saat Anda mencari dan melihat produk dalam daftar atau halaman detail. Masukkan yang berikut ini:
   - Nama Produk – Nama dari produk tersebut.
   - Deskripsi Produk — Deskripsi ditampilkan dalam daftar produk untuk membantu Anda memilih produk yang benar.
   - Pemilik — Orang atau organisasi yang menerbitkan produk ini. Pemilik dapat berupa nama organisasi TI Anda, atau administrator.
   - Distributor (opsional) — Nama penerbit aplikasi. Bidang ini memungkinkan Anda mengurutkan daftar produk agar lebih mudah menemukan produk.
4. Detail versi memungkinkan Anda untuk menambahkan file template Anda dan membangun produk Anda. Masukkan yang berikut ini:
   - Pilih metode — Ada empat cara untuk menambahkan file template.
     - Gunakan file templat lokal - Unggah AWS CloudFormation templat atau file konfigurasi Terraform tar.gz dari drive lokal.
     - Gunakan URL Amazon S3 - Tentukan URL yang mengarah ke AWS CloudFormation templat atau file konfigurasi Terraform tar.gz yang disimpan di Amazon S3. Jika Anda menentukan URL Amazon S3, URL tersebut harus dimulai dengan `https://`.
     - Gunakan repositori eksternal - Tentukan repositori kode GitHub, GitHub Enterprise, atau Bitbucket Anda. AWS Service Catalogmemungkinkan Anda untuk menyinkronkan produk

ke file template. Untuk produk Terraform, format file template harus berupa satu file yang diarsipkan dalam Tar dan dikompresi dalam Gzip.

- Gunakan CloudFormation tumpukan yang ada - Masukkan ARN untuk tumpukan yang ada CloudFormation . Metode ini tidak mendukung produk Terraform Cloud atau Eksternal.

- Nama versi (opsional) - Nama versi produk (misalnya, “v1", “v2beta”). Tidak ada spasi yang diizinkan.
- Deskripsi (opsional) — Deskripsi versi produk, termasuk bagaimana versi ini berbeda dari versi lainnya.
- Panduan - Dikelola di tab versi pada halaman Detail Produk. Bila versi produk dibuat—selama alur kerja create produk—panduan untuk versi tersebut disetel ke default. Untuk mempelajari panduan selengkapnya, lihat Mengelola Versi.

5. Detail Support mengidentifikasi organisasi dalam perusahaan Anda, dan menyediakan titik kontak untuk dukungan. Masukkan yang berikut ini:

   - Kontak email (opsional) – Alamat email untuk melaporkan masalah dengan produk.
   - Support Link (opsional) — URL ke situs tempat pengguna dapat menemukan informasi dukungan atau tiket file. URL harus dimulai dengan `http://` atau `https://`. Administrator bertanggung jawab untuk menjaga keakuratan dan akses informasi dukungan.
   - Deskripsi Support (opsional) - Deskripsi tentang bagaimana Anda harus menggunakan kontak Email dan tautan Support.

6. Kelola tag (opsional) — Selain menggunakan tag untuk mengkategorikan sumber daya Anda, Anda juga dapat menggunakannya untuk mengautentikasi izin Anda untuk membuat sumber daya ini.
7. Buat produk — Setelah Anda mengisi formulir, pilih Buat produk. Setelah beberapa detik, produk muncul di halaman daftar Produk. Mungkin Anda perlu menyegarkan peramban untuk melihat produk.

Anda juga dapat menggunakan CodePipeline untuk membuat dan mengonfigurasi pipeline untuk menyebarkan template produk Anda AWS Service Catalog dan mengirimkan perubahan yang telah Anda buat di repositori sumber Anda. Untuk informasi selengkapnya, lihat Tutorial: Buat Alur yang Men-deploy ke AWS Service Catalog.

Anda dapat menentukan properti parameter di template AWS CloudFormation atau Terraform Anda dan menerapkan aturan tersebut selama penyediaan. Properti ini dapat menentukan panjang minimum dan maksimum, nilai minimum dan maksimum, nilai yang diizinkan, dan ekspresi reguler

untuk nilai tersebut. AWS Service Catalogmengeluarkan peringatan selama penyediaan jika nilai yang diberikan tidak mematuhi properti parameter. Untuk mempelajari lebih lanjut tentang properti parameter, lihat Parameter di Panduan AWS CloudFormation Pengguna.

Memecahkan masalah

Anda harus memiliki izin untuk mengambil objek dari ember Amazon S3. Jika tidak, Anda mungkin mengalami kesalahan berikut saat meluncurkan atau memperbarui produk.

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

Jika Anda menemukan pesan ini, pastikan memiliki izin untuk mengambil objek dari bucket berikut:

- Ember tempat templat artefak penyediaan disimpan.
- Ember yang dimulai dengan "cf-templates-*" dan tempat AWS Service Catalog menyimpan templat artefak penyediaan.
- Bucket internal yang dimulai dengan "sc-*" dan tempat AWS Service Catalog menyimpan metadata. Anda tidak akan dapat melihat bucket ini dari akun Anda.

Kebijakan contoh berikut menunjukkan izin minimum yang diperlukan untuk mengambil objek dari bucket yang disebutkan sebelumnya.

```
{
          "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-*/*"
          ]
      }
```

Menambahkan produk ke portofolio

Anda dapat menambahkan produk ke sejumlah portofolio. Ketika produk diperbarui, semua portofolio (termasuk portofolio bersama) yang berisi produk secara otomatis menerima versi baru.

Menambahkan produk dari katalog Anda ke portofolio

1. Arahkan ke halaman daftar Produk.
2. Pilih produk, lalu pilih Tindakan. Dari menu dropdown, pilih Tambahkan produk ke portofolio. Anda diarahkan ke halaman Tambahkan ***name-of-product***ke portofolio.
3. Pilih portofolio, lalu pilih Tambahkan produk ke portofolio.

Saat menambahkan produk Terraform ke portofolio, produk memerlukan batasan peluncuran. Anda harus memilih peran IAM dari akun Anda, memasukkan ARN peran IAM, atau memasukkan nama peran. Jika Anda menentukan nama peran dan jika akun menggunakan batasan peluncuran, akun akan menggunakan nama tersebut untuk peran IAM. Ini memungkinkan batasan peran peluncuran menjadi agnostik akun, memastikan Anda dapat membuat lebih sedikit sumber daya per akun bersama. Untuk detail dan instruksi, tinjau Langkah 6: Tambahkan batasan Peluncuran ke produk Terraform Anda

Portofolio dapat berisi banyak produk yang merupakan campuran AWS CloudFormation dan jenis produk Terraform.

Memperbarui produk

Ketika Anda memperbarui template produk, Anda membuat versi baru dari produk. Versi produk baru secara otomatis tersedia untuk semua pengguna yang memiliki akses ke portofolio yang berisi produk.

> **Note**
>
> Saat memperbarui produk yang ada, Anda tidak dapat mengubah jenis produk (AWS CloudFormationatau Teraform). Misalnya, jika Anda memperbarui AWS CloudFormation produk, Anda tidak dapat mengganti AWS CloudFormation template yang ada dengan file konfigurasi Terraform tar.gz. Anda harus memperbarui file AWS CloudFormation template yang ada dengan file AWS CloudFormation template baru.

Pengguna akhir yang saat ini menjalankan produk yang disediakan dari versi produk sebelumnya dapat memperbarui produk yang disediakan ke versi baru. Ketika versi baru produk tersedia, pengguna dapat menggunakan perintah Perbarui produk yang disediakan pada daftar produk yang disediakan atau halaman detail produk yang disediakan.

Sebelum Anda membuat versi baru suatu produk, AWS Service Catalog sarankan Anda menguji pembaruan produk Anda di AWS CloudFormation atau di mesin Terraform untuk memastikan bahwa mereka berfungsi dengan baik.

Untuk membuat versi produk baru

1. Arahkan ke halaman daftar Produk.
2. Pilih produk produk yang ingin Anda perbarui. Anda diarahkan ke halaman Detail Produk.
3. Pada halaman Detail produk, buka tab Versi, lalu pilih Buat versi baru.
4. Di bawah Detail versi, lakukan hal berikut:

   - Pilih template — Ada empat cara untuk menambahkan file template.

     Gunakan file templat lokal - Unggah AWS CloudFormation templat atau file konfigurasi Terraform tar.gz dari drive lokal.

     Gunakan URL Amazon S3 - Tentukan URL yang mengarah ke AWS CloudFormation templat atau file konfigurasi Terraform tar.gz yang disimpan di Amazon S3. Jika Anda menentukan URL Amazon S3, itu harus dimulai dengan https://.

     Gunakan repositori eksternal - Tentukan repositori kode GitHub, GitHub Enterprise, atau Bitbucket Anda. AWS Service Catalogmemungkinkan Anda untuk menyinkronkan produk ke file template. Untuk produk Terraform, format file template harus berupa satu file yang diarsipkan dalam Tar dan dikompresi dalam Gzip.

     Gunakan CloudFormation tumpukan yang ada - Masukkan ARN untuk tumpukan yang ada CloudFormation . Metode ini tidak mendukung produk Terraform Cloud atau Eksternal.
   - Judul versi — Nama versi produk (misalnya, “v1", “v2beta”). Spasi tidak diperbolehkan.
   - Deskripsi (opsional) — Deskripsi versi produk, termasuk bagaimana versi ini berbeda dari versi sebelumnya.
5. Pilih Buat versi produk.

Anda juga dapat menggunakan CodePipeline untuk membuat dan mengonfigurasi pipeline untuk menerapkan template produk AndaAWS Service Catalog, dan mengirimkan perubahan di repositori sumber Anda. Untuk informasi selengkapnya, lihat Tutorial: Buat Alur yang Men-deploy ke AWS Service Catalog.

Menyinkronkan produk ke file template dari GitHub, GitHub Enterprise, atau Bitbucket

AWS Service Catalog memungkinkan Anda untuk menyinkronkan produk ke file template yang dikelola melalui penyedia repositori eksternal. AWS Service Catalog mengacu pada produk dengan jenis koneksi template ini sebagai produk yang disinkronkan dengan GIT. Opsi repositori termasuk GitHub, GitHub Enterprise, atau Bitbucket. Setelah Anda mengotorisasi akun repositori eksternal, Anda dapat membuat AWS Service Catalog produk baru atau memperbarui produk yang ada untuk disinkronkan ke file templat di repositori. Akun AWS Ketika perubahan dilakukan pada file template dan dilakukan dalam repositori (misalnya, menggunakan git-push), AWS Service Catalog secara otomatis mendeteksi perubahan dan membuat versi produk baru (artefak).

Topik

Izin yang diperlukan untuk menyinkronkan produk ke file template eksternal

Anda dapat menggunakan kebijakan berikut AWS Identity and Access Management (IAM) sebagai templat untuk memungkinkan AWS Service Catalog administrator menyinkronkan produk ke file templat dari repositori eksternal. Kebijakan ini mencakup izin yang diperlukan dari keduanya CodeConnections dan AWS Service Catalog. AWS Service Catalog merekomendasikan agar Anda menyalin kebijakan templat di bawah ini, dan juga menggunakan kebijakan AWS Service Catalog `AWSServiceCatalogAdminFullAccess` terkelola saat mengaktifkan produk yang disinkronkan dengan repositori.

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

Buat koneksi akun

Sebelum menyinkronkan file template ke AWS Service Catalog produk, Anda harus membuat dan mengotorisasi koneksi satu kali. account-to-account Anda menggunakan koneksi ini untuk menentukan detail repositori yang berisi file template yang diinginkan. Anda dapat membuat koneksi menggunakan AWS Service Catalog konsol, CodeConnections konsol, AWS Command Line Interface (CLI), atau CodeConnections API.

Setelah membuat koneksi, Anda dapat menggunakan AWS Service Catalog konsol, AWS Service Catalog API, atau CLI untuk membuat produk yang disinkronkan AWS Service Catalog . AWS Service Catalog administrator dapat membuat produk baru atau memperbarui AWS Service Catalog

produk yang ada berdasarkan file template di repositori dan cabang. Jika perubahan dilakukan di repositori, AWS Service Catalog secara otomatis mendeteksi perubahan dan membuat versi produk baru. Versi produk sebelumnya dipertahankan hingga batas versi yang ditentukan dan diberi status usang.

Selain itu, AWS Service Catalog secara otomatis membuat peran terkait layanan (SLR) setelah koneksi dibuat. SLR ini memungkinkan AWS Service Catalog untuk mendeteksi setiap perubahan file template yang berkomitmen ke repositori. SLR juga memungkinkan AWS Service Catalog untuk secara otomatis membuat versi produk baru untuk produk yang disinkronkan. Untuk informasi selengkapnya tentang izin dan fungsionalitas SLR, lihat Peran terkait layanan untuk. AWS Service Catalog

Untuk membuat produk baru yang disinkronkan dengan GIT

1. Di panel navigasi kiri, pilih Daftar produk, lalu pilih Buat produk.
2. Masukkan detail Produk.
3. Di Detail versi, pilih Tentukan repositori kode Anda menggunakan AWS CodeStar penyedia, lalu pilih tautan Buat AWS CodeStar koneksi baru.
4. Setelah Anda membuat koneksi, segarkan daftar koneksi, lalu pilih koneksi baru. Tentukan detail repositori, termasuk jalur file repositori, cabang, dan templat.

   Untuk informasi tentang penggunaan file konfigurasi Terraform, lihat. Menyinkronkan produk Terraform ke file template dari GitHub, GitHub Enterprise, atau Bitbucket

   a. (Opsional saat membuat sumber daya AWS Service Catalog produk baru) Di bagian Detail Dukungan, tambahkan metadata untuk produk.

   b. (Opsional saat membuat sumber daya AWS Service Catalog produk baru) Di bagian Tag, pilih Tambahkan tag baru dan masukkan pasangan Kunci dan Nilai.
5. Pilih Buat produk baru.

Untuk membuat beberapa produk yang disinkronkan dengan GIT

1. Di panel navigasi kiri AWS Service Catalog konsol, pilih Daftar produk, lalu pilih Buat beberapa produk yang dikelola oleh git.
2. Masukkan detail produk umum.
3. Di detail repositori eksternal, pilih AWS CodeStar koneksi, lalu tentukan repositori dan cabang.

4. Di panel Tambahkan produk, masukkan jalur file Template dan Nama produk. Pilih Tambahkan item baru dan lanjutkan menambahkan produk sesuai keinginan.
5. Setelah menambahkan semua produk yang diinginkan, pilih Massal membuat produk.

Untuk menghubungkan AWS Service Catalog produk yang ada ke repositori eksternal

1. Di panel navigasi kiri AWS Service Catalog konsol, pilih Daftar produk, lalu pilih Connect products to an external repository.
2. Pada halaman Pilih produk, pilih produk yang ingin Anda sambungkan ke repositori eksternal, lalu pilih Berikutnya.
3. Pada halaman Tentukan detail sumber, pilih AWS CodeStar koneksi yang ada, lalu tentukan repositori, cabang, dan jalur file templat.
4. Pilih Berikutnya.
5. Pada halaman Tinjau dan kirim, verifikasi detail koneksi, lalu pilih Connect products ke repositori eksternal.

Melihat koneksi produk yang disinkronkan dengan Git

Anda dapat menggunakan AWS Service Catalog konsol, API, atau AWS CLI untuk melihat detail koneksi repositori. Untuk AWS Service Catalog produk yang ditautkan ke file template, Anda dapat mengambil informasi tentang koneksi repositori dan terakhir kali template disinkronkan dengan produk dari Status Sinkronisasi Terakhir.

> **Note**
>
> Anda dapat melihat informasi repositori dan Status Sinkronisasi Terakhir di tingkat produk. Pengguna harus memiliki izin IAM di CodeConnections API untuk melihat detail repositori. Lihat Izin yang diperlukan untuk menyinkronkan AWS Service Catalog produk ke file templat untuk informasi selengkapnya tentang kebijakan yang diperlukan untuk izin IAM ini.

Untuk melihat detail koneksi dan repositori menggunakan AWS Management Console

1. Di panel navigasi kiri, pilih Daftar produk.
2. Pilih produk dari daftar.
3. Pada halaman Produk, navigasikan ke bagian Detail sumber produk.

4. Untuk melihat ID revisi sumber untuk versi produk, pilih tautan Versi terakhir yang dibuat. Bagian Detail versi menampilkan ID revisi sumber.

Untuk melihat detail koneksi dan repositori menggunakan AWS CLI

Dari AWS CLI, jalankan perintah berikut:

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

$ aws servicecatalog describe-provisioning-artifact

$ aws servicecatalog search-product-as-admin

$ aws servicecatalog list-provisioning-artifacts
```

Memperbarui koneksi produk yang disinkronkan dengan Git

Anda dapat memperbarui koneksi akun yang ada dan produk yang disinkronkan dengan GIT menggunakan AWS Service Catalog konsol, AWS Service Catalog API, atau. AWS CLI

Untuk mempelajari cara menghubungkan AWS Service Catalog produk yang sudah ada ke file template, lihat Membuat koneksi produk baru yang disinkronkan dengan GIT.

Untuk memperbarui produk yang ada ke produk yang disinkronkan dengan GIT

1. Di panel navigasi kiri, pilih Daftar produk, lalu pilih salah satu opsi berikut:
   - Untuk memperbarui satu produk, pilih produk, navigasikan ke bagian Detail sumber produk, lalu pilih Edit detail.
   - Untuk memperbarui beberapa produk, pilih Connect products ke repositori eksternal, pilih hingga sepuluh produk, lalu pilih Next.
2. Di bagian Detail sumber produk, lakukan pembaruan berikut:
   - Tentukan koneksi.
   - Tentukan repositori.
   - Tentukan cabang.
   - Beri nama file template.
3. Pilih Simpan perubahan.

> **Note**
>
> Untuk produk yang belum terhubung ke repositori eksternal, Anda dapat menggunakan opsi Connect to an external repository yang ditampilkan di peringatan di bagian atas halaman info produk setelah memilih produk.

Anda juga dapat menggunakan AWS Service Catalog konsol atau AWS CLI to

- Connect AWS Service Catalog produk yang sudah ada ke file template di repositori eksternal
- Perbarui metadata produk, termasuk nama produk, deskripsi, dan tag.
- Konfigurasi ulang (perbarui sinkronisasi untuk menggunakan sumber repositori yang berbeda) koneksi untuk produk yang terhubung sebelumnya. AWS Service Catalog

Untuk memperbarui detail koneksi dan repositori menggunakan konsol AWS Service Catalog

1. Di panel navigasi kiri AWS Service Catalog konsol, pilih Daftar produk, lalu pilih produk yang saat ini terhubung ke repositori eksternal.
2. Di bagian Detail sumber produk, pilih Edit sumber produk.
3. Di bagian Detail sumber produk, tentukan repositori baru yang diinginkan.
4. Pilih Simpan perubahan.

Untuk memperbarui koneksi dan detail repositori menggunakan AWS CLI

Dari AWS CLI run the `$ aws servicecatalog update-product` and `$ aws servicecatalog update-provisioning-artifact` command.

Menghapus koneksi produk yang disinkronkan dengan Git

Anda dapat menghapus koneksi antara AWS Service Catalog produk dan file template menggunakan AWS Service Catalog konsol, CodeConnections API, atau file AWS CLI. Saat Anda memutuskan sambungan produk dari file templat, produk yang disinkronkan akan beralih ke AWS Service Catalog produk yang dikelola secara teratur. Setelah memutuskan sambungan produk, jika file template diubah dan dilakukan di repositori yang terhubung sebelumnya, perubahan tidak tercermin. Untuk menghubungkan kembali AWS Service Catalog produk ke file template di repositori eksternal, lihat Memperbarui koneksi dan produk yang disinkronkan. AWS Service Catalog

Untuk memutuskan sambungan produk yang disinkronkan dengan GIT menggunakan konsol AWS Service Catalog

1. Dalam AWS Management Console, pilih Daftar produk dari panel navigasi kiri.
2. Pilih produk dari daftar.
3. Pada halaman Produk, navigasikan ke bagian Detail sumber produk.
4. Pilih Putuskan sambungan.
5. Konfirmasikan tindakan, lalu pilih Putuskan sambungan.

Untuk memutuskan sambungan produk yang disinkronkan dengan GIT menggunakan AWS CLI

Dari AWS CLI, jalankan `$ aws servicecatalog update-product` perintah. Dalam `ConnectionParameters` input, hapus koneksi yang ditentukan.

Untuk menghapus koneksi menggunakan CodeConnections API atau AWS CLI

Di CodeConnections API atau AWS CLI, jalankan `$ aws codestar-connections delete-connection` perintah.

Menyinkronkan produk Terraform ke file template dari GitHub, GitHub Enterprise, atau Bitbucket

Saat membuat produk yang disinkronkan GIT menggunakan file konfigurasi Terraform, jalur file hanya menerima format tar.gz. Format folder Terraform tidak diterima di jalur file.

Wilayah AWS dukungan untuk produk yang disinkronkan dengan GIT

AWS Service Catalog mendukung produtcs yang disinkronkan GIT Wilayah AWS seperti yang ditunjukkan pada tabel di bawah ini.

Wilayah AWS nama	Wilayah AWS identitas	Support untuk produk yang disinkron kan dengan GIT
AS Timur (Virginia Utara)	us-east-1	Ya
US East (Ohio)	us-east-2	Ya
US West (N. California)	us-west-1	Ya

Wilayah AWS nama	Wilayah AWS identitas	Support untuk produk yang disinkron kan dengan GIT
US West (Oregon)	us-west-2	Ya
Afrika (Cape Town)	af-south-1	Tidak
Asia Pasifik (Hong Kong)	ap-east-1	Tidak
Asia Pasifik (Jakarta)	ap-southeast-3	Tidak
Asia Pasifik (Mumbai)	ap-south-1	Ya
Asia Pacific (Osaka)	ap-northeast-3	Tidak
Asia Pasifik (Seoul)	ap-northeast-2	Ya
Asia Pacific (Singapore)	ap-southeast-1	Ya
Asia Pacific (Sydney)	ap-southeast-2	Ya
Asia Pacific (Tokyo)	ap-northeast-1	Ya
Canada (Central)	ca-sentral-1	Ya
Eropa (Frankfurt)	eu-central-1	Ya
Eropa (Irlandia)	eu-west-1	Ya
Eropa (London)	eu-west-2	Ya
Eropa (Milan)	eu-south-1	Tidak
Eropa (Paris)	eu-west-3	Ya
Eropa (Stockholm)	eu-north-1	Ya
Timur Tengah (Bahrain)	me-south-1	Tidak
Amerika Selatan (Sao Paulo)	sa-east-1	Ya

Wilayah AWS nama	Wilayah AWS identitas	Support untuk produk yang disinkron kan dengan GIT
AWS GovCloud (AS-Timur)	us-gov-east-1	Tidak
AWS GovCloud (AS-Barat)	us-gov-west-1	Tidak

Menghapus produk

Saat Anda menghapus produk, AWS Service Catalog hapus semua versi produk dari setiap portofolio yang berisi produk.

AWS Service Catalogmemungkinkan Anda untuk menghapus produk menggunakan AWS Service Catalog konsol atauAWS CLI. Agar berhasil menghapus produk, Anda harus memisahkan semua sumber daya yang terkait dengan produk terlebih dahulu. Contoh asosiasi sumber daya produk termasuk asosiasi portofolio, anggaran TagOptions, dan Tindakan Layanan.

> **Important**
>
> Anda tidak dapat memulihkan produk setelah dihapus.

Untuk menghapus produk menggunakan AWS Service Catalog konsol

1. Arahkan ke halaman Portofolio dan pilih portofolio yang berisi produk yang ingin Anda hapus.
2. Pilih produk yang ingin Anda hapus, lalu pilih Hapus di kanan atas panel produk.
3. Untuk produk tanpa sumber daya terkait, konfirmasikan produk yang ingin Anda hapus dengan memasukkan hapus di kotak teks, lalu pilih Hapus.

   Untuk produk dengan sumber daya terkait, lanjutkan ke langkah 4.
4. Di jendela Hapus produk, tinjau tabel Asosiasi, yang menampilkan semua sumber daya terkait produk. AWS Service Catalogmencoba untuk memisahkan sumber daya ini saat Anda menghapus produk.
5. Konfirmasikan bahwa Anda ingin menghapus produk dan menghapus semua sumber daya terkait dengan memasukkan hapus di kotak teks.
6. Pilih Putuskan dan hapus.

Jika AWS Service Catalog tidak dapat memisahkan semua sumber daya produk, produk tidak dihapus. Jendela Delete product menampilkan jumlah disasosiasi yang gagal dan deskripsi untuk setiap kegagalan. Untuk informasi selengkapnya tentang menyelesaikan disasosiasi sumber daya yang gagal saat menghapus produk, lihat Menyelesaikan disasosiasi sumber daya yang gagal saat menghapus produk di bawah ini.

Topik

- Menghapus produk menggunakan AWS CLI
- Menyelesaikan disasosiasi sumber daya yang gagal saat menghapus produk

Menghapus produk menggunakan AWS CLI

AWS Service Catalogmemungkinkan Anda menggunakan AWS Command Line Interface(AWS CLI) untuk menghapus produk dari portofolio Anda. AWS CLIIni adalah alat open source yang memungkinkan Anda berinteraksi dengan AWS layanan menggunakan perintah di shell baris perintah Anda. Fungsi AWS Service Catalog force-delete memerlukan AWS CLIalias, yang merupakan pintasan yang dapat Anda buat AWS CLI untuk mempersingkat perintah atau skrip yang sering Anda gunakan.

Prasyarat

- Instal dan konfigurasikan AWS CLI. Untuk informasi selengkapnya, lihat Menginstal atau memperbarui versi terbaru dari dasar-dasar Konfigurasi AWS CLI dan. Gunakan AWS CLI versi minimum 1.11.24 atau 2.0.0.
- Alias CLI produk hapus memerlukan terminal yang kompatibel dengan bass dan prosesor JSON baris perintah JQ. Untuk informasi selengkapnya tentang menginstal prosesor JSON baris perintah, lihat Download jq.
- Buat AWS CLI Alias untuk mengumpulkan panggilan `Disassociation` API, memungkinkan Anda menghapus produk dalam satu perintah.

Agar berhasil menghapus produk, Anda harus memisahkan semua sumber daya yang terkait dengan produk terlebih dahulu. Contoh asosiasi sumber daya produk termasuk asosiasi portofolio, anggaran, Opsi Tag, dan Tindakan Layanan. Saat menggunakan CLI untuk menghapus produk, `force-delete-product` alias CLI memungkinkan Anda memanggil API untuk memisahkan sumber daya apa pun yang akan mencegah `Disassociate` API. `DeleteProduct` Ini menghindari panggilan terpisah untuk disasosiasi individu.

> **Note**
>
> Jalur file yang ditunjukkan dalam prosedur di bawah ini dapat bervariasi tergantung pada sistem operasi yang Anda gunakan untuk melakukan tindakan ini.

Membuat AWS CLI alias untuk menghapus produk AWS Service Catalog

Saat menggunakan AWS CLI untuk menghapus AWS Service Catalog produk, `force-delete-product` alias CLI memungkinkan Anda memanggil `Disassociate` API untuk memisahkan sumber daya apa pun yang akan mencegah panggilan. `DeleteProduct`

Buat **`alias`** file di folder AWS CLI konfigurasi Anda

1. Di AWS CLI konsol, arahkan ke folder configuraiton. Secara default, jalur folder konfigurasi ada `~/.aws/` di Linux dan macOS, atau `%USERPROFILE%\.aws\` di Windows.
2. Buat sub-folder bernama `cli` menggunakan navigasi file atau dengan memasukkan perintah berikut di terminal pilihan Anda:

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

   Jalur default `cli` folder yang dihasilkan ada `~/.aws/cli/` di Linux dan macOS, atau `%USERPROFILE%\.aws\cli` di Windows.
3. Di `cli` folder baru, buat file teks bernama `alias` tanpa ekstensi file. Anda dapat membuat `alias` file menggunakan navigasi file atau dengan memasukkan perintah berikut di terminal pilihan Anda:

   ```
   $ touch ~/.aws/cli/alias
   ```
4. Masukkan `[toplevel]` pada baris pertama.
5. Simpan file tersebut.

Selanjutnya, Anda dapat menambahkan force-delete-product alias ke `alias` file Anda dengan menempelkan skrip alias secara manual ke dalam file, atau dengan menggunakan perintah di jendela terminal.

Tambahkan force-delete-product alias ke file Anda **`alias`** secara manual

1. Di AWS CLI konsol, navigasikan ke folder AWS CLI konfigurasi Anda dan buka `alias` file.
2. Masukkan alias kode berikut ke dalam file, di bawah `[toplevel]` baris:

```
            [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. Simpan file tersebut.

Gunakan jendela terminal untuk menambahkan force-delete-product alias ke file Anda **`alias`**

1. Buka jendela terminal Anda dan jalankan perintah berikut

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

2. Tempel skrip alias ke jendela terminal, lalu tekan CTRL+D untuk keluar dari perintah. `cat`

Panggil force-delete-product alias

1. Di jendela terminal Anda, jalankan perintah berikut untuk memanggil alias delete product

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

   Contoh di bawah ini menunjukkan perintah `force-delete-product` alias dan respons yang dihasilkan

   ```
   $ 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. Masukkan y untuk mengonfirmasi bahwa Anda ingin menghapus produk.

Setelah berhasil menghapus produk, jendela terminal menampilkan hasil berikut

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

Sumber daya tambahan

Untuk informasi selengkapnya tentangAWS CLI, menggunakan alias, dan menghapus AWS Service Catalog produk, tinjau sumber daya berikut:

- Membuat dan menggunakan AWS CLI alias dalam panduan pengguna AWS Command Line Interface(CLI).
- AWS CLIrepositori alias repositori git.
- Menghapus AWS Service Catalog produk.
- AWSRe: Invent 2016: Pengguna yang Efektif AWS CLI di. YouTube

Menyelesaikan disasosiasi sumber daya yang gagal saat menghapus produk

Jika upaya Anda sebelumnya untuk menghapus produk gagal karena pengecualian disasosiasi sumber daya, tinjau daftar pengecualian dan resolusinya di bawah ini.

> **Note**
>
> Jika Anda menutup jendela Menghapus produk sebelum menerima pesan pemutusan sumber daya yang gagal, Anda dapat mengikuti langkah satu hingga tiga di bagian Hapus produk untuk membuka jendela lagi.

Untuk mengatasi pemisahan sumber daya yang gagal

Di jendela Hapus produk, tinjau kolom Status tabel Asosiasi. Identifikasi pengecualian pemisahan sumber daya yang gagal dan resolusi yang disarankan:

Jenis pengecualian status	Penyebab	Penyelesaian
Produk prod-****	AWS Service Catalogti dak dapat menghapus produk karena produk masih terkait TagOption s, anggaran, setidakny a satu `Provision ingArtifact`	Cobalah untuk menghapus produk lagi.

Jenis pengecualian status	Penyebab	Penyelesaian
	dengan tindakan terkait, produk masih ditetapkan ke Portofolio, produk memiliki pengguna, atau produk memiliki kendala.	
Pengguna: `username` tidak berwenang untuk melakukan:	Pengguna yang mencoba menghapus produk tidak memiliki izin yang diperlukan untuk memisahkan sumber daya produk.	AWS Service Catalogmerekomendasikan untuk menghubungi administrator akun Anda untuk informasi selengkapnya tentang pemutusan sumber daya produk yang saat ini tidak memiliki izin untuk memisahkan diri.

Mengelola Versi

Anda menetapkan versi produk ketika Anda membuat produk, dan Anda dapat memperbarui versi produk setiap saat.

Versi memiliki templat AWS CloudFormation, judul, deskripsi, status, dan panduan.

Status Versi

Versi dapat memiliki salah satu dari tiga status:

- Aktif - Versi aktif muncul dalam daftar versi dan mengizinkan pengguna untuk meluncurkannya.
- Tidak aktif - Versi tidak aktif tersembunyi dari daftar versi. Produk yang sudah tersedia yang diluncurkan dari versi ini tidak akan terpengaruh.
- Dihapus - Versi yang dihapus dihapus dari daftar versi. Menghapus versi tidak dapat dibatalkan.

Panduan Versi

Anda dapat mengatur panduan versi untuk menyediakan informasi kepada pengguna akhir tentang versi produk. Panduan versi hanya mempengaruhi versi produk yang aktif.

Ada dua opsi untuk panduan versi:

- Tidak ada - Secara default, versi produk tidak memiliki panduan apa pun. Pengguna akhir dapat menggunakan versi tersebut untuk memperbarui dan meluncurkan produk yang disediakan.
- Usang - Pengguna tidak dapat meluncurkan produk baru yang disediakan menggunakan versi produk yang tidak digunakan lagi. Jika produk yang disediakan p yang diluncurkan sebelumnya menggunakan versi yang sekarang tidak digunakan lagi, pengguna hanya dapat memperbarui produk yang disediakan tersebut menggunakan versi yang ada atau versi baru.

Memperbarui Versi

Anda menetapkan versi produk saat membuat sebuah produk, dan juga dapat memperbarui versi kapan pun. Untuk informasi selengkapnya tentang pembuatan produk, lihat Membuat Produk.

Untuk memperbarui versi produk

1. Di dalam konsol AWS Service Catalog, pilih Produk.
2. Dari daftar produk, pilih produk yang ingin Anda perbarui versinya.
3. Pada halaman Detail Produk, pilih tab Versi, lalu pilih versi yang ingin Anda perbarui.
4. Pada halaman Detail versi, edit versi produk, lalu pilih Simpan perubahan.

Menggunakan Batasan AWS Service Catalog

Anda menerapkan batasan untuk mengontrol aturan yang diterapkan ke produk dalam portofolio tertentu ketika pengguna akhir meluncurkannya. Ketika pengguna akhir meluncurkan produk, mereka akan melihat aturan yang telah Anda terapkan menggunakan batasan. Anda dapat menerapkan batasan untuk sebuah produk setelah dimasukkan ke dalam portofolio. Batasan akan aktif segera setelah Anda membuatnya, dan batasan tersebut diterapkan ke semua versi terbaru dari produk yang belum diluncurkan.

Batasan

- Batasan Peluncuran AWS Service Catalog
- Batasan Notifikasi AWS Service Catalog
- Batasan Pembaruan Tanda AWS Service Catalog
- Batasan Set Tumpukan AWS Service Catalog
- Batasan Templat AWS Service Catalog

Batasan Peluncuran AWS Service Catalog

Batasan peluncuran menentukan peran AWS Identity and Access Management (IAM) yang AWS Service Catalog mengasumsikan saat pengguna akhir meluncurkan, memperbarui, atau menghentikan produk. Peran IAM adalah kumpulan izin yang dapat diasumsikan oleh pengguna atau AWS layanan sementara untuk menggunakan AWS layanan. Untuk contoh pengantar, lihat:

- AWS CloudFormationjenis produk: Langkah 6: Tambahkan batasan peluncuran untuk menetapkan peran IAM
- Jenis produk Terraform Open Source atau Terraform Cloud: Langkah 5: Buat peran peluncuran

Batasan peluncuran berlaku untuk produk dalam portofolio (asosiasi portofolio produk). Batasan peluncuran tidak berlaku pada tingkat portofolio atau produk di semua portofolio. Untuk mengaitkan batasan peluncuran dengan semua produk dalam portofolio, Anda harus menerapkan batasan peluncuran untuk setiap produk satu per satu.

Tanpa batasan peluncuran, pengguna akhir harus meluncurkan dan mengelola produk menggunakan kredensial IAM mereka sendiri. Untuk melakukannya, mereka harus memiliki izin untuk AWS CloudFormation, layanan AWS yang digunakan oleh produk, dan AWS Service Catalog. Dengan menggunakan peran peluncuran, Anda dapat membatasi izin pengguna akhir seminimal mungkin yang mereka butuhkan untuk produk tersebut. Untuk informasi selengkapnya tentang izin pengguna akhir, lihat Manajemen Identitas dan Akses di AWS Service Catalog.

Untuk membuat dan menetapkan IAM role, Anda harus memiliki izin administratif IAM berikut:

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

Mengonfigurasi Peran Peluncuran

Peran IAM yang Anda tetapkan ke produk sebagai kendala peluncuran harus memiliki izin untuk menggunakan yang berikut:

Untuk produk Cloudformation

- Kebijakan yang `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess` AWS CloudFormation dikelola
- Layanan dalam templat AWS CloudFormation untuk produk
- Baca akses ke AWS CloudFormation template dalam bucket Amazon S3 milik layanan.

Untuk produk Terraform

- Layanan dalam template Amazon S3 untuk produk
- Baca akses ke template Amazon S3 dalam bucket Amazon S3 milik layanan.
- `resource-groups:Tag`untuk menandai instans Amazon EC2 (diasumsikan oleh mesin penyediaan Terraform saat melakukan operasi penyediaan)
- `resource-groups:CreateGroup`untuk penandaan grup sumber daya (diasumsikan oleh AWS Service Catalog untuk membuat grup sumber daya dan menetapkan tag)

Kebijakan kepercayaan peran IAM harus memungkinkan AWS Service Catalog untuk mengambil peran tersebut. Pada prosedur di bawah ini, kebijakan kepercayaan akan disetel secara otomatis saat Anda memilih AWS Service Catalog sebagai tipe peran. Jika Anda tidak menggunakan konsol, lihat bagian Membuat kebijakan kepercayaan untuk AWS layanan yang mengambil peran dalam Cara menggunakan kebijakan kepercayaan dengan peran IAM.

> **Note**
>
> Izin `servicecatalog:ProvisionProduct`, `servicecatalog:TerminateProvisionedProduct`, dan `servicecatalog:UpdateProvisionedProduct` tidak dapat ditetapkan dalam peran peluncuran. Anda harus menggunakan peran IAM, seperti yang ditunjukkan dalam langkah-langkah kebijakan sebaris di bagian Memberikan Izin kepada AWS Service Catalog Pengguna Akhir.

> **Note**
>
> Untuk melihat produk dan sumber daya Cloudformation yang disediakan di AWS Service Catalog konsol, pengguna akhir memerlukan akses baca. AWS CloudFormation Melihat produk dan sumber daya yang disediakan di konsol tidak menggunakan peran peluncuran.

Untuk membuat peran peluncuran

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.

   Produk Terraform memerlukan konfigurasi peran peluncuran tambahan. Untuk informasi lebih lanjut, tinjau Langkah 5: Buat peran peluncuran di Memulai dengan produk Terraform Open Source.
2. Pilih Peran.
3. Pilih Buat Peran Baru.
4. Masukkan nama peran dan pilih Langkah Selanjutnya.
5. Di bawah Peran Layanan AWS di samping AWS Service Catalog, pilih Pilih.
6. Pada halaman Lampirkan Kebijakan, pilih Langkah Selanjutnya.
7. Untuk membuat peran, pilih Buat Peran.

Untuk melampirkan kebijakan ke peran baru

1. Pada halaman peran yang telah Anda buat untuk melihat halaman detail perannya.
2. Pilih tab Izin, dan perluas bagian Kebijakan Sebaris. Lalu, pilih klik di sini.
3. Pilih Kebijakan Kustom, lalu pilih Pilihan.
4. Masukkan nama untuk kebijakan, lalu tempelkan bagian berikut ke bagian editor Dokumen Kebijakan:

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

> **Note**
>
> Saat Anda mengonfigurasi peran peluncuran untuk batasan peluncuran, Anda harus menggunakan string ini:. `"s3:ExistingObjectTag/servicecatalog:provisioning":"true"`

5. Tambahkan baris ke kebijakan untuk setiap layanan tambahan yang digunakan oleh produk. Misalnya, untuk menambahkan izin untuk Amazon Relational Database Service (Amazon RDS), masukkan koma pada akhir baris terakhir pada daftar `Action`, lalu tambahkan baris berikut:

```
"rds:*"
```

6. Pilih Terapkan Kebijakan.

Menerapkan Batasan Peluncuran

Setelah Anda mengonfigurasi peran peluncuran, tetapkan peran ke produk sebagai batasan peluncuran. Tindakan ini memberitahu AWS Service Catalog untuk mengambil peran saat pengguna akhir meluncurkan produk.

Menetapkan peran ke sebuah produk

1. Buka konsol Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Pilih portofolio yang berisi produk.
3. Pilih tab Batasan dan pilih Buat batasan.
4. Pilih produk dari Produk lalu pilih Luncurkan di Tipe batasan. Pilih Lanjutkan.
5. Di bagian Batasan peluncuran, Anda dapat memilih IAM role dari akun Anda dan memasukkan ARN IAM role, atau memasukkan nama peran.

   Jika Anda menetapkan nama peran dan jika akun menggunakan batasan peluncuran, akun akan menggunakan nama tersebut untuk IAM role. Pendekatan ini memungkinkan batasan peran peluncuran menjadi akun agnostik sehingga Anda dapat membuat lebih sedikit sumber daya per akun bersama.

> **Note**
>
> Nama peran yang diberikan harus muncul di akun yang menciptakan batasan peluncurannya dan di akun pengguna yang meluncurkan produk dengan batasan peluncuran ini.

6. Setelah menentukan IAM role, pilih Buat.

Menambahkan Deputi Bingung untuk Meluncurkan Kendala

AWS Service Catalogmendukung perlindungan Deputi Bingung untuk API yang berjalan dengan permintaan Asumsikan Peran. Saat menambahkan batasan peluncuran, Anda dapat membatasi akses peran peluncuran dengan menggunakan `sourceAccount` dan `sourceArn` kondisi dalam kebijakan kepercayaan peran peluncuran. Ini memastikan bahwa peran peluncuran dipanggil oleh sumber tepercaya.

Dalam contoh berikut, AWS Service Catalog pengguna akhir milik akun 111111111111. Saat AWS Service Catalog administrator membuat `LaunchConstraint` untuk produk, pengguna akhir dapat menentukan kondisi berikut dalam kebijakan kepercayaan peran peluncuran untuk membatasi peran yang diasumsikan ke akun 111111111111.

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

}
```

Pengguna yang menyediakan produk dengan produk `LaunchConstraint` harus memiliki yang sama `AccountId` (111111111111). Jika tidak, operasi gagal dengan `AccessDenied` kesalahan, mencegah penyalahgunaan peran peluncuran.

AWS Service CatalogAPI berikut diamankan untuk perlindungan Deputi Bingung:

- `LaunchConstraint`
- `ProvisionProduct`

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

`sourceArn` Perlindungan AWS Service Catalog hanya mendukung ARN templat, seperti "`arn:<aws-partition>:servicecatalog:<region>:<accountId>:`" Itu tidak mendukung ARN sumber daya tertentu.

Memverifikasi Kendala Peluncuran

Untuk memverifikasi AWS Service Catalog penggunaan peran untuk meluncurkan produk dan berhasil menyediakan produk, luncurkan produk dari AWS Service Catalog konsol. Untuk menguji batasan sebelum melepaskannya ke pengguna, buat portofolio uji yang berisi produk yang sama dan uji batasan dengan portofolio tersebut.

Untuk meluncurkan produk

1. Dalam menu untuk konsol AWS Service Catalog, pilih Service Catalog, Pengguna akhir.
2. Pilih produk untuk membuka halaman Detail produk. Di tabel Opsi peluncuran, verifikasi Amazon Resource Name (ARN) dari peran yang muncul.
3. Pilih Luncurkan produk.
4. Lanjutkan melalui langkah-langkah peluncuran, mengisi informasi yang diperlukan.
5. Verifikasi bahwa produk yang dimulai berhasil.

Batasan Notifikasi AWS Service Catalog

> **Note**
>
> AWS Service Catalogtidak mendukung batasan pemberitahuan untuk produk Terraform Open Source atau Terraform Cloud.

Batasan notifikasi menentukan topik Amazon SNS untuk menerima notifikasi tentang peristiwa tumpukan.

Gunakan prosedur berikut untuk membuat topik SNS dan berlangganlah ke topik tersebut.

Untuk membuat topik SNS dan sebuah langganan

1. Buka konsol Amazon SNS di https://console.aws.amazon.com/sns/v3/home.
2. Pilih Buat topik.
3. Ketik nama topik lalu pilih Buat topik.
4. Pilih Buat langganan.
5. Untuk Protokol, pilih Email. Untuk Titik Akhir, ketik alamat email yang bisa Anda gunakan untuk menerima notifikasi. Pilih Buat langganan.
6. Anda akan menerima email konfirmasi dengan baris subjek `AWS Notification - Subscription Confirmation`. Buka email dan ikuti petunjuk untuk menyelesaikan langganan Anda.

Gunakan prosedur berikut untuk menerapkan batasan notifikasi menggunakan topik SNS yang Anda buat menggunakan prosedur sebelumnya.

Untuk menerapkan batasan notifikasi pada sebuah produk

1. Buka konsol Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Pilih portofolio yang berisi produk.
3. Perluas Batasan dan pilih Tambahkan batasan.
4. Pilih produk dari Produk dan atur Tipe batasan ke Notifikasi. Pilih Lanjutkan.
5. Pilih Pilih topik dari akun Anda dan pilih topik SNS yang Anda buat dari Nama topik.
6. Pilih Kirim.

Batasan Pembaruan Tanda AWS Service Catalog

> **Note**
>
> AWS Service Catalogtidak mendukung batasan pembaruan tag untuk produk Terraform Open Source.

Dengan batasan pembaruan tag, AWS Service Catalog administrator dapat mengizinkan atau melarang pengguna akhir memperbarui tag pada sumber daya yang terkait dengan produk yang disediakan. Jika memperbarui tanda diperbolehkan, maka tanda baru yang terkait dengan produk atau portofolio akan diterapkan ke sumber daya yang ditetapkan selama pembaruan produk yang ditetapkan.

Cara mengaktifkan pembaruan tanda pada produk

1. Buka konsol Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Pilih portofolio yang berisi produk yang ingin Anda perbarui.
3. Pilih tab Batasan dan pilih Tambahkan batasan.
4. Di bawah Tipe batasan, pilih Pembaruan Tanda.
5. Pilih produk dari Produk, lalu pilih Lanjutkan.
6. Pada halaman Pembaruan Tanda, pilih Aktifkan Pembaruan Tanda.
7. Pilih Kirim.

Batasan Set Tumpukan AWS Service Catalog

> **Note**
>
> - AWS Service Catalogtidak mendukung batasan set tumpukan untuk produk Terraform Open Source.
> - AutoTags saat ini tidak didukung dengan AWS CloudFormation StackSets.

Batasan set tumpukan memungkinkan Anda mengonfigurasi opsi penerapan produk menggunakan. AWS CloudFormation StackSets Anda dapat menentukan beberapa akun dan wilayah untuk peluncuran produk. Pengguna akhir dapat mengelola akun tersebut dan menentukan tempat produk di-deploy dan urutan deployment.

Untuk menerapkan batasan set tumpukan ke produk

1. Buka konsol Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Pilih portofolio dengan produk yang Anda inginkan.
3. Pilih Batasan lalu pilih Buat batasan.

4. Pada Produk, pilih produk. Pada Tipe batasan, pilih Set tumpukan.
5. Konfigurasikan akun, wilayah, dan izin untuk batasan set tumpukan Anda.
   - Di Pengaturan akun, identifikasi akun tempat Anda ingin membuat produk.
   - Pada Pengaturan wilayah, pilih wilayah geografis untuk men-deploy produk dan urutan produk yang Anda inginkan untuk di-deploy pada wilayah tersebut.
   - Di Izin, pilih Peran StackSet Administrator IAM untuk mengelola akun target Anda. Jika Anda tidak memilih peran, StackSets gunakan ARN default. Pelajari lebih lanjut tentang menyiapkan izin set tumpukan.
6. Pilih Buat.

Batasan Templat AWS Service Catalog

> **Note**
>
> AWS Service Catalogtidak mendukung batasan template untuk produk Terraform Open Source atau Terraform Cloud.

Untuk membatasi opsi yang tersedia untuk pengguna akhir saat mereka meluncurkan produk tersebut, Anda terapkan batasan templat. Terapkan batasan templat guna memastikan bahwa pengguna akhir dapat menggunakan produk tanpa melanggar persyaratan kepatuhan organisasi Anda. Anda menerapkan batasan template untuk produk dalam portofolio. AWS Service Catalog Portofolio harus berisi satu atau beberapa produk sebelum Anda dapat menentukan batasan templat.

Sebuah batasan templat terdiri dari satu atau lebih aturan yang mempersempit nilai-nilai yang diizinkan untuk parameter yang ditentukan dalam templat AWS CloudFormation utama milik produk. Parameter dalam templat AWS CloudFormation menentukan kumpulan nilai yang dapat ditentukan pengguna saat membuat sebuah tumpukan. Misalnya, parameter dapat menentukan berbagai tipe instans yang dapat dipilih oleh pengguna ketika meluncurkan tumpukan yang mencakup instans EC2.

Jika set nilai parameter dalam templat terlalu banyak untuk target audiens portofolio Anda, Anda dapat menentukan batasan templat guna membatasi nilai yang dapat dipilih pengguna saat meluncurkan produk. Misalnya, jika parameter templat termasuk tipe instans EC2 yang terlalu besar untuk pengguna yang harus menggunakan hanya tipe instans kecil (seperti `t2.micro` atau `t2.small`), maka Anda dapat menambahkan sebuah batasan templat untuk membatasi tipe instans

yang dapat dipilih oleh pengguna akhir. Untuk informasi selengkapnya tentang parameter templat AWS CloudFormation, lihat Parameter dalam Panduan Pengguna AWS CloudFormation.

Batasan templat terikat dalam portofolio. Jika Anda menerapkan batasan templat untuk sebuah produk dalam satu portofolio, lalu jika Anda menyertakan produk ke dalam portofolio lain, batasan tidak akan berlaku untuk produk dalam portofolio kedua.

Jika Anda menerapkan batasan templat untuk produk yang telah dibagi dengan pengguna, batasan langsung aktif untuk semua peluncuran produk berikutnya dan untuk semua versi produk dalam portofolio.

Anda menentukan aturan batasan templat dengan menggunakan editor aturan atau dengan menulis aturan sebagai teks JSON di dalam konsol administrator AWS Service Catalog. Untuk informasi selengkapnya tentang aturan, termasuk sintaks dan contoh, lihat Aturan Batasan Templat.

Untuk menguji batasan sebelum melepaskannya ke pengguna, buat portofolio uji yang berisi produk yang sama dan uji batasan dengan portofolio tersebut.

Untuk menerapkan batasan templat ke suatu produk

1. Buka konsol Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Pada halaman Portofolio, Anda terapkan batasan templat ke portofolio yang berisi produk yang Anda pilih.
3. Perluas bagian Batasan dan pilih Tambahkan batasan.
4. Pada jendela Pilih produk dan tipe, untuk Produk, Anda tetapkan batasan templat ke produk yang ingin Anda pilih. Lalu, untuk Tipe batasan, pilih Templat. Pilih Lanjutkan.
5. Pada halaman Pembangun batasan templat, edit aturan batasan dengan menggunakan editor JSON atau antarmuka pembangun aturan.

   - Untuk mengedit kode JSON untuk aturan, pilih tab Editor Teks Batasan. Beberapa sampel disediakan pada tab ini untuk membantu Anda memulai.

     Untuk membangun aturan dengan menggunakan antarmuka pembangun aturan, pilih tab Pembuat Aturan. Pada tab ini, Anda dapat memilih parameter yang ditentukan dalam templat untuk produknya, dan Anda dapat menentukan nilai yang diizinkan untuk parameter tersebut. Tergantung pada tipe parameter, Anda menentukan nilai yang diizinkan dengan memilih item dalam daftar periksa, dengan menentukan nomor, atau dengan menentukan satu set nilai dalam daftar dipisahkan dengan koma.

Setelah Anda selesai membangun aturan, pilih Tambahkan aturan. Aturan muncul dalam tabel pada tab Pembuat Aturan. Untuk meninjau dan mengedit output JSON, pilih tab Editor Teks Batasan.

6. Setelah selesai mengedit aturan untuk batasan Anda, pilih Kirim. Untuk melihat batasan, buka halaman detail portofolio dan perluas Batasan.

Aturan Batasan Templat

Aturan yang menentukan batasan template dalam AWS Service Catalog portofolio menjelaskan kapan pengguna akhir dapat menggunakan template dan nilai mana yang dapat mereka tentukan untuk parameter yang dideklarasikan dalam AWS CloudFormation template yang digunakan untuk membuat produk yang mereka coba gunakan. Aturan berguna untuk mencegah pengguna akhir menentukan nilai yang salah secara tidak sengaja. Misalnya, Anda dapat menambahkan aturan untuk memverifikasi bahwa pengguna akhir menentukan subnet yang valid ke dalam VPC tertentu atau menggunakan tipe instans `m1.small` untuk lingkungan pengujian. AWS CloudFormation menggunakan aturan untuk memvalidasi nilai parameter sebelum menciptakan sumber daya untuk produk.

Setiap aturan terdiri dari dua sifat: syarat aturan (opsional) dan pernyataan (wajib). Syarat aturan menentukan waktu berlakunya aturan. Pernyataan menjelaskan nilai yang dapat ditentukan pengguna untuk parameter tertentu. Jika Anda tidak menentukan syarat aturan, pernyataan aturan selalu berlaku. Untuk menentukan syarat aturan dan pernyataan, Anda menggunakan fungsi intrinsik khusus aturan, yang merupakan fungsi yang hanya dapat digunakan dalam bagian `Rules` dari templat. Anda dapat membuat nest fungsi, tetapi hasil akhir dari syarat aturan atau pernyataan harus berupa benar atau salah.

Sebagai contoh, anggap bahwa Anda telah menyatakan VPC dan subnet parameter pada bagian `Parameters`. Anda dapat membuat aturan yang memvalidasi bahwa subnet yang diberikan berada di VPC tertentu. Jadi ketika pengguna menentukan VPC, AWS CloudFormation mengevaluasi pernyataan untuk memeriksa bahwa nilai parameter subnet berada dalam VPC tersebut sebelum membuat atau memperbarui tumpukan. Jika nilai parameter tidak valid, AWS CloudFormation gagal untuk membuat atau memperbarui tumpukan. Jika pengguna tidak menentukan VPC, AWS CloudFormation tidak memeriksa nilai parameter subnet.

Sintaks

Bagian `Rules` dari templat terdiri dari nama kunci `Rules`, diikuti oleh titik dua. Kurung kurawal melampirkan semua deklarasi aturan. Jika Anda mendeklarasikan beberapa aturan, aturan-aturan tersebut dibatasi dengan koma. Untuk setiap aturan, Anda nyatakan nama logis dalam tanda kutip diikuti oleh titik dua dan tanda kurung kurawal yang menyertakan syarat dan pernyataan aturan.

Aturan dapat mencakup properti `RuleCondition` dan harus mencakup properti `Assertions`. Untuk setiap aturan, Anda dapat menentukan hanya satu aturan syarat; Anda dapat menentukan satu atau beberapa pernyataan dalam properti `Assertions`. Anda menentukan sebuah syarat dan pernyataan aturan dengan menggunakan fungsi intrinsik khusus aturan, seperti yang ditampilkan pada templat semu berikut:

```
"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"
         }
      ]
```

```
    }
}
```

Templat semu menunjukkan bagian `Rules` yang berisi dua aturan bernama `Rule01` dan `Rule02`. `Rule01` mencakup syarat aturan dan dua pernyataan. Jika fungsi dalam syarat aturan bernilai true (benar), kedua fungsi dalam setiap pernyataan dievaluasi dan diterapkan. Jika syarat aturan adalah false (salah), aturan tidak berlaku. `Rule02` selalu berlaku karena tidak memiliki syarat aturan, yang berarti satu pernyataan selalu dievaluasi dan diterapkan.

Untuk informasi tentang fungsi intrinsik khusus aturan guna menentukan kondisi dan pernyataan aturan, lihat Fungsi AWSAturan di Panduan Pengguna. AWS CloudFormation

Contoh: Verifikasi Nilai Parameter secara Bersyarat

Dalam contoh berikut, dua aturan tersebut memeriksa nilai parameter `InstanceType`. Tergantung pada nilai parameter Lingkungan (`test` atau `prod`), pengguna harus menentukan `m1.small` atau `m1.large` untuk parameter `InstanceType`. Parameter `InstanceType` dan `Environment` harus dideklarasikan dalam bagian `Parameters` dari templat yang sama.

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

Tindakan Layanan AWS Service Catalog

> **Note**
>
> AWS Service Catalogtidak mendukung tindakan layanan untuk produk Terraform Open Source atau Terraform Cloud.

AWS Service Catalog memungkinkan Anda untuk mengurangi pemeliharaan administratif dan pelatihan pengguna akhir sambil mematuhi langkah-langkah kepatuhan dan keamanan. Dengan tindakan layanan, sebagai administrator, Anda dapat mengaktifkan pengguna akhir untuk melakukan tugas operasional, memecahkan masalah, menjalankan perintah yang disetujui, atau meminta izin di AWS Service Catalog. Anda menggunakan dokumen AWS Systems Manager untuk menentukan tindakan layanan. AWS Systems ManagerDokumen menyediakan akses ke tindakan yang telah ditentukan sebelumnya yang menerapkan praktik AWS terbaik, seperti Amazon EC2 berhenti dan reboot, dan Anda juga dapat menentukan tindakan kustom.

Dalam tutorial ini, Anda menyediakan pengguna akhir dengan kemampuan untuk memulai ulang instans Amazon EC2. Anda menambahkan izin yang diperlukan, menentukan tindakan layanan, mengaitkan tindakan layanan dengan produk, dan menguji pengalaman pengguna akhir menggunakan tindakan dengan produk yang tersedia.

Prasyarat

Tutorial ini mengasumsikan bahwa Anda memiliki izin administrator AWS penuh, Anda sudah terbiasa dengan AWS Service Catalog, dan bahwa Anda sudah memiliki set dasar produk, portofolio, dan pengguna. Jika Anda tidak terbiasa AWS Service Catalog, selesaikan Penyiapan dan tugas Memulai sebelum menggunakan tutorial ini.

Topik

Langkah 1: Konfigurasikan izin pengguna akhir

Pengguna akhir harus memiliki izin yang diperlukan untuk melihat dan melakukan tindakan layanan tertentu. Dalam contoh ini, pengguna akhir membutuhkan izin untuk mengakses fitur tindakan layanan AWS Service Catalog dan untuk melakukan mulai ulang Amazon EC2.

Untuk memperbarui izin

1. Buka konsol AWS Identity and Access Management (IAM) di https://console.aws.amazon.com/iam/.
2. Dari menu, cari grup pengguna.
3. Pilih grup yang akan digunakan pengguna akhir untuk mengakses AWS Service Catalog sumber daya. Dalam contoh ini, kami memilih grup pengguna akhir. Dalam implementasi Anda sendiri, pilih grup yang digunakan oleh pengguna akhir yang relevan.
4. Pada tab Izin dari halaman detail grup Anda, Anda dapat membuat kebijakan baru atau mengedit kebijakan yang sudah ada. Dalam contoh ini, kami menambahkan izin ke kebijakan yang sudah ada dengan memilih kebijakan kustom yang dibuat untuk izin Penyediaan dan Penghentian AWS Service Catalog milik grup.
5. Pada halaman Kebijakan, pilih Edit Kebijakan untuk menambahkan izin yang dibutuhkan. Anda dapat menggunakan editor visual atau editor JSON untuk mengedit kebijakan. Dalam contoh ini, kami menggunakan editor JSON untuk menambahkan izin. Untuk tutorial ini, tambahkan izin berikut ke dalam kebijakan:

```
{
 "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. Setelah Anda mengedit kebijakan, tinjau dan setujui perubahan kebijakan. Pengguna di grup pengguna akhir sekarang memiliki izin yang diperlukan untuk melakukan tindakan mulai ulang Amazon EC2 di AWS Service Catalog.

Langkah 2: Buat tindakan layanan

Selanjutnya, Anda membuat tindakan layanan untuk memulai ulang instans Amazon EC2.

1. Buka konsol AWS Service Catalog di https://console.aws.amazon.com/sc/.
2. Dari menu, pilih Tindakan layanan.
3. Pada halaman Tindakan layanan, pilih Buat tindakan.
4. Pada halaman Buat tindakan, pilih dokumen AWS Systems Manager untuk menentukan tindakan layanan. Tindakan Mulai Ulang Instans Amazon EC2 ditentukan oleh dokumen AWS Systems Manager, jadi kami menyimpan opsi default pada menu tarik turun, Dokumen Amazon.
5. Cari dan pilih tindakan AWS-Restartec2Instance.
6. Berikan nama dan deskripsi untuk tindakan yang masuk akal bagi lingkungan dan tim Anda. Pengguna akhir akan melihat deskripsi ini, jadi pilihlah sesuatu yang membantu mereka memahami tindakan yang dilakukan.
7. Di bawah Parameter dan konfigurasi target, pilih parameter dokumen SSM yang akan menjadi target tindakan (misalnya, ID Instans), dan pilih target parameter. Pilih Tambahkan parameter untuk menambahkan parameter tambahan.
8. Di bawah Izin, pilih peran. Kami menggunakan izin default untuk contoh ini. Konfigurasi izin lainnya dimungkinkan dan ditentukan di halaman ini.
9. Setelah Anda meninjau konfigurasi, pilih Buat tindakan.
10. Pada halaman selanjutnya, konfirmasi muncul saat tindakan telah dibuat dan siap digunakan.

Langkah 3: Kaitkan tindakan layanan dengan versi produk

Setelah menentukan sebuah tindakan, Anda harus mengaitkan produk dengan tindakan tersebut.

1. Pada halaman Tindakan layanan, pilih AWS-Restartec2Instance, lalu pilih Tindakan asosiasi.
2. Pada halaman Kaitkan tindakan, pilih produk yang Anda inginkan agar dilakukan tindakan layanan oleh pengguna akhir Anda. Dalam contoh ini, kami memilih Desktop Linux.
3. Pilih versi produk. Perhatikan bahwa Anda dapat menggunakan kotak centang paling atas untuk memilih semua versi.
4. Pilih Kaitkan tindakan.
5. Di halaman selanjutnya, pesan konfirmasi muncul.

Anda sekarang telah membuat tindakan layanan di AWS Service Catalog. Langkah berikutnya dari tutorial ini adalah dengan menggunakan tindakan layanan sebagai pengguna akhir.

Langkah 4: Uji pengalaman pengguna akhir

Pengguna akhir dapat melakukan tindakan layanan pada produk yang tersedia. Untuk tujuan tutorial ini, pengguna akhir harus memiliki setidaknya satu produk yang tersedia. Produk yang tersedia harus diluncurkan dari versi produk yang Anda kaitkan dengan tindakan layanan di langkah sebelumnya.

Untuk mengakses tindakan layanan sebagai pengguna akhir

1. Masuk ke konsol AWS Service Catalog sebagai pengguna akhir.
2. Pada dasbor AWS Service Catalog, di panel navigasi, pilih Daftar Produk yang Tersedia. Daftar menunjukkan produk yang tersedia untuk akun pengguna akhir.
3. Pada halaman Daftar produk yang Tersedia, pilih instans yang tersedia.
4. Pada halaman Detail produk yang disediakan, pilih Tindakan di sisi kanan atas, lalu pilih tindakan AWS-Restartec2Instance.
5. Konfirmasikan bahwa Anda ingin mengeksekusi tindakan kustom. Anda menerima konfirmasi bahwa tindakan telah dikirim.

Langkah 5: Mengelola tindakan layanan dengan AWS CloudFormation

Anda dapat membuat tindakan layanan dan asosiasi mereka dengan AWS CloudFormation sumber daya. Untuk informasi selengkapnya, pelajari topik berikut di Panduan Pengguna AWS CloudFormation:

- AWS::ServiceCatalog::CloudFormationProduk ProvisioningArtifactProperties
- AWS::ServiceCatalog::ServiceActionAsosiasi

> **Note**
>
> Jika Anda mengelola asosiasi tindakan layanan dengan AWS CloudFormation sumber daya, jangan menambahkan atau menghapus tindakan layanan melalui AWS Command Line Interface atauAWS Management Console. Saat Anda melakukan pembaruan tumpukan, perubahan apa pun pada tindakan sevice yang dibuat di luar akan AWS CloudFormation diganti.

Langkah 6: Pemecahan Masalah

Jika eksekusi tindakan layanan Anda gagal, Anda dapat menemukan pesan kesalahan di bagian Output dari peristiwa eksekusi tindakan layanan pada halaman Produk yang Tersedia. Di bawah ini Anda dapat melihat penjelasan untuk pesan kesalahan umum yang mungkin Anda temukan.

> **Note**
>
> Teks yang tepat dari pesan kesalahan dapat berubah, jadi Anda harus menghindari penggunaannya dalam proses otomatis apa pun.

Kegagalan internal

AWS Service Catalog mengalami kesalahan internal. Coba lagi nanti. Jika masalah berlanjut, hubungi dukungan pelanggan.

Terjadi kesalahan (ThrottlingException) saat memanggil StartAutomationExecution operasi

Eksekusi tindakan layanan di-throttle oleh layanan backend, seperti SSM.

Akses ditolak saat mengambil peran

AWS Service Catalog tidak dapat mengasumsikan peran yang ditentukan dalam ketentuan tindakan layanan. Pastikan bahwa pelaku utama servicecatalog.amazonaws.com, atau wilayah utama seperti servicecatalog.us-east-1.amazonaws.com, diizinkan dalam kebijakan kepercayaan peran.

Terjadi kesalahan (AccessDeniedException) saat memanggil StartAutomationExecution operasi: Pengguna tidak berwenang untuk melakukan: ssm: StartAutomationExecution pada sumber daya.

Peran yang ditentukan dalam definisi tindakan layanan tidak memiliki izin untuk memanggil ssm:. StartAutomationExecution Pastikan peran memiliki izin SSM yang sesuai.

Tidak dapat menemukan sumber daya apa pun dengan tipe ***TargetType***produk yang disediakan

Produk yang disediakan tidak berisi sumber daya apa pun yang cocok dengan jenis target yang ditentukan dalam dokumen SSM, sepertiAWS: :EC2: :Instance. Periksa produk yang Anda sediakan untuk sumber daya ini atau konfirmasikan bahwa dokumen sudah benar.

Dokumen dengan nama itu tidak ada

Dokumen yang ditentukan dalam ketentuan tindakan layanan tidak ada.

Gagal mendeskripsikan dokumen SSM Automation

AWS Service Catalog mengalami pengecualian yang tidak diketahui dari SSM saat mencoba mendeskripsikan dokumen yang ditentukan.

Gagal mengambil kredensi untuk peran

AWS Service Catalog mengalami kesalahan yang tidak diketahui saat mengambil peran yang ditentukan.

Parameter memiliki nilai ***InvalidValue***"" tidak ditemukan di ***{ValidValue1}, {ValidValue2}***

Nilai parameter yang diteruskan ke SSM tidak ada dalam daftar nilai yang diizinkan untuk dokumen. Konfirmasikan bahwa parameter yang tersedia adalah valid, dan coba lagi.

Kesalahan tipe parameter. Nilai yang diberikan untuk ***ParameterName***bukan string yang valid.

Nilai parameter yang diteruskan ke SSM tidak valid untuk tipe pada dokumen.

Parameter tidak didefinisikan dalam definisi tindakan layanan

Parameter diteruskan ke AWS Service Catalog yang tidak ditentukan dalam ketentuan tindakan layanan. Anda hanya dapat menggunakan parameter yang ditentukan dalam ketentuan tindakan layanan.

Langkah gagal saat mengeksekusi/membatalkan tindakan. ***Pesan kesalahan.*** Silakan merujuk ke Panduan Pemecahan Masalah Layanan Otomatisasi untuk detail diagnosis selengkapnya.

Langkah dalam dokumen otomatisasi SSM gagal. Lihat kesalahan dalam pesan untuk memecahkan masalah lebih lanjut.

Nilai berikut untuk parameter tidak diperbolehkan karena tidak ada dalam produk yang disediakan: ***InvalidResourceId***

Pengguna meminta tindakan pada sumber daya yang tidak ada dalam produk yang tersedia.

TargetType tidak ditentukan untuk dokumen SSM Automation

Tindakan layanan memerlukan dokumen otomatisasi SSM untuk memiliki yang TargetType ditentukan. Periksa dokumen otomatisasi SSM Anda.

Menambahkan Produk AWS Marketplace untuk Portofolio Anda

Anda dapat menambahkan produk AWS Marketplace ke portofolio Anda untuk membuat produk tersebut tersedia bagi pengguna akhir AWS Service Catalog Anda.

AWS Marketplace adalah toko online tempat Anda dapat menemukan, berlangganan, dan segera mulai menggunakan banyak pilihan perangkat lunak dan layanan. Tipe produk di AWS Marketplace mencakup basis data, server aplikasi, alat pengujian, alat pemantauan, alat manajemen konten, dan perangkat lunak kecerdasan bisnis. AWS Marketplace tersedia di https://aws.amazon.com/marketplace. Perhatikan bahwa Anda tidak dapat menambahkan produk perangkat lunak sebagai layanan (SaaS) dari keAWS Marketplace. AWS Service Catalog

Anda mendistribusikan AWS Marketplace produk ke pengguna AWS Service Catalog akhir dengan menyalin produk dengan AWS CloudFormation template keAWS Service Catalog, dan kemudian menambahkan produk ke portofolio.

> **Note**
>
> AWS Service Catalogtidak mendukung distribusi AWS Marketplace produk ke pengguna AWS Service Catalog akhir menggunakan templat produk Terraform Open Source atau Terraform Cloud.

AWS Marketplace mendukung AWS Service Catalog secara langsung atau berlangganan dan menambahkan produk menggunakan opsi manual. Kami rekomendasikan untuk menambahkan produk menggunakan fungsionalitas yang didesain khusus untuk AWS Service Catalog.

Mengelola Produk AWS Marketplace Menggunakan AWS Service Catalog

Anda dapat menambahkan langganan produk AWS Marketplace Anda langsung ke AWS Service Catalog menggunakan antarmuka kustom. Di AWS Marketplace, pilih Service Catalog. Untuk informasi selengkapnya, lihat Menyalin Produk AWS Service Catalog di AWS MarketplaceBantuan dan FAQ.

Mengelola dan Menambahkan Produk AWS Marketplace secara Manual

Selesaikan langkah-langkah berikut untuk berlangganan AWS Marketplace produk, tentukan produk itu dalam AWS CloudFormation templat, dan tambahkan templat ke AWS Service Catalog portofolio.

Untuk berlangganan produk AWS Marketplace

1. Buka AWS Marketplace di https://aws.amazon.com/marketplace.
2. Jelajahi produk atau cari untuk menemukan produk yang ingin Anda tambahkan ke dalam portofolio AWS Service Catalog Anda. Pilih produk untuk melihat halaman detail produk.
3. Pilih Lanjutkan untuk melihat halaman pengisian, dan kemudian pilih tab Peluncuran Manual.

   Informasi pada halaman pemenuhan mencakup jenis instans Amazon Elastic Compute Cloud (Amazon EC2) yang didukung, yang Wilayah AWS didukung, dan ID Amazon Machine Image (AMI) yang digunakan produk untuk setiap wilayah. AWS Perhatikan bahwa beberapa pilihan akan mempengaruhi biaya. Anda akan menggunakan informasi ini untuk menyesuaikan templat AWS CloudFormation pada langkah selanjutnya.
4. Pilih Terima Persyaratan untuk berlangganan produk.

Setelah Anda berlangganan produk, Anda dapat mengakses informasi pada halaman pengisian produk di AWS Marketplace setiap saat dengan memilih Perangkat Lunak Anda, lalu memilih produk.

Untuk menentukan produk AWS Marketplace Anda dalam templat AWS CloudFormation

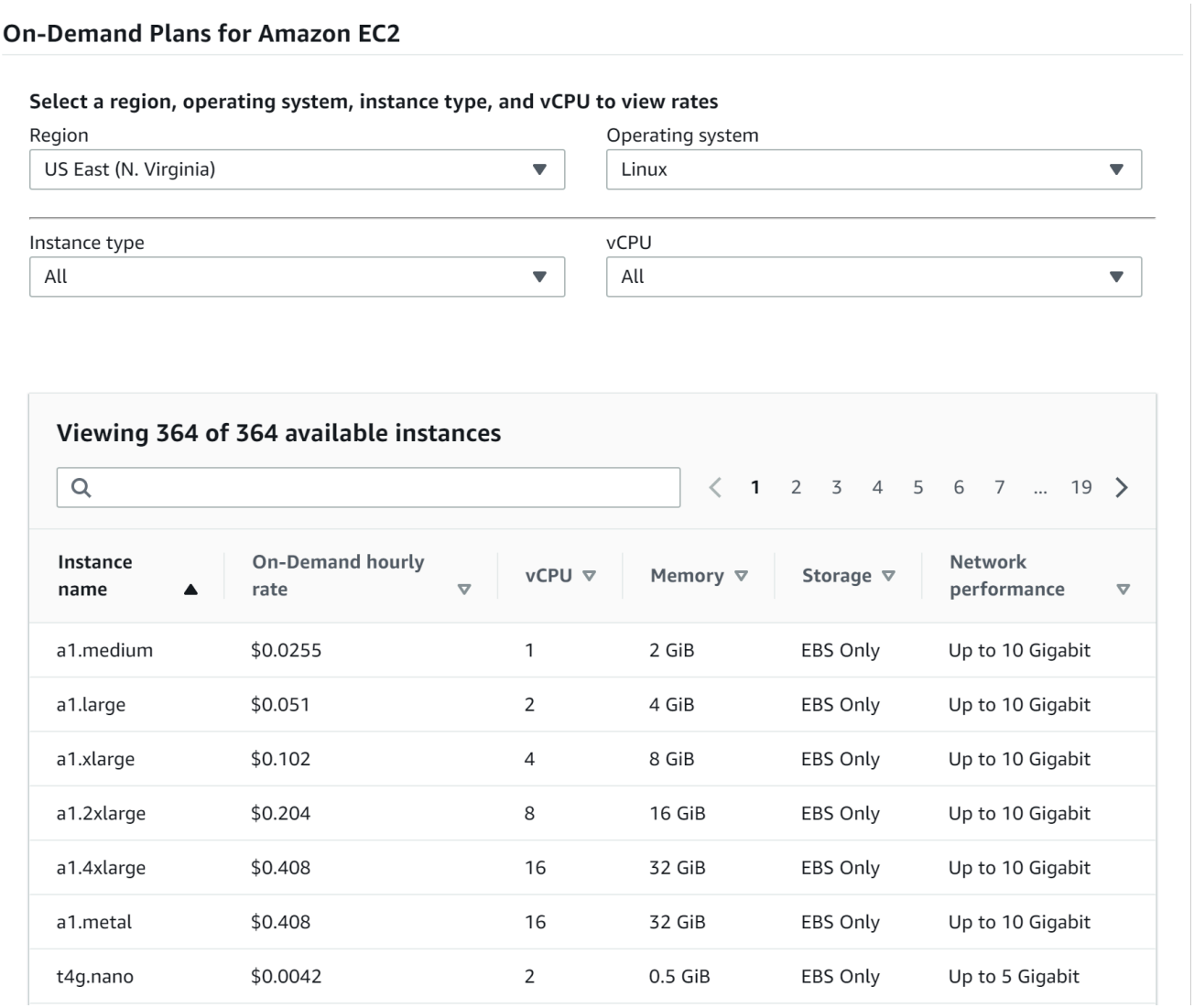
Untuk menyelesaikan langkah-langkah berikut, Anda akan menggunakan salah satu templat sampel AWS CloudFormation sebagai titik awal, dan Anda akan menyesuaikan templat agar dapat menunjukkan produk AWS Marketplace Anda. Untuk mengakses templat sampel, lihat Templat Sampel dalam Panduan Pengguna AWS CloudFormation.

1. Pada halaman Template Contoh di Panduan AWS CloudFormation Pengguna, pilih AWS Wilayah untuk produk Anda. AWSWilayah harus didukung oleh AWS Marketplace produk Anda. Anda dapat melihat wilayah yang didukung pada halaman pengisian produk di AWS Marketplace.
2. Untuk melihat daftar layanan templat sampel yang sesuai untuk Wilayah tersebut, pilih tautan Layanan.
3. Anda dapat menggunakan salah satu sampel yang sesuai untuk kebutuhan Anda sebagai titik awal. Langkah-langkah dalam prosedur ini menggunakan templat instans Amazon EC2 dalam grup keamanan. Untuk melihat templat sampel, pilih Lihat, lalu simpan salinan templat secara lokal sehingga Anda dapat mengeditnya. File lokal Anda harus memiliki ekstensi `.template`.
4. Buka file templat Anda di editor teks.
5. Sesuaikan deskripsi di bagian atas templat. Deskripsi Anda mungkin terlihat seperti contoh berikut:

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

6. Sesuaikan parameter `InstanceType` sehingga hanya mencakup tipe instans EC2 yang didukung oleh produk Anda. Jika templat Anda mencakup tipe instans EC2 yang tidak didukung, produk akan gagal untuk peluncuran pengguna akhir Anda.

   a. Pada halaman pengisian produk di AWS Marketplace, lihat tipe instans EC2 yang didukung di bagian Detail Harga.



b. Dalam templat Anda, ubah tipe instans default untuk tipe instans EC2 yang didukung dari pilihan Anda.

c. Edit daftar `AllowedValues` sehingga hanya mencakup tipe instans EC2 yang didukung oleh produk Anda.

d. Hapus tipe instans EC2 yang tidak Anda inginkan untuk digunakan pengguna akhir Anda ketika mereka meluncurkan produk dari daftar `AllowedValues`.

Setelah Anda selesai mengedit parameter `InstanceType`, hal tersebut mungkin terlihat serupa dengan contoh berikut:

```
"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. Di bagian `Mappings` dari templat Anda, edit pemetaan `AWSInstanceType2Arch` sehingga hanya didukung tipe instans EC2 dan arsitektur yang disertakan.

   a. Edit daftar pemetaan dengan menghapus semua tipe instans EC2 yang tidak termasuk dalam daftar `AllowedValues` untuk parameter `InstanceType`.

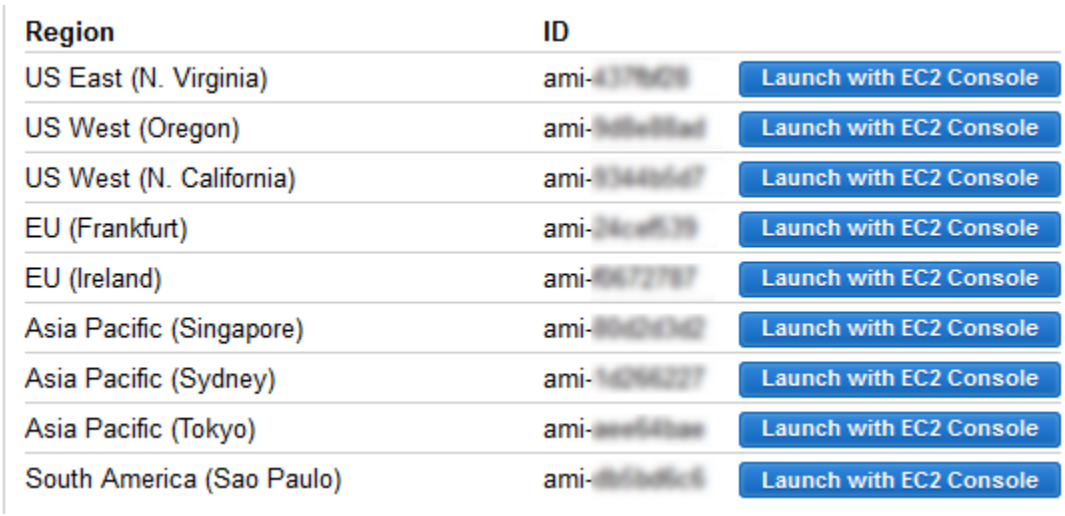
   b. Edit nilai `Arch` untuk setiap tipe instans EC2 menjadi tipe arsitektur yang didukung oleh produk Anda. Nilai yang valid adalah `PV64`, `HVM64`, dan `HVMG2`. Untuk mempelajari arsitektur mana yang didukung produk Anda, lihat halaman detail produk di AWS Marketplace. Untuk mempelajari arsitektur mana yang didukung oleh keluarga instans EC2, lihat Matrix Tipe Instans Amazon Linux AMI.

   Setelah selesai mengedit pemetaan `AWSInstanceType2Arch`, hal tersebut mungkin terlihat serupa dengan contoh berikut:

```
    "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. Di `Mappings` bagian template Anda, edit `AWSRegionArch2AMI` pemetaan untuk mengaitkan setiap AWS Wilayah dengan arsitektur yang sesuai dan ID AMI untuk produk Anda.

   a. Pada halaman pemenuhan produk diAWS Marketplace, lihat ID AMI yang digunakan produk Anda untuk setiap AWS Wilayah, seperti pada contoh berikut:



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. Di template Anda, hapus pemetaan untuk AWS Wilayah mana pun yang tidak Anda dukung.

   c. Edit pemetaan untuk setiap wilayah guna menghapus arsitektur yang tidak didukung (`PV64`, `HVM64`, atau `HVMG2`) dan ID AMI terkait mereka.

   d. Untuk setiap pemetaan AWS Wilayah dan arsitektur yang tersisa, tentukan ID AMI yang sesuai dari halaman detail produk diAWS Marketplace.

   Setelah selesai mengedit pemetaan `AWSRegionArch2AMI`, kode Anda mungkin terlihat serupa dengan contoh berikut:

```
"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"}
}
```

Anda sekarang dapat menggunakan template untuk menambahkan produk ke AWS Service Catalog portofolio. Jika Anda ingin melakukan perubahan tambahan, lihat Bekerja dengan Templat AWS CloudFormation untuk mempelajari selengkapnya tentang templat.

Untuk menambahkan AWS Marketplace produk Anda ke AWS Service Catalog portofolio

1. Masuk ke AWS Management Console dan navigasikan ke konsol administrator AWS Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Pada halaman Portofolio, pilih portofolio yang ingin Anda tambahkan produk AndaAWS Marketplace.
3. Pada halaman detail portofolio, pilih Unggah produk baru.
4. Ketik produk yang diminta dan detail support.
5. Pada halaman Detail Versi, pilih Unggah sebuah file templat, pilih Jelajahi, lalu pilih file templat Anda.
6. Ketik judul versi dan deskripsi.
7. Pilih Berikutnya.
8. Pada halaman Tinjauan, verifikasi bahwa ringkasan akurat, lalu pilih Konfirmasi dan unggah. Produk telah ditambahkan ke portfolio Anda. Produk kini tersedia bagi pengguna akhir yang memiliki akses ke portofolio.

Menggunakan AWS CloudFormation StackSets

> **Note**
>
> AutoTags saat ini tidak didukung dengan AWS CloudFormation StackSets.

Anda dapat menggunakan AWS CloudFormation StackSets untuk meluncurkan AWS Service Catalog produk di beberapa Wilayah AWS dan akun. Anda dapat menentukan urutan penyebaran produk secara berurutan di dalamnya. Wilayah AWS Di seluruh akun, produk di-deploy secara paralel. Saat meluncurkan, pengguna dapat menentukan toleransi kegagalan dan jumlah maksimum akun yang digunakan secara paralel. Untuk informasi selengkapnya, lihat Bekerja dengan AWS CloudFormation StackSets.

Set tumpukan vs instans tumpukan

Satu set tumpukan memungkinkan Anda untuk membuat tumpukan di akun AWS di seluruh Wilayah AWS dengan menggunakan templat AWS CloudFormation tunggal.

Sebuah tumpukan instans mengacu pada tumpukan di akun target dalam Wilayah AWS dan terhubung hanya dengan satu set tumpukan.

Untuk informasi selengkapnya, lihatStackSetsKonsep.

Batasan set tumpukan

Di AWS Service Catalog, Anda dapat menggunakan batasan set tumpukan untuk mengonfigurasi opsi deployment produk.

AWS Service Catalogmendukung batasan set tumpukan pada produk dalam duaAWS GovCloud (US) Regions: AWS GovCloud (AS-Barat) dan AWS GovCloud (AS-Timur).

Untuk informasi selengkapnya, lihat AWS Service CatalogStack Set Constraints.

Mengelola Anggaran

Anda dapat menggunakan Anggaran AWS untuk melacak biaya layanan dan penggunaan Anda dalam AWS Service Catalog. Anda dapat mengaitkan anggaran dengan produk dan portfolio AWS Service Catalog.

> **Note**
>
> AWS Service Catalogtidak mendukung anggaran untuk produk Terraform Open Source.

Anggaran AWS memberikan Anda kemampuan untuk menetapkan anggaran kustom yang dapat memberitahu Anda saat biaya atau penggunaan Anda melebihi (atau diperkirakan melebihi) jumlah anggaran Anda yang telah ditetapkan. Informasi tentang Anggaran AWS tersedia di https://aws.amazon.com/aws-cost-management/aws-budgets.

Tugas

- Prasyarat
- Membuat anggaran

- Mengaitkan Anggaran
- Melihat Anggaran
- Memisahkan Anggaran

Prasyarat

Sebelum menggunakan Anggaran AWS, Anda perlu mengaktifkan tanda alokasi biaya di konsol AWS Billing and Cost Management. Untuk informasi selengkapnya, lihat Mengaktifkan Tanda Alokasi Biaya Buatan Pengguna dalam Panduan Pengguna AWS Billing and Cost Management.

> **Note**
>
> Tanda memerlukan waktu hingga 24 jam agar aktif.

Anda juga harus mengaktifkan akses pengguna ke AWS Billing and Cost Management untuk setiap pengguna atau grup yang akan menggunakan fitur Anggaran. Anda dapat melakukannya dengan membuat kebijakan baru untuk pengguna Anda.

Untuk memungkinkan pengguna membuat anggaran, Anda juga harus mengizinkan pengguna untuk melihat informasi penagihan. Jika Anda ingin menggunakan notifikasi Amazon SNS, Anda dapat memberikan pengguna kemampuan untuk membuat notifikasi Amazon SNS, seperti yang ditunjukkan pada contoh kebijakan di bawah ini.

Untuk membuat kebijakan anggaran

1. Buka konsol IAM di https://console.aws.amazon.com/iam/.
2. Di panel navigasi, pilih Kebijakan.
3. Di panel konten, pilih Buat kebijakan.
4. Pilih tab JSON dan salin teks dari dokumen kebijakan JSON berikut. Tempel teks ini ke kotak teks 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. Setelah Anda selesai, pilih Tinjau kebijakan. Validator Kebijakan melaporkan kesalahan sintaksis.
6. Pada halaman Ulasan, beri nama kebijakan Anda. Tinjau Ringkasan kebijakan untuk melihat izin yang diberikan oleh kebijakan Anda, lalu pilih Buat kebijakan untuk menyimpan pekerjaan Anda.

   Kebijakan baru muncul pada daftar kebijakan terkelola dan siap dilampirkan kepada pengguna dan grup Anda. Untuk informasi selengkapnya, lihat Membuat dan melampirkan Kebijakan Terkelola Pelanggan di Panduan Pengguna AWS Identity and Access Management.

Membuat anggaran

Di konsol AWS Service Catalog administrator, daftar Produk dan halaman Portofolio mencantumkan informasi tentang produk dan portofolio yang ada dan memungkinkan Anda untuk mengambil tindakan terhadapnya. Untuk membuat anggaran, pertama-tama tentukan produk atau portofolio mana yang ingin Anda kaitkan dengan anggaran tersebut.

Untuk membuat bucket

1. Buka konsol Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Pilih daftar Produk atau Portofolio.
3. Pilih produk atau portofolio yang ingin Anda tambahkan anggaran.
4. Buka menu Tindakan, lalu pilih Buat anggaran.
5. Pada halaman Pembuatan anggaran, kaitkan satu tipe tanda ke anggaran Anda.

   Ada dua jenis tag: AutoTags dan TagOptions. AutoTags mengidentifikasi portofolio, produk, dan pengguna yang meluncurkan produk. AWS Service Catalogmenerapkan tag ini secara otomatis ke sumber daya yang disediakan. A TagOption adalah pasangan nilai kunci yang ditentukan administrator yang dikelola. AWS Service Catalog

   Agar pengeluaran yang terjadi di portofolio atau produk dapat digambarkan pada anggaran terkait, anggaran terkait harus memiliki tanda yang sama. Perhatikan bahwa kunci tanda yang digunakan pertama kalinya dapat memakan waktu 24 jam agar dapat diaktifkan. Untuk informasi selengkapnya, lihat the section called “Prasyarat”.
6. Pilih Buat di AWS Budgets. Anda diarahkan ke halaman Tetapkan anggaran Anda. Lanjutkan menyiapkan anggaran Anda dengan mengikuti langkah-langkah dalam Membuat Anggaran.

> **Note**
>
> Setelah Anda membuat anggaran, Anda harus mengaitkannya dengan produk atau portofolio.

Mengaitkan Anggaran

Setiap portofolio atau produk dapat memiliki satu anggaran yang terkait dengannya. Setiap anggaran dapat dikaitkan dengan beberapa portofolio dan produk.

Ketika Anda mengaitkan anggaran ke portofolio atau produk, Anda dapat melihat informasi tentang anggaran dari portofolio atau halaman detail produk tersebut. Agar pengeluaran yang terjadi pada portofolio atau produk tercermin pada anggaran, Anda harus mengaitkan tag yang sama pada anggaran dan portofolio atau produk.

> **Note**
>
> Jika Anda menghapus anggaran dariAWS Budgets, asosiasi yang ada dengan AWS Service Catalog produk dan portofolio masih ada. AWS Service Catalogtidak akan dapat menampilkan informasi apa pun tentang anggaran yang dihapus.

Untuk mengaitkan anggaran

1. Buka konsol Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Pilih daftar Produk atau Portofolio.
3. Pilih produk atau portofolio yang ingin Anda kaitkan dengan anggaran.
4. Buka menu Actions, lalu pilih Associate budget.
5. Pada halaman Asosiasi anggaran, pilih anggaran yang ada, lalu pilih Lanjutkan.
6. Tabel produk atau portofolio sekarang menyertakan data untuk anggaran yang baru saja Anda tambahkan.

Melihat Anggaran

Jika anggaran dikaitkan dengan suatu produk, Anda dapat melihat informasi tentang anggaran pada detail Produk dan halaman daftar Produk. Jika anggaran dikaitkan dengan portofolio, Anda dapat melihat informasi tentang anggaran di halaman detail Portofolio dan Portofolio.

Halaman daftar Portofolio dan Produk menampilkan informasi anggaran untuk sumber daya yang ada. Anda dapat melihat kolom yang menampilkan Saat ini vs. anggaran dan Prakiraan vs. Anggaran.

Ketika Anda memilih produk atau portofolio, Anda diarahkan ke halaman detail. Rincian Portofolio dan halaman detail Produk memiliki bagian dengan informasi rinci tentang anggaran terkait. Anda dapat melihat jumlah yang dianggarkan, pengeluaran saat ini, dan pengeluaran yang diperkirakan. Anda juga memiliki pilihan untuk melihat detail anggaran dan mengedit anggaran.

Memisahkan Anggaran

Anda dapat memisahkan anggaran dari portofolio atau produk.

> **Note**
>
> Jika Anda menghapus AWS anggaran dari Anggaran, asosiasi yang ada dengan AWS Service Catalog produk dan portofolio masih ada. AWS Service Catalogtidak akan dapat menampilkan informasi apa pun tentang anggaran yang dihapus.

Untuk memisahkan anggaran

1. Buka konsol Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Pilih daftar Produk atau Portofolio.
3. Pilih produk atau portofolio yang ingin Anda putuskan dari anggaran.
4. Pilih Tindakan. Dari dropdown, pilih Disassociate budget. Peringatan konfirmasi muncul.
5. Setelah Anda mengonfirmasi bahwa Anda ingin membongkar anggaran dari produk atau portofolio, pilih Konfirmasi.

Mengelola Produk yang Tersedia

AWS Service Catalog menyediakan antarmuka untuk mengelola produk yang tersedia. Anda dapat melihat, memperbarui, dan mengakhiri semua produk yang tersedia untuk katalog Anda berdasarkan tingkat akses. Lihat bagian berikut untuk contoh prosedur.

Topik

Mengelola produk yang disediakan sebagai administrator

Untuk mengelola semua produk yang disediakan untuk akun, Anda harus memiliki `AWSServiceCatalogAdminFullAccess` atau izin IAM yang setara untuk mengakses operasi penulisan produk yang disediakan. Untuk informasi selengkapnya, lihat Manajemen Identitas dan Akses di AWS Service Catalog.

> **Tip**
>
> Untuk rantai produk yang disediakan statis, Anda harus mereferensikan keluaran produk yang disediakan dalam templat artefak produk sebelum produk yang disediakan disediakan. Untuk informasi selengkapnya, termasuk contoh, lihat berikut ini:
>
> - AWS::ServiceCatalog::CloudFormationProvisionedProduct di Panduan Pengguna AWS CloudFormation.
> - DescribeProvisioningParameters (ProvisioningArtifactOutputKeys) di Panduan AWS Service Catalog Pengembang.

Untuk melihat dan mengelola semua produk yang tersedia

1. Buka konsol AWS Service Catalog di https://console.aws.amazon.com/servicecatalog/.

Jika Anda sudah masuk ke konsol AWS Service Catalog, pilih Service Catalog, lalu Pengguna akhir.

2. Jika perlu, gulir ke bawah ke bagian Produk yang Tersedia.
3. Di bagian Produk yang Tersedia, pilih daftar Lihat: dan pilih tingkat akses yang ingin Anda lihat: Pengguna, Peran, atau Akun. Tindakan ini menampilkan semua produk yang tersedia dalam katalog.
4. Pilih produk yang tersedia untuk melihat, memperbarui, atau mengakhiri. Untuk informasi selengkapnya tentang informasi yang tersedia dalam tampilan ini, lihat Melihat Informasi Produk yang Tersedia.

Mengubah Pemilik Produk yang Tersedia

Anda dapat mengubah pemilik produk yang tersedia kapan saja. Anda perlu mengetahui ARN dari pengguna atau peran yang ingin Anda tetapkan sebagai pemilik baru.

Secara default, fitur ini tersedia untuk administrator menggunakan kebijakan yang dikelola `AWSServiceCatalogAdminFullAccess`. Anda dapat mengaktifkannya untuk pengguna akhir dengan memberikan para pengguna izin `servicecatalog:UpdateProvisionedProductProperties` di AWS Identity and Access Management (IAM).

Untuk mengubah pemilik produk yang tersedia

1. Di konsol AWS Service Catalog tersebut, pilih Daftar produk yang Tersedia.
2. Cari produk tersedia yang ingin Anda perbarui, lalu pilih tiga titik di sampingnya dan pilih Ubah pemilik produk yang tersedia.Anda juga dapat menemukan opsi Ubah pemilik pada halaman detail produk yang tersedia, di menu Tindakan.
3. Di kotak dialog, masukkan ARN pengguna atau peran yang ingin Anda tetapkan sebagai pemilik baru. ARN dimulai dengan `arn:` dan mencakup informasi lain yang dipisahkan oleh titik dua atau garis miring, misalnya, `arn:aws:iam::123456789012:user/NewOwner`.
4. Pilih Kirim. Anda akan melihat pesan berhasil saat pemilik telah diperbarui.

Lihat Juga

- UpdateProvisionedProductProperties

Memperbarui template untuk produk yang disediakan

Anda dapat mengubah template saat ini dari produk yang disediakan ke template yang berbeda. Misalnya jika Anda memiliki produk EC2 di Service Catalog, Anda dapat memperbarui produk EC2 tersebut untuk mempertahankan ID produk yang disediakan yang sama, tetapi mengubah template menjadi bucket S3.

> **Note**
>
> Memperbarui templat tidak didukung untuk produk Terraform Open Source atau Terraform Cloud yang disediakan. Jika Anda ingin menggunakan templat yang berbeda untuk produk Terraform yang ada, Anda harus menghapus produk dan kemudian membuat produk baru menggunakan templat yang diinginkan.

Untuk memperbarui template untuk produk yang disediakan

1. Di menu navigasi kiri, pilih Produk yang disediakan.
2. Di Produk yang disediakan, pilih produk yang disediakan dan pilih Tindakan, Perbarui.

   Perhatikan bahwa Anda juga dapat memilih Tindakan, Perbarui di halaman Detail produk yang disediakan.
3. (Opsional) Dalam detail Produk, pilih Ubah produk.

   Di Ubah produk, perhatikan peringatan ini:

   Mengubah produk akan memperbarui produk yang disediakan ini ke templat produk yang berbeda. Ini dapat menghentikan sumber daya dan membuat sumber daya baru.

   Anda dapat memperbarui produk yang disediakan ke versi yang berbeda dalam produk yang sama.
4. (Opsional) Dalam Produk, pilih produk yang ingin Anda perbarui dengan template yang berbeda. Kemudian pilih Ubah.

   Dalam detail Produk, perhatikan peringatan ini:

   [Nama produk] akan diperbarui dari [nama template saat ini] ke [nama template baru]. Namun, nama produk yang Anda sediakan, [Nama Produk yang Diberikan], tidak akan berubah.

Anda dapat memperbarui produk yang disediakan ke versi yang berbeda dalam produk yang sama.

5. Dalam versi Produk, pilih versi produk yang Anda inginkan.
6. Dalam Parameter, pilih parameter yang sesuai.
7. Pilih Perbarui.

   Di detail produk yang disediakan, Anda dapat melihat detail pembaruan. Nama produk yang disediakan tidak berubah, tetapi produk yang disediakan sekarang memiliki template yang berbeda.

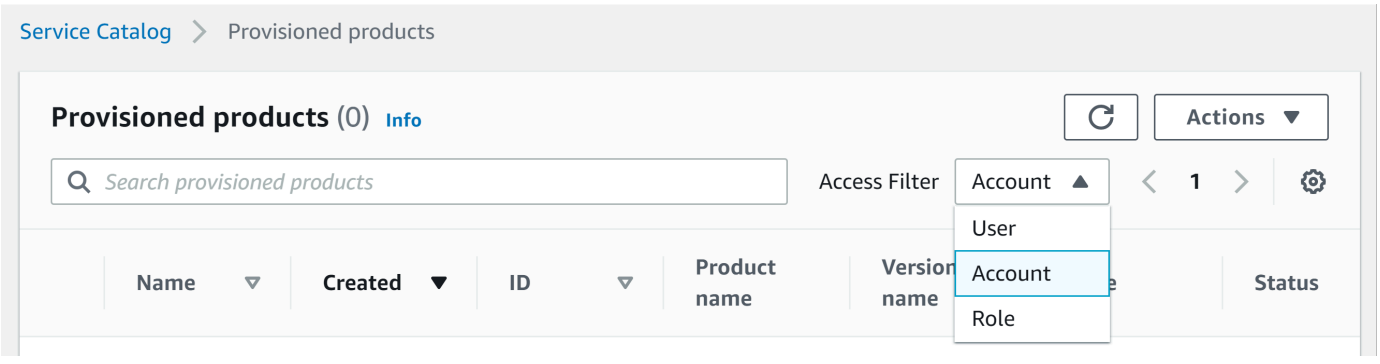
Tutorial: Mengidentifikasi Alokasi Sumber Daya Pengguna

Anda dapat mengidentifikasi pengguna yang menyediakan produk dan sumber daya yang terkait dengan produk menggunakan konsolAWS Service Catalog. Tutorial ini membantu menerjemahkan contoh ini untuk produk tersedia khusus milik Anda sendiri.

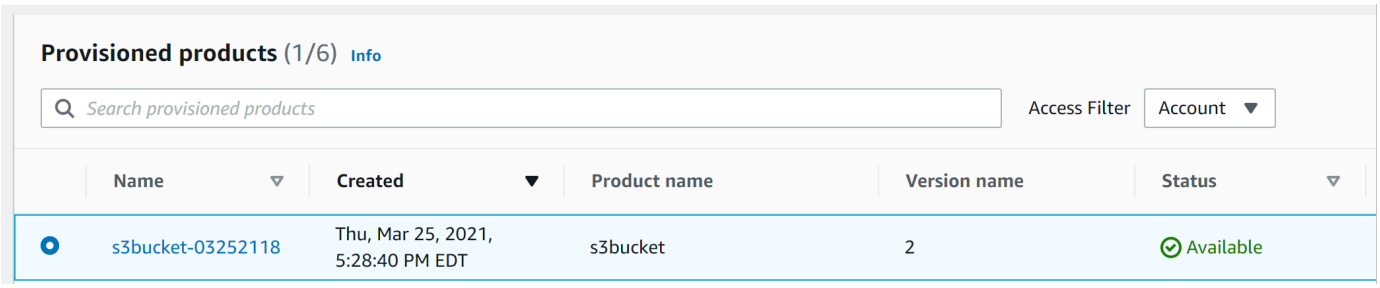
Untuk mengelola semua produk yang tersedia untuk akun tersebut, Anda memerlukan `AWSServiceCatalogAdminFullAccess` atau akses yang setara ke operasi penulisan produk yang tersedia. Untuk informasi selengkapnya, lihat Identity and Access Management dalam Panduan Administrator AWS Service Catalog.

Untuk mengidentifikasi pengguna yang menyediakan produk dan sumber daya terkait

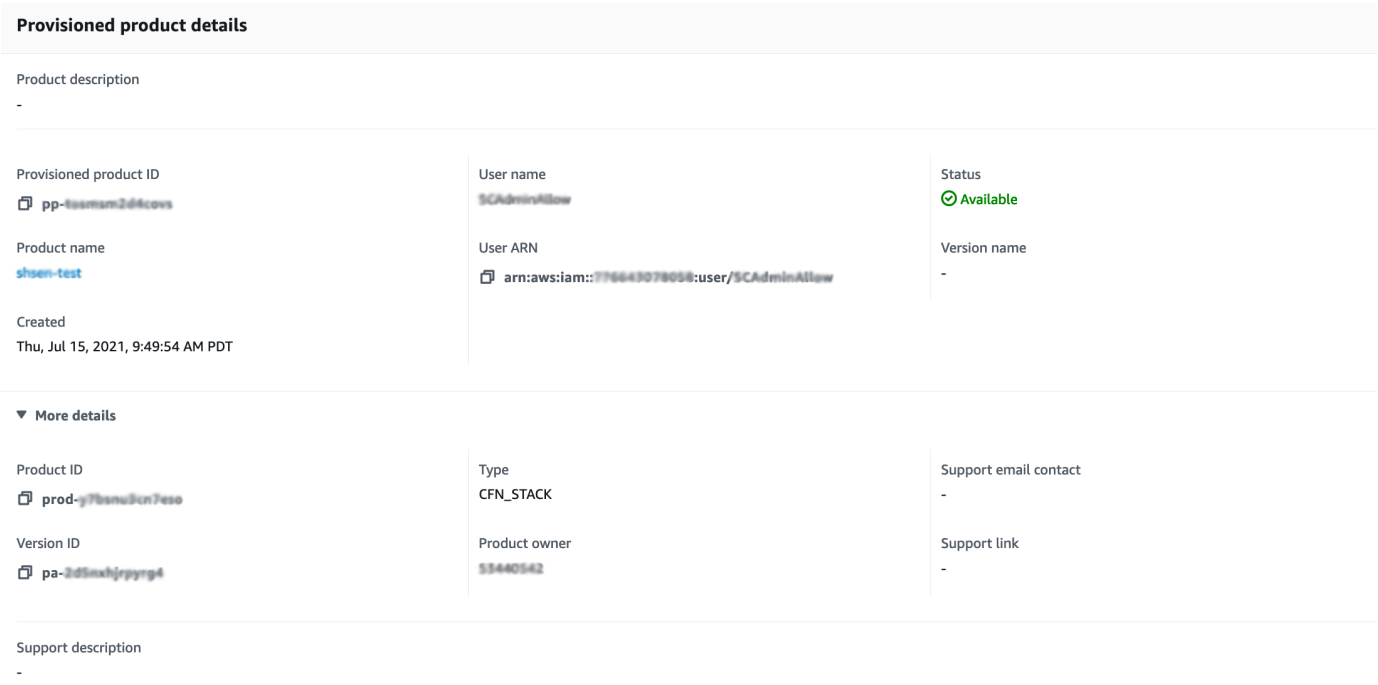
1. Buka https://console.aws.amazon.com/servicecatalog.
2. Di menu navigasi sebelah kiri, pilih Produk yang Tersedia.
3. Di menu tarik-turun Filter akses, pilih Akun.



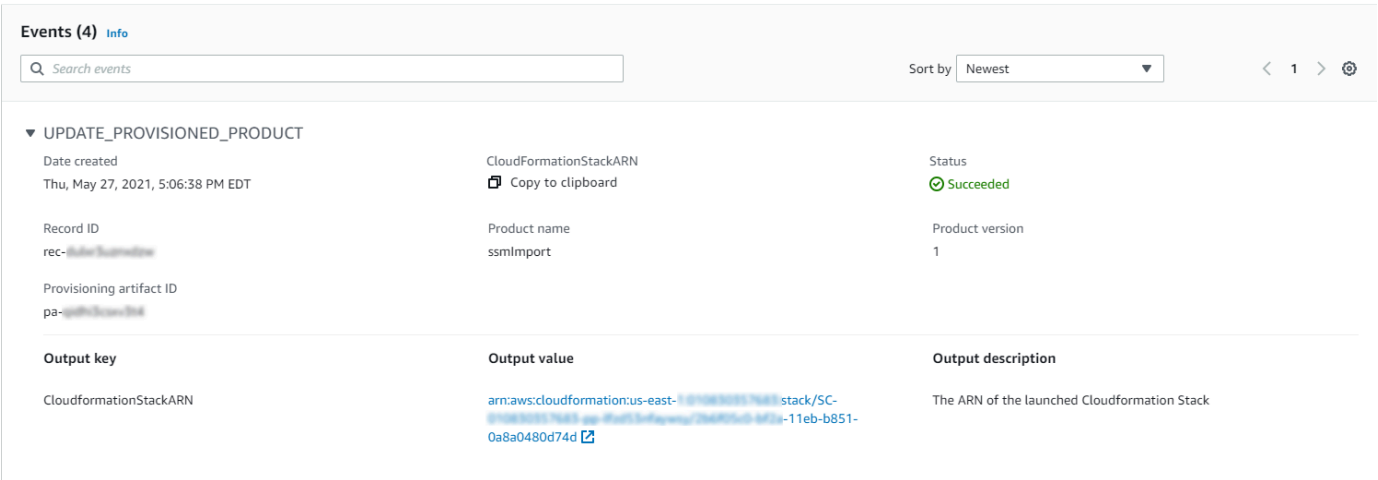
4. Di tampilan Akun, pilih dan buka produk yang tersedia untuk menampilkan detail.



Anda dapat melihat detail produk yang tersedia.



5. Gulir ke bawah untuk memperluas bagian Peristiwa. Perhatikan `Provisioned product ID` dan nilai `CloudformationStackARN`.



6. Gunakan ID produk yang tersedia untuk mengidentifikasi catatan AWS CloudTrail yang sesuai dengan peluncuran ini dan mengidentifikasi pengguna yang meminta (biasanya, Anda memasukkan alamat email selama federasi). Dalam contoh ini, ID tersebut adalah “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. Gunakan nilai `CloudformationStackARN` untuk mengidentifikasi peristiwa AWS CloudFormation untuk menemukan informasi tentang sumber daya yang dibuat. Anda juga dapat menggunakan API AWS CloudFormation untuk mendapatkan informasi ini. Untuk informasi selengkapnya, lihat Referensi API AWS CloudFormation.

Anda dapat melakukan langkah 1 hingga 4 menggunakan API AWS Service Catalog atau AWS CLI. Untuk informasi selengkapnya, lihat Panduan AWS Service Catalog Pengembang. dan Referensi Baris AWS Service Catalog Perintah.

Mengelola kesalahan status produk Terraform Open Source

`ProvisionProduct`Kegagalan Sumber Terbuka Terraform dialihkan ke `TAINTED` status, memungkinkan setiap produk yang disediakan untuk melanjutkan ke. `UpdateProvisionedProduct` Ketika ini terjadi:

- `UpdateProvisionedProduct`tidak melakukan upaya untuk memperbarui atau memperbaiki tag, atau untuk membuat atau memodifikasi grup sumber daya.
- `UpdateProvisionedProduct`tidak mempertimbangkan kegagalan dari operasi penyediaan sebelumnya ketika memutuskan apakah produk yang disediakan harus disetel ke atau. `AVAILABLE` `TAINTED`

AWS Service Cataloghanya berlaku Tag selama`ProvisionProduct`. Setiap penandaan yang gagal yang dihasilkan dari kegagalan `ProvisionProduct` operasi tidak diselesaikan secara otomatis.

Contoh kesalahan status

Contoh 1: AWS Service Catalog tidak membuat grup sumber daya selama `ProvisionProduct`

Dalam skenario di bawah ini, Anda memiliki produk yang disediakan di `AVAILABLE` negara bagian meskipun tidak ada grup sumber daya pendukung, dan tanpa tag apa pun yang diterapkan ke sumber daya.

1. Tindakan Anda dimulai. `ProvisionProduct`
2. Mesin penyediaan Terraform merespons `ProvisionProduct` dengan kegagalan alur kerja dan tidak menyediakan file. `ResourceIdentifier`
3. `ProvisionProduct`Alur kerja tidak membuat grup sumber daya, lalu menyetel status produk yang disediakan ke. `ERROR`
4. Anda kemudian memulai `UpdateProvisionedproduct` operasi.
5. Mesin penyediaan Terraform merespons yang menunjukkan “kesuksesan.”
6. Akibatnya, `UpdateprovisionedProduct` alur kerja menyetel status produk yang disediakan ke`AVAILABLE`, tetapi tidak membuat grup sumber daya, atau mencoba menerapkan Tag apa pun.

Contoh 2: AWS Service Catalog membuat sumber daya baru selama `UpdateProvisionedProduct`

Dalam skenario di bawah ini, Anda memiliki produk yang disediakan di `AVAILABLE` negara bagian meskipun sumber daya baru tidak memiliki tag yang diterapkan.

1. Tindakan Anda dimulai. `ProvisionProduct`

2. Mesin penyediaan Terraform merespons yang menunjukkan “keberhasilan” dan menyediakan a. `ResourceIdentifier`
3. `ProvisionProduct`Alur kerja membuat grup sumber daya dan menerapkan tag ke semua sumber daya yang diidentifikasi.
4. Anda memulai `UpdateProvisionedProduct` artefak baru yang menciptakan sumber daya baru.
5. Mesin penyediaan Terraform merespons yang menunjukkan “kesuksesan.”
6. `UpdateProvisionedProduct`Alur kerja menyetel status produk yang disediakan ke `AVAILABLE` tetapi tidak mencoba menerapkan tag tambahan apa pun ke sumber daya baru.

Solusi kesalahan status

AWS Service Catalogmemastikan bahwa grup sumber daya dibuat untuk semua produk yang disediakan disetel ke `TAINTED` from. `ProvisionProduct` Jika mesin penyediaan Terraform tidak mengembalikan`ResourceIdentifier`, atau jika AWS Service Catalog gagal membuat grup sumber daya, maka produk yang disediakan disetel ke `ERROR` status, memaksa Anda untuk mengakhiri.

Mengelola file status produk Terraform Open Source

Setiap produk yang disediakan Terraform Open Source memiliki file status tunggal. Ada hubungan 1:1 antara produk yang disediakan dan file statusnya. File disimpan dalam ember Amazon S3 bernama. `sc-terraform-engine-state-${AWS::AccountId}-${AWS::Region}` File status disimpan di bawah tombol `AccountID` atau `ProvisionedProductID` objek.

Akses file status terbatas pada templat peluncuran `GetStateFile` AWS Lambda dan Amazon EC2. AWS Service Catalogadministrator tidak memiliki akses langsung ke file status di Amazon S3. Administrator harus mengakses file menggunakan Amazon EC2. Secara default, AWS Service Catalog administrator dapat melihat daftar file status, tetapi tidak dapat membaca atau menulis konten file. Hanya mesin penyediaan Terraform yang dapat membaca atau menulis konten file.

Mengelola Tanda di AWS Service Catalog

AWS Service Catalog menyediakan tanda sehingga Anda dapat mengategorikan sumber daya Anda. Ada dua jenis tag: AutoTags dan TagOptions.

AutoTags adalah tag yang mengidentifikasi informasi tentang asal sumber daya yang disediakan AWS Service Catalog dan diterapkan secara otomatis AWS Service Catalog ke sumber daya yang disediakan.

TagOptions adalah pasangan nilai kunci yang dikelola AWS Service Catalog yang berfungsi sebagai templat untuk membuat AWS tag.

Topik

AWS Service Catalog AutoTags

> **Note**
>
> AWS Service Catalogtidak mendukung AutoTags produk Terraform Open Source.

AutoTags adalah tag yang mengidentifikasi informasi tentang asal sumber daya yang disediakan AWS Service Catalog dan diterapkan secara otomatis AWS Service Catalog ke sumber daya yang disediakan.

AutoTags menyertakan tag untuk pengidentifikasi unik untuk portofolio, produk, pengguna, versi produk, dan produk yang disediakan. Ini menyediakan satu set tanda yang mencerminkan struktur AWS Service Catalog yang telah dikonfigurasi pelanggan dalam katalog. AutoTags jangan dihitung terhadap batas 50 tag pelanggan.

> **Note**
>
> AWS Service Catalogtidak mendukung AutoTags produk Terraform Open Source.

AWS Service Catalog AutoTags dapat membantu memberikan penandaan yang konsisten untuk sumber daya Anda, yang berguna saat menetapkan anggaran untuk portofolio, produk, atau pengguna. Anda juga dapat menggunakan AutoTags untuk mengidentifikasi sumber daya untuk operasi pasca-peluncuran seperti menetapkan AWS Config aturan. AutoTags untuk sumber daya yang disediakan dapat dilihat di bagian Tag pada layanan hilir yang digunakan untuk penyediaan, seperti, Amazon AWS CloudFormation EC2, dan Amazon S3.

> **Note**
>
> AWS Service Catalogtidak diperbarui AutoTags setelah Anda mendaftar AutoTags ke sumber daya yang disediakan. Jika Anda memperbarui produk yang disediakan ke produk lain, artefak yang disediakan, atau jalur peluncuran baru, yang ada AutoTags masih menampilkan nilai aslinya.

AutoTag rincian

- aws:servicecatalog:portfolioArn - ARN portofolio tempat asal produk yang disediakan diluncurkan.
- aws:servicecatalog:portfolioArn - ARN produk tempat asal produk yang disediakan diluncurkan.
- aws:servicecatalog: - provisioningPrincipalArn ARN dari prinsipal penyediaan (pengguna) yang menciptakan produk yang disediakan.
- aws:servicecatalog: - Produk yang disediakan ARNprovisionedProductArn.
- aws:servicecatalog: provisioningArtifactIdentifier - ID artefak penyediaan asli (versi produk).

AWS Service Catalog TagOption Perpustakaan

Untuk memungkinkan administrator mengelola tag pada produk yang disediakan dengan mudah, AWS Service Catalog sediakan pustaka. TagOption A TagOption adalah pasangan kunci-nilai yang dikelola di. AWS Service Catalog Ini bukan AWS tag, tetapi berfungsi sebagai template untuk membuat AWS tag berdasarkan TagOption.

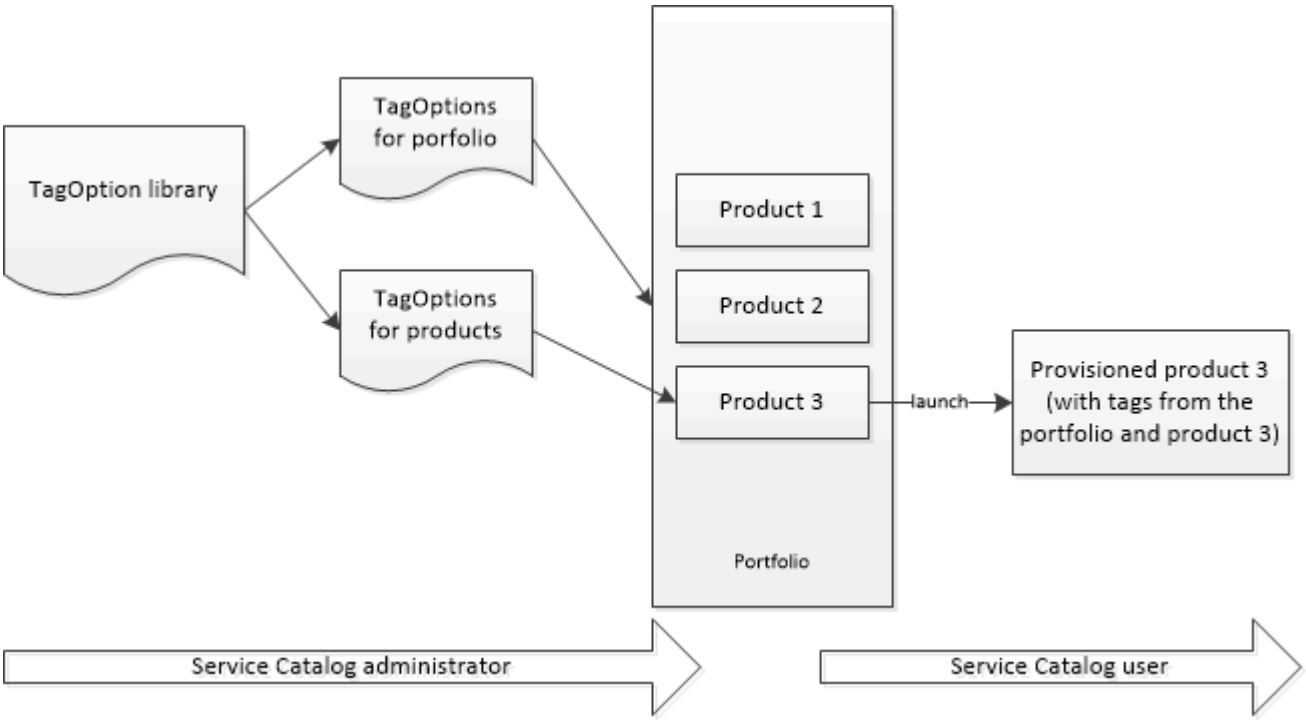
AWS Service Catalogtidak mendukung TagOptions produk Terraform Open Source atau Terraform Cloud.

TagOption Perpustakaan membuatnya lebih mudah untuk menegakkan hal-hal berikut:

- Taksonomi yang konsisten

- Penandaan yang tepat dari sumber daya AWS Service Catalog
- Opsi yang ditentukan dan dapat dipilih pengguna untuk tanda yang diizinkan

Administrator dapat mengasosiasikan TagOptions dengan portofolio dan produk. Selama peluncuran produk (penyediaan), AWS Service Catalog agregat portofolio dan produk terkait TagOptions, dan menerapkannya pada produk yang disediakan, seperti yang ditunjukkan pada diagram berikut.



Dengan TagOption perpustakaan, Anda dapat menonaktifkan TagOptions dan mempertahankan asosiasi mereka ke portofolio atau produk, dan mengaktifkannya kembali saat Anda membutuhkannya. Pendekatan ini tidak hanya membantu menjaga integritas perpustakaan, tetapi juga memungkinkan Anda untuk mengelola TagOptions yang mungkin digunakan sebentar-sebentar, atau hanya dalam keadaan khusus.

Anda mengelola TagOptions dengan AWS Service Catalog konsol atau API TagOption pustaka. Untuk informasi selengkapnya, lihat Referensi API Service Catalog.

Daftar Isi

Meluncurkan Produk dengan TagOptions

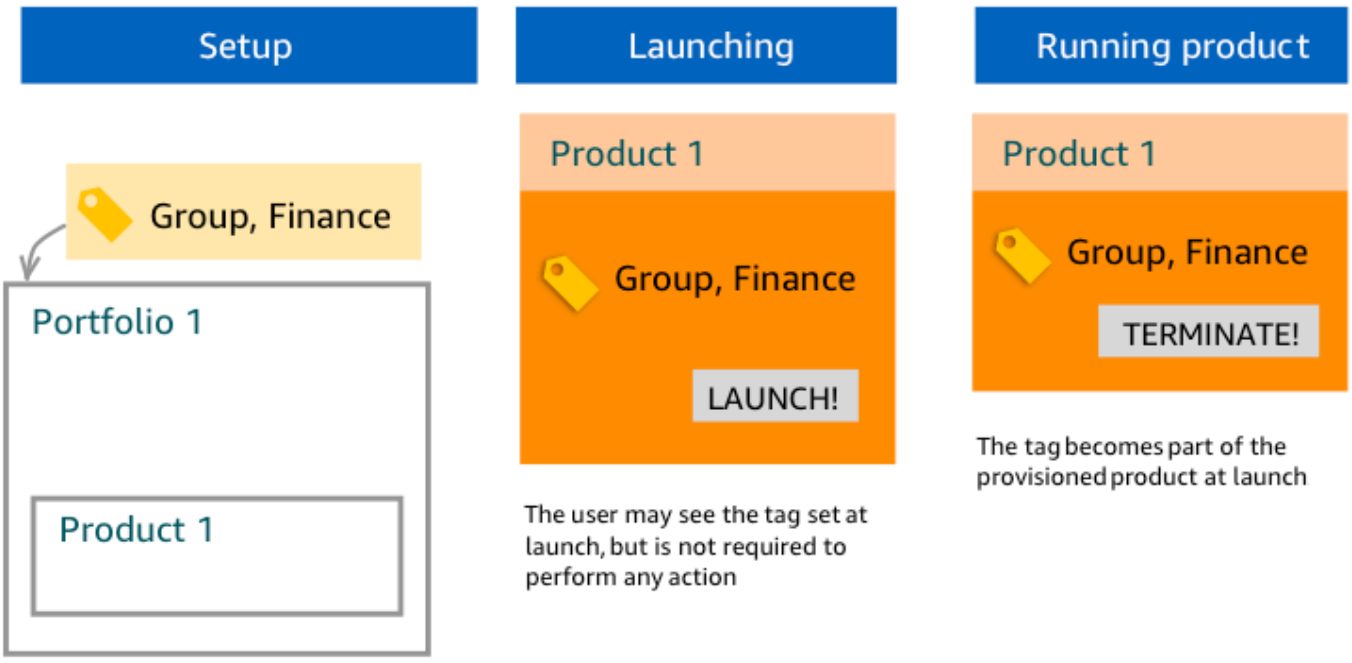
Saat pengguna meluncurkan produk yang memiliki TagOptions, AWS Service Catalog lakukan tindakan berikut atas nama Anda:

- Mengumpulkan semua TagOptions untuk produk dan portofolio peluncuran.
- Memastikan bahwa hanya TagOptions dengan kunci unik yang digunakan dalam tag pada produk yang disediakan. Para pengguna mendapatkan daftar nilai pilihan ganda untuk sebuah kunci. Setelah pengguna memilih nilai, nilai tersebut menjadi tanda pada produk yang tersedia.
- Memungkinkan pengguna untuk menambahkan tanda yang tidak bertentangan dengan produk selama penyediaan.

Kasus penggunaan berikut menunjukkan cara TagOptions kerja selama peluncuran.

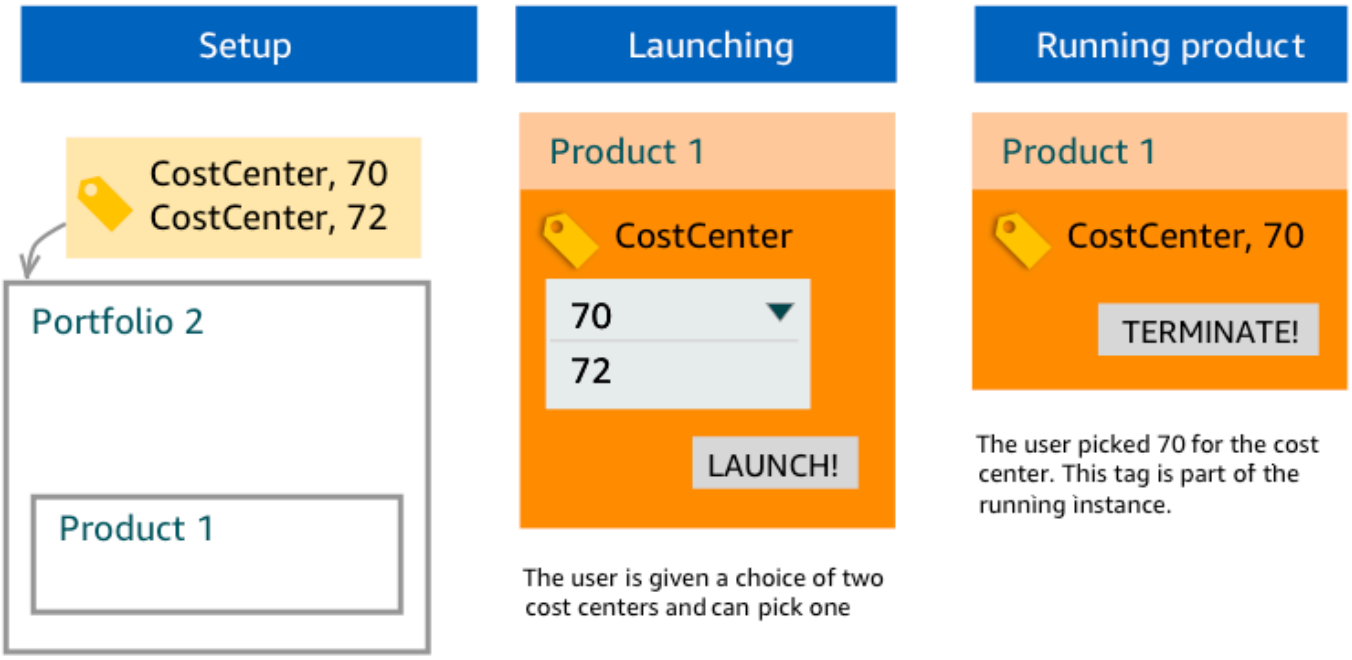
Contoh 1: TagOption Kunci Unik

Administrator membuat TagOption[Group=Finance] dan mengaitkannya dengan Portfolio1, yang memiliki Product1 tanpa. TagOptions Ketika pengguna meluncurkan produk yang disediakan, single TagOption menjadi Tag [Group=Finance], sebagai berikut:



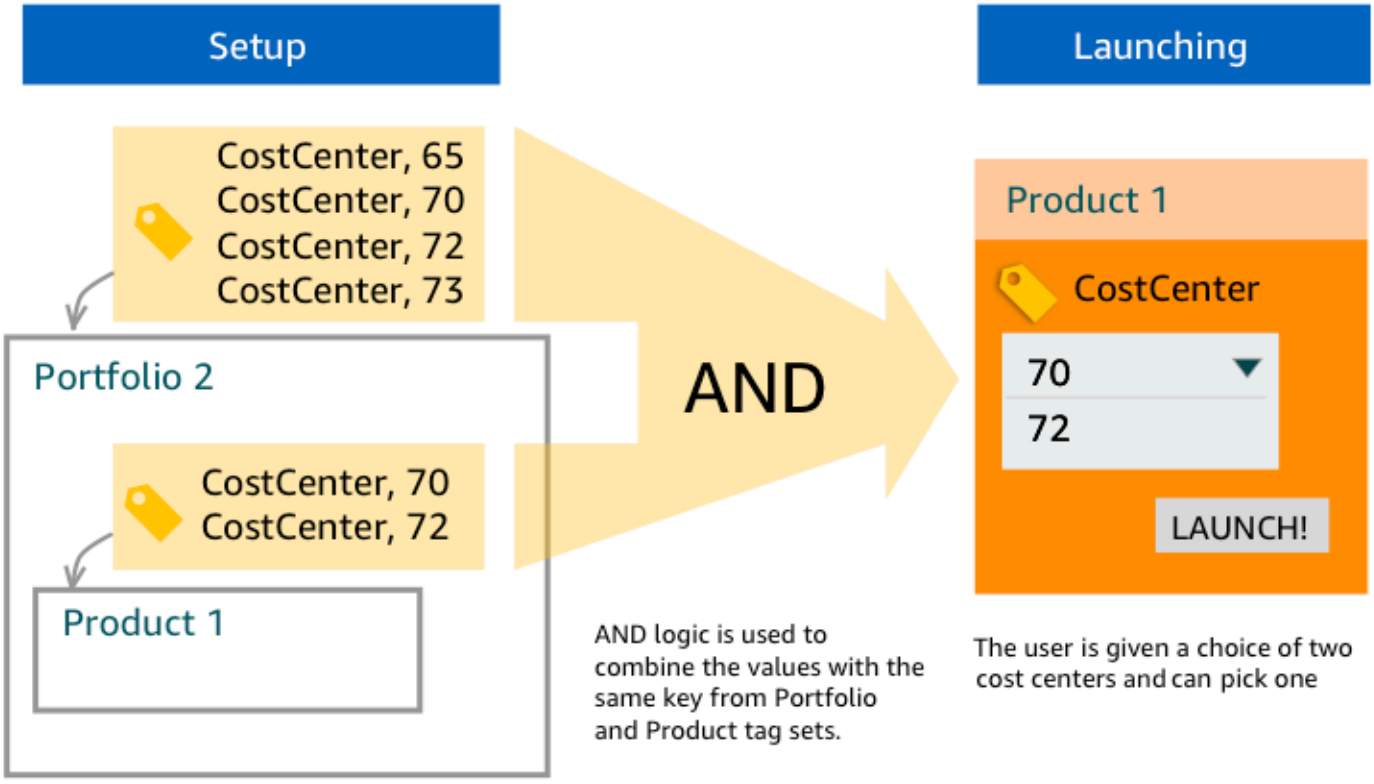
Contoh 2: Satu Set TagOptions dengan Kunci yang Sama pada Portofolio

Administrator telah menempatkan dua TagOptions dengan kunci yang sama pada portofolio, dan tidak ada TagOptions dengan kunci yang sama pada produk apa pun dalam portofolio itu. Selama peluncuran, pengguna harus memilih salah satu dari dua nilai yang terkait dengan kunci. Produk yang tersedia lalu ditandai dengan kunci dan nilai yang dipilih pengguna.



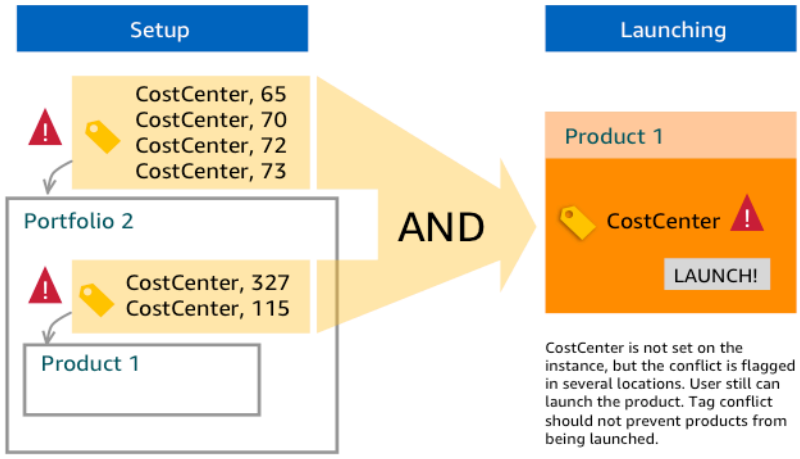
Contoh 3: Satu Set TagOptions dengan Kunci yang Sama pada Portofolio dan Produk dalam Portofolio itu

Seorang administrator telah menempatkan beberapa TagOptions dengan kunci yang sama pada portofolio, dan ada juga beberapa TagOptions dengan kunci yang sama pada produk dalam portofolio itu. AWS Service Catalogmenciptakan satu set nilai dari agregasi (logis DAN operasi) dari. TagOptions Saat pengguna meluncurkan produk, ia akan melihat dan memilih dari set nilai ini. Produk yang tersedia ditandai dengan kunci dan nilai yang dipilih pengguna.



Contoh 4: Beberapa TagOptions dengan Kunci yang Sama dan Nilai yang Bertentangan

Seorang administrator telah menempatkan beberapa TagOptions dengan kunci yang sama pada portofolio, dan ada juga beberapa TagOptions dengan kunci yang sama pada produk dalam portofolio itu. AWS Service Catalogmenciptakan satu set nilai dari agregasi (logis DAN operasi) dari. TagOptions Jika agregasi tidak menemukan nilai untuk kunci, AWS Service Catalog membuat tanda dengan kunci dan nilai `sc-tagconflict-`*`portfolioid`*`-`*`productid`* yang sama, tempat *`portfolioid`* dan *`productid`* adalah ARN portofolio dan produk. Hal ini memastikan bahwa produk yang tersedia ditandai dengan kunci yang benar, dan dengan nilai yang dapat administrator temukan dan benar.



Mengelola TagOptions

Sebagai administrator, Anda dapat melakukan tindakan berikut untuk mengelola TagOptions di TagOptions perpustakaan:

- Buat dan hapus
- Aktifkan atau Nonaktifkan
- Kaitkan atau putuskan kaitan
- Sunting

Untuk membuat TagOptions di konsol

1. Buka konsol Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Di menu navigasi kiri, pilih TagOptionsperpustakaan.
3. Di Buat baru TagOption, masukkan kunci dan nilai, lalu pilih Tambah.

   Setelah yang baru TagOption dibuat, itu dikelompokkan berdasarkan pasangan kunci-nilai dan diurutkan menurut abjad dalam daftar. TagOptions

   Untuk membuat TagOption menggunakan AWS Service Catalog API, lihat CreateTagOption.

Untuk menghapus TagOptions di konsol

1. Buka konsol Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Di menu navigasi kiri, pilih TagOptions perpustakaan dan kemudian pilih Tindakan.

3. Pilih Hapus dan konfirmasikan penghapusan.

Untuk mengaktifkan atau menonaktifkan satu atau lebih TagOptions di konsol

1. Buka konsol Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Di menu navigasi kiri, pilih TagOptions perpustakaan dan kemudian pilih Tindakan.
3. Untuk mengaktifkan, pilih yang tidak aktif yang TagOption Anda inginkan. Kemudian pilih Tindakan dan pilih Aktifkan dari menu tarik-turun, dan konfirmasikan pilihan Anda.

   Untuk menonaktifkan, pilih yang aktif yang TagOption Anda inginkan. Kemudian pilih Tindakan dan pilih Nonaktifkan dari menu tarik-turun, dan konfirmasikan pilihan Anda.

Untuk mengaitkan atau memisahkan satu atau lebih TagOptions dengan portofolio di konsol

1. Buka konsol Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Di menu navigasi kiri, pilih Portofolio, lalu buka portofolio yang ingin Anda kaitkan atau lepaskan.
3. Pilih TagOptionstab dan pilih satu atau lebih TagOptions untuk mengaitkan atau memisahkan diri dengan portofolio.
4. Pilih Tindakan. Kemudian pilih Associate atau Disassociate dan konfirmasikan pilihan Anda.

Untuk mengaitkan atau memisahkan satu atau lebih TagOptions dengan produk di konsol

1. Buka AWS Service Catalog konsol di: https://console.aws.amazon.com/servicecatalog/.
2. Di menu navigasi kiri, di bawah Administrasi, pilih Produk. Kemudian buka produk yang ingin Anda kaitkan atau pisahkan.
3. Pilih TagOptionstab dan pilih satu atau lebih TagOptions untuk mengaitkan atau memisahkan diri dengan portofolio.
4. Pilih Tindakan. Kemudian pilih Associate atau Disassociate dan konfirmasikan pilihan Anda.

> **Note**
>
> Untuk mengaitkan TagOptions dengan portofolio atau produk menggunakan AWS Service Catalog API, lihat AssociateTagOptionWithResource.

Untuk menghapus (memisahkan) TagOptions menggunakan AWS Service Catalog API, lihat DisassociateTagOptionFromResource.

Untuk mengedit nilai untuk TagOptions di konsol

1. Buka konsol Service Catalog di https://console.aws.amazon.com/servicecatalog/.
2. Di menu navigasi kiri, pilih TagOptionsperpustakaan.
3. Pilih TagOption dan buka nilainya. (Nilainya di-hyperlink.) Lalu pilih Edit.
4. Di dalam bidang Nilai, edit nilai dan pilih Simpan perubahan.

Menggunakan TagOptions dengan kebijakan AWS Organizations tag

Topik ini memberikan gambaran singkat tentang kebijakan tag untuk AWS Organizations dan TagOptions untukAWS Service Catalog. Ini juga menyarankan cara mencegah konflik penandaan saat menggunakan kedua fitur secara bersamaan.

TagOptions untuk AWS Service Catalog berlaku untuk produk yang disediakan (CloudFormationtumpukan), sementara kebijakan tag untuk AWS Organizations berlaku untuk AWS akun dan unit organisasi (OU) atau akar organisasi. Misalnya, jika Anda melampirkan kebijakan tag ke OU, kebijakan tag yang sama berlaku untuk semua akun di OU tersebut. Jika Anda menggunakan kedua fitur penandaan secara bersamaan, Anda harus mengonfigurasinya agar tidak bertentangan.

Kebijakan tag

Kebijakan tag memungkinkan Anda menentukan aturan tentang cara menggunakan tag pada AWS sumber daya di akun AndaAWS Organizations. Anda dapat menggunakan kebijakan tag untuk membuat dan mempertahankan pendekatan yang konsisten untuk menandai AWS sumber daya di tingkat akun.

Kebijakan tag menyediakan cara mudah untuk memastikan pengguna menerapkan tag yang konsisten, mengaudit sumber daya yang ditandai, dan mempertahankan kategorisasi sumber daya yang tepat. Anda juga dapat menentukan bagaimana kunci tag harus dikapitalisasi, dan nilai yang ingin Anda izinkan. Misalnya, Anda dapat mengharuskan semua instans EC2 di akun harus memiliki kunci tag yang disetel sebagai **`CostCenter`** dan nilai agar tag tersebut menjadi **`Data Insights`** atau. **`Marketing`**

Kebijakan tag memungkinkan Anda memilih opsi untuk menerapkan aturan penandaan, mencegah operasi tag yang tidak sesuai, dan menentukan jenis sumber daya yang diterapkan penegakan hukum. Jika Anda tidak memilih opsi penegakan, kebijakan tag memungkinkan Anda membuat atau mengubah tag yang tidak sesuai, tetapi melaporkannya sebagai tidak sesuai di konsol. AWS Organizations

Untuk informasi selengkapnya tentang cara mengatur penegakan penandaan tingkat akun, lihat Kebijakan tag di AWS Organizations.

TagOptions

TagOptions adalah fitur penandaan yang AWS Service Catalog berlaku untuk produk yang disediakan di tingkat CloudFormation tumpukan jika diterapkan ke produk terkait. AWS Service Catalogmenyediakan TagOptions pustaka tempat Anda dapat menentukan pasangan kunci-nilai untuk dikaitkan dengan produk AndaAWS Service Catalog. Saat meluncurkan AWS Service Catalog produk, Anda harus memilih TagOption nilai untuk TagOption kunci yang ada yang terkait dengan portofolio atau produk tersebut untuk meluncurkan produk tersebut. Karena Anda menetapkan TagOptions pada tingkat portofolio atau produk, Anda dapat menerapkan taksonomi yang konsisten untuk menandai dengan portofolio yang dibagikan di seluruh akun dan wilayah.

Untuk informasi selengkapnya tentang TagOptions cara mengaturAWS Service Catalog, lihat AWS Service Catalog TagOption Perpustakaan.

Menghindari konflik antara kebijakan AWS Organizations tag dan AWS Service Catalog TagOptions

Jika Anda mengonfigurasi kebijakan AWS Organizations tag untuk akun di organisasi Anda, kami merekomendasikan hal berikut:

- Bagikan persyaratan untuk tag kesesuaian dengan administrator yang juga mengelola TagOptions portofolio dan produk. AWS Service Catalog
- Bagikan persyaratan untuk tag kesesuaian dengan pengguna akhir yang mungkin meluncurkan produk AWS Service Catalog dan menambahkan tag pengguna akhir opsional ke peluncuran produk mereka.

Misalkan Anda ingin meluncurkan produk AWS Service Catalog yang menggunakan TagOption kuncicity, dan Anda memiliki kebijakan tag yang mengharuskan kunci tag `city` untuk memiliki nilai tag kota AS, seperti**`Atlanta`**,**`San Francisco`**, atau**`Austin`**. AWS Service Catalogtidak

memungkinkan Anda untuk meluncurkan produk tanpa memilih TagOption nilai untuk TagOption kunci yang diperlukan untuk suatu produk.

Dalam hal ini, jika Anda memiliki TagOption nilai untuk TagOption kunci `city` yang mencakup kota-kota Amerika Selatan, seperti **`Rio de Janeiro`** atau**`Buenos Aires`**, tidak AWS Service Catalog akan meluncurkan produk. Sebagai gantinya, Anda harus memilih TagOption nilai yang mencakup kota AS selama peluncuran untuk mematuhi kebijakan tag.

Tabel berikut menyediakan skenario yang menjelaskan cara mengatasi masalah konflik penandaan yang mungkin Anda temui saat menggunakan kebijakan tag dan TagOptions pada saat yang bersamaan.

Skenario	Alasan	Solusi
Produk gagal diluncurkan karena tag yang tidak sesuai jika penegakan tag diperiksa dalam kebijakan tag.	Menentukan TagOptions dengan kunci dan nilai yang belum Anda tambahkan ke daftar tag yang sesuai yang diizinkan dalam kebijakan tag Anda. Menambahkan tag kustom opsional yang tidak sesuai dengan kebijakan tag Anda.	Jika Anda mengonfigurasi skema kapitalisasi tertentu dalam penegakan kapitalis asi kunci tag kebijakan tag, pastikan bahwa kunci tag dan kunci TagOptions tag kustom opsional konsisten dengan apa yang telah Anda tentukan dalam kebijakan tag Anda. Perhatikan ketika kotak penegakan kapitalisasi kunci tag tidak dicentang dalam kebijakan tag Anda, hal itu mengakibatkan semua kunci tag huruf kecil sesuai, dan memastikan kunci tag dan kunci TagOptions tag kustom opsional Anda konsisten (seperti semua huruf kecil) dengan apa yang Anda perlukan dalam kebijakan tag Anda.

Skenario	Alasan	Solusi
Produk gagal diluncurkan karena kapitalisasi kunci tag yang tidak sesuai.	Menentukan kapitalisasi dalam TagOptions kunci yang tidak konsisten dengan aturan penegakan kapitalisasi kebijakan tag Anda.	Konfigurasikan kebijakan tag Anda dengan benar. Jika Anda tidak menentukan kepatuhan kapitalisasi kunci tag, kapitalisasi kunci tag default semuanya huruf kecil. Selain itu, jika Anda tidak menentukan kepatuhan kapitalisasi kunci tag dalam kebijakan tag Anda, pastikan kunci TagOptions tag Anda semua huruf kecil untuk mematuhi aturan penegakan. AWS Service Catalog Jika Anda menggunakan kebijakan tag yang tidak mengaktifkan kepatuhan kapitalisasi, kebijakan tag tersebut hanya mengangga p semua kunci tag huruf kecil sesuai.
Produk gagal diluncurkan karena nilai tag yang tidak kompatibel.	Memilih nilai TagOptions tag untuk peluncuran produk yang tidak ada dalam kebijakan tag Anda Daftar yang diizinkan Kepatuhan Nilai Tag.	Kaitkan TagOptions dengan produk dan portofolio Anda yang konsisten dengan apa yang Anda perlukan dalam kebijakan tag daftar Nilai Tag Kepatuhan nilai tag yang diizinkan.

Pemantauan di AWS Service Catalog

Anda dapat memantau AWS Service Catalog sumber daya Anda menggunakan Amazon CloudWatch, yang mengumpulkan dan memproses data mentah dari metrik AWS Service Catalog yang dapat dibaca. Statistik ini dicatat untuk jangka waktu dua minggu, sehingga Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang kinerja layanan Anda. AWS Service CatalogData metrik secara otomatis dikirim ke CloudWatch dalam periode 1 menit. Untuk informasi selengkapnya CloudWatch, lihat Panduan CloudWatch Pengguna Amazon.

Untuk daftar metrik dan dimensi yang tersedia, lihat AWS Service Catalog CloudWatch Metrik.

Pemantauan adalah bagian penting dari pemeliharaan keandalan, ketersediaan, dan performa AWS Service Catalog solusi AWS Anda. Anda harus mengumpulkan data pemantauan dari semua bagian solusi AWS sehingga Anda dapat melakukan debug kegagalan multititik secara lebih mudah jika terjadi kegagalan. Namun sebelum Anda mulai memantau AWS Service Catalog, Anda harus membuat rencana pemantauan yang mencakup jawaban atas pertanyaan berikut:

- Apa saja sasaran pemantauan Anda?
- Sumber daya apa yang akan Anda pantau?
- Seberapa sering Anda akan memantau sumber daya ini?
- Alat pemantauan apa yang akan Anda gunakan?
- Siapa yang akan melakukan tugas pemantauan?
- Siapa yang harus diberi tahu saat terjadi kesalahan?

Alat Pemantauan

AWS menyediakan berbagai alat yang dapat Anda gunakan untuk memantau AWS Service Catalog. Anda dapat mengonfigurasi beberapa alat ini untuk melakukan pemantauan untuk Anda, sementara beberapa alat memerlukan intervensi manual. Kami menyarankan agar Anda mengautomasi tugas pemantauan sebanyak mungkin.

Alat Pemantauan Otomatis

Anda dapat menggunakan CloudWatch alarm Amazon untuk memantau AWS Service Catalog dan melaporkan gangguan.

CloudWatch alarm menonton satu metrik selama periode waktu yang Anda tentukan, dan melakukan satu atau beberapa tindakan berdasarkan nilai metrik relatif terhadap ambang batas tertentu selama beberapa periode waktu. Tindakannya adalah pemberitahuan yang dikirim ke topik Amazon Simple Notification Service (Amazon SNS) atau kebijakan Amazon EC2 Auto Scaling. CloudWatch alarm tidak memanggil tindakan hanya karena mereka berada dalam keadaan tertentu; negara harus telah berubah dan dipertahankan untuk sejumlah periode tertentu. Untuk mempelajari cara membuat alarm, lihat Membuat CloudWatch Alarm Amazon. Untuk informasi selengkapnya tentang menggunakan CloudWatch metrik Amazon denganAWS Service Catalog, lihatAWS Service Catalog CloudWatch Metrik.

AWS Service Catalog CloudWatch Metrik

Anda dapat memantau AWS Service Catalog sumber daya Anda menggunakan Amazon CloudWatch, yang mengumpulkan dan memproses data mentah dari metrik AWS Service Catalog yang dapat dibaca. Statistik ini dicatat untuk jangka waktu dua minggu, sehingga Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang kinerja layanan Anda. AWS Service CatalogData metrik secara otomatis dikirim ke CloudWatch dalam periode 1 menit. Untuk informasi selengkapnya CloudWatch, lihat Panduan CloudWatch Pengguna Amazon.

Topik

- Mengaktifkan Metrik CloudWatch
- Metrik dan dimensi yang tersedia
- Melihat metrik AWS Service Catalog

Mengaktifkan Metrik CloudWatch

CloudWatch Metrik Amazon diaktifkan secara default.

Metrik dan dimensi yang tersedia

Metrik dan dimensi yang AWS Service Catalog dikirim ke Amazon CloudWatch tercantum di bawah ini.

Metrik AWS Service Catalog

Namespace `AWS/ServiceCatalog` mencakup metrik berikut.

Metrik	Deskripsi
`ProvisionedProductLaunch`	Jumlah produk yang diluncurkan disediakan untuk produk tertentu dan penyediaan artefak dalam jangka waktu tertentu. Unit: Count (Jumlah) Statistik yang valid: Minimum, Maksimum, Jumlah, Rata-rata

Dimensi untuk AWS Service Catalog Metrik

AWS Service Catalogmengirimkan dimensi berikut ke Amazon CloudWatch.

Dimensi	Deskripsi
`State`	Dimensi ini memfilter data yang Anda minta untuk semua produk yang disediakan yang diluncurkan dengan status tertentu. Membantu Anda mengategorikan data berdasarkan status peluncuran. Status yang Valid: BERHASIL, GAGAL
`ProductId`	Dimensi ini memfilter data yang Anda minta untuk produk yang teridentifikasi saja. Hal ini membantu Anda menentukan produk yang tepat untuk diluncurkan.
`ProvisioningArtifactId`	Dimensi ini memfilter data yang Anda minta untuk penyediaan artefak yang teridentifikasi saja. Hal ini membantu Anda menentukan versi produk yang tepat untuk diluncurkan.

Melihat metrik AWS Service Catalog

Anda dapat melihat CloudWatch metrik Amazon di CloudWatch konsol Amazon, yang menyediakan tampilan sumber daya yang berbutir halus dan dapat disesuaikan, serta jumlah tugas yang berjalan dalam suatu layanan.

Topik

Melihat AWS Service Catalog Metrik di Konsol Amazon CloudWatch

Anda dapat melihat AWS Service Catalog metrik di CloudWatch konsol Amazon. CloudWatch Konsol Amazon menyediakan tampilan AWS Service Catalog metrik yang mendetail, dan Anda dapat menyesuaikan tampilan agar sesuai dengan kebutuhan Anda. Untuk informasi selengkapnya tentang Amazon CloudWatch, lihat Panduan CloudWatch Pengguna Amazon.

Untuk melihat metrik di konsol Amazon CloudWatch

1. Buka CloudWatch konsol Amazon di https://console.aws.amazon.com/cloudwatch/.
2. Di bagian Metrik di navigasi kiri, pilih Service Catalog.
3. Pilih metrik untuk dilihat.

Mencatat panggilan API AWS Service Catalog menggunakan AWS CloudTrail

AWS Service Catalogterintegrasi denganAWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan diAWS Service Catalog. CloudTrail menangkap semua panggilan API untuk AWS Service Catalog sebagai peristiwa. Panggilan yang direkam mencakup panggilan dari AWS Service Catalog konsol dan panggilan kode ke operasi API AWS Service Catalog ini. Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara berkelanjutan ke bucket Amazon S3, termasuk acara untuk. AWS Service Catalog Jika Anda tidak mengonfigurasi jejak, Anda masih dapat melihat peristiwa terbaru di CloudTrail konsol dalam Riwayat acara. Dengan menggunakan informasi yang dikumpulkan oleh CloudTrail, Anda dapat menentukan permintaan yang dibuatAWS Service Catalog, alamat IP dari mana permintaan dibuat, siapa yang membuat permintaan, kapan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat Panduan AWS CloudTrail Pengguna.

AWS Service Cataloginformasi di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuatnya. Ketika aktivitas terjadi diAWS Service Catalog, aktivitas tersebut dicatat dalam suatu CloudTrail peristiwa bersama dengan

peristiwa AWS layanan lainnya dalam riwayat Acara. Anda dapat melihat, mencari, dan mengunduh peristiwa terbaru di akun AWS. Untuk informasi selengkapnya, lihat Melihat peristiwa dengan Riwayat CloudTrail acara.

Untuk catatan berkelanjutan tentang peristiwa di akun AWS Anda, termasuk peristiwa untuk AWS Service Catalog, buat jejak. Jejak memungkinkan CloudTrail untuk mengirimkan file log ke bucket Amazon S3. Secara default, saat Anda membuat jejak di konsol, jejak tersebut berlaku untuk semua Wilayah AWS. Jejak mencatat peristiwa dari semua Wilayah di partisi AWS dan mengirimkan file log ke bucket Amazon S3 yang Anda tentukan. Selain itu, Anda dapat mengonfigurasi AWS layanan lain untuk menganalisis lebih lanjut dan menindaklanjuti data peristiwa yang dikumpulkan dalam CloudTrail log. Untuk informasi selengkapnya, lihat berikut:

- Gambaran umum untuk membuat jejak
- AWS CloudTraillayanan dan integrasi yang didukung
- Mengonfigurasi notifikasi Amazon SNS untuk AWS CloudTrail
- Menerima file log AWS CloudTrail dari beberapa wilayah dan Menerima file log AWS CloudTrail dari beberapa akun

CloudTrail mencatat semua AWS Service Catalog tindakan. Misalnya, panggilan ke`CreatePortfolio`, `CreateProduct` dan `UpdateProvisionedProduct` tindakan menghasilkan entri dalam file CloudTrail log.

Setiap peristiwa atau entri log berisi informasi tentang siapa yang membuat permintaan tersebut. Informasi identitas membantu Anda menentukan berikut ini:

- Bahwa permintaan tersebut dibuat dengan kredensial pengguna root atau pengguna (IAM) AWS Identity and Access Management.
- Baik permintaan tersebut dibuat dengan kredensial keamanan sementara untuk peran atau pengguna gabungan.
- Apakah permintaan dibuat oleh layanan AWS lain.

Untuk informasi selengkapnya, lihat Elemen userIdentity CloudTrail .

Memahami entri file log AWS Service Catalog

Trail adalah konfigurasi yang memungkinkan pengiriman peristiwa sebagai file log ke bucket Amazon S3 yang Anda tentukan. CloudTrail file log berisi satu atau lebih entri log. Peristiwa mewakili

permintaan tunggal dari sumber manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu. Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `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"
```

```
}
```

Preferensi branding konsol

AWS Service Catalogmemungkinkan administrator untuk menentukan preferensi pencitraan merek konsol untuk akun. Administrator dapat menggunakan merek konsol untuk menentukan nama perusahaan, gambar logo, dan warna primer dan sekunder (aksen) untuk berbagai komponen situs. Preferensi branding ini dapat dilihat oleh administrator dan pengguna akhir saat menggunakan konsol.

Preferensi branding konsol meningkatkan tampilan akun dan mencapai hal berikut:

- Menciptakan transisi visual yang mulus antara konsol dan aplikasi internal
- Membedakan akun yang digunakan oleh tim internal yang berbeda dalam perusahaan yang sama
- Membedakan akun di berbagai lingkungan, seperti pengembangan, pementasan, atau produksi

> **Note**
>
> Administrator menentukan preferensi pencitraan merek konsol di tingkat akun.

Untuk menentukan preferensi branding konsol

1. Di menu navigasi kiri, pilih Preferensi.
2. Pilih Edit untuk preferensi pencitraan merek mode terang atau mode gelap.
3. Unggah Logo, masukkan nama Merek, lalu pilih warna Primer dan Warna sekunder.
4. Pilih Simpan.

Untuk daftar wilayah yang AWS Service Catalog mendukung pencitraan merek konsol, tinjau Wilayah AWSdukungan untuk pencitraan merek konsol.

Wilayah AWSdukungan untuk preferensi merek konsol

AWS Service Catalogmendukung preferensi merek konsol dalam Wilayah AWS tercantum dalam tabel di bawah ini.

Wilayah AWS nama	Wilayah AWSidentitas	
US East (Northern Virginia)	us-east-1	
US East (Ohio)	us-east-2	
US West (Northern California)	us-west-1	
US West (Oregon)	as-barat-2	
Afrika (Cape Town)	af-selatan-1	
Asia Pasifik (Hong Kong)	ap-east-1	
Asia Pasifik (Jakarta)	ap-southeast-3	
Asia Pasifik (Mumbai)	ap-south-1	
Asia Pacific (Osaka)	ap-northeast-3	
Asia Pacific (Seoul)	ap-northeast-2	
Asia Pacific (Singapore)	ap-southeast-1	
Asia Pacific (Sydney)	ap-southeast-2	
Asia Pacific (Tokyo)	ap-northeast-1	
Canada (Central)	ca-sentral-1	
Europe (Frankfurt)	eu-central-1	
Europe (Ireland)	eu-west-1	
Europe (London)	eu-barat-2	
Eropa (Milan)	eu-selatan-1	
Eropa (Paris)	eu-west-3	
Europe (Stockholm)	eu-utara-1	

Wilayah AWS nama	Wilayah AWSidentitas	
Timur Tengah (Bahrain)	me-selatan-1	
Amerika Selatan (São Paulo)	sa-east-1	
AWS GovCloud (AS-Timur)	us-gov-east-1	
AWS GovCloud (AS-Barat)	us-gov-west-1	

Riwayat Dokumen

Tabel ini menjelaskan tambahan penting pada dokumentasi AWS Service Catalog.

Fitur	Deskripsi	Tanggal rilis
AWS Service Catalog	Untuk mempelajari tentang perubahan Hashicorp pada lisensi Terraform dan memperbarui ke jenis produk Eksternal, tinjau. Memperbarui produk Terraform Open Source yang ada dan produk yang disediakan ke jenis produk Eksternal	20 Oktober 2023
AWS Service Catalog	Untuk mempelajari tentang Berbagi portofolio dengan AWS Organizations dan memungkinkan AWS Service Catalog untuk melakukan sinkronisasiAWS Organizations, lihat AWSServiceCatalogOrgsDataSyncServiceRolePolicykebijakan dan peran AWSServiceRoleForServiceCatalogOrgsDataSyncterkait layanan.	April 14, 2023
AWS Service Catalog	Untuk mempelajari cara mengelola produk yang terhubung dengan git dan memungkinkan AWS Service Catalog untuk menyinkronkan templat di repositori eksternal ke AWS Service Catalog	18 November 2022

Fitur	Deskripsi	Tanggal rilis
	produk Anda, lihat AWSServiceCatalogSyncServiceRolePolicykebijakan dan peran terkait layanan. AWSServiceRoleForServiceCatalogSync	
AWS Service Catalog AppRegistry	Untuk mempelajari cara AppRegistry menyimpan AWS aplikasi Anda, koleksi sumber daya terkait, dan grup atribut aplikasi, lihat AWS Service Catalog AppRegistry.	15 Juni 2022
AWS Service Management Connector	Untuk mempelajari tentang Konektor untuk Manajemen Layanan JIRA dan ServiceNow, lihat Konektor Manajemen AWS Layanan.	9 Juni 2022
Konektor untuk Jira Service Management	Untuk mempelajari tentang pembaruan Konektor untuk Manajemen Layanan JIRA, lihat Konektor Manajemen AWS Layanan untuk Manajemen Layanan JIRA.	25 Mei 2021
Konektor untuk ServiceNow	Untuk mempelajari tentang pembaruan pada Konektor ServiceNow, lihat Konektor Manajemen AWS Layanan untuk ServiceNow.	7 April 2021

Fitur	Deskripsi	Tanggal rilis
Konektor untuk ServiceNow	Untuk mempelajari tentang pembaruan pada Konektor ServiceNow, lihat Konektor Manajemen AWS Layanan untuk ServiceNow.	24 September 2020
Service Quotas AWS	Untuk mempelajari tentang cara kerja AWS Service Catalog dengan Service Quotas AWS, lihat service quotas default AWS Service Catalog.	24 Maret 2020
Memulai Perpustakaan	Untuk mempelajari tentang perpustakaan templat produk yang dirancang dengan baik yang ditawarkan olehAWS Service Catalog, lihat Memulai Perpustakaan	10 Maret 2020
Panduan Versi	Untuk mempelajari tentang panduan versi produk, lihat Panduan Versi.	17 Desember 2019
Konektor untuk Jira Service Desk	Untuk mulai menggunak an Konektor untuk Meja Layanan JIRA, lihat Konektor Manajemen AWS Layanan untuk Meja Layanan JIRA.	21 November 2019
Konektor untuk ServiceNow	Untuk mempelajari tentang pembaruan pada Konektor ServiceNow, lihat Konektor Manajemen AWS Layanan untuk ServiceNow.	18 November 2019

Fitur	Deskripsi	Tanggal rilis
Bab keamanan baru	Untuk mempelajari tentang keamanan di AWS Service Catalog, lihat Keamanan di AWS Service Catalog.	31 Oktober 2019
Mengubah pemilik produk yang disediakan	Untuk mempelajari tentang cara mengubah pemilik produk yang disediakan, lihat Mengubah Pemilik Produk yang disediakan.	31 Oktober 2019
Batasan pembaruan sumber daya baru	Untuk mempelajari tentang cara penggunaan batasan RESOURCE_UPDATE untuk memperbarui tanda dalam produk yang disediakan, lihat Batasan Pembaruan Tanda AWS Service Catalog.	17 April 2019
Konektor untuk ServiceNow	Untuk mulai menggunakan Konektor ServiceNow, lihat Konektor Manajemen AWS Layanan untuk ServiceNow.	19 Maret 2019
Support untuk AWS CloudFormation StackSets	Untuk mulai menggunak an AWS CloudFormation StackSets, lihat Menggunak an AWS CloudFormation StackSets.	14 November 2018
Tindakan layanan mandiri	Untuk mulai menggunakan tindakan layanan mandiri, lihat Tindakan Layanan AWS CloudFormation.	17 Oktober 2018

Fitur	Deskripsi	Tanggal rilis
CloudWatch Metrik Amazon	Untuk mempelajari CloudWatch metrik Amazon, lihat AWS Service CatalogAmazon CloudWatch.	26 September 2018
Support untuk TagOptions	Untuk mengelola tag, lihat AWS Service Catalog TagOptionPerpustakaan.	28 Juni 2017
Mengimpor portofolio	Untuk mengimpor portofolio yang dibagikan dari AWS akun lain, lihat Mengimpor Portofolio.	16 Februari 2016
Pembaruan informasi perizinan	Untuk memberikan akses ke tampilan konsol pengguna akhir, lihat Akses konsol untuk pengguna akhir.	16 Februari 2016
Rilisan awal	Ini adalah rilisan awal dari Panduan Administrator AWS Service Catalog.	9 Juli 2015

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.