Guide de l'administrateur

AWS Service Catalog

AWS Service Catalog: Guide de l'administrateur

Table of Contents

Qu'est-ce que Service Catalog ?

Service Catalog permet aux entreprises de créer et de gérer des catalogues de services informatiques approuvés. AWS Ces services informatiques peuvent inclure des images de machines virtuelles, des serveurs, des logiciels, des bases de données, etc., ainsi que des architectures d'applications complètes à plusieurs niveaux.

Service Catalog permet aux entreprises de gérer de manière centralisée les services informatiques couramment déployés, et les aide à assurer une gouvernance cohérente et à répondre aux exigences de conformité. Les utilisateurs finaux peuvent déployer rapidement uniquement les services informatiques approuvés dont ils ont besoin, en respectant les contraintes définies par votre organisation.

Service Catalog offre les avantages suivants :

- Normalisation

  Administrez et gérez des ressources approuvées en limitant l'emplacement où le produit peut être lancé, le type d'instance qui peut être utilisé et de nombreuses autres options de configuration. Cela se traduit par un environnement normalisé pour le provisionnement de produits pour l'ensemble de votre entreprise.
- Découverte et lancement en libre service

  Les utilisateurs parcourent des listes de produits (services ou applications) auxquels ils ont accès, et recherchent le produit qu'ils souhaitent utiliser et lancer par eux-mêmes en tant que produit provisionné.
- Contrôle précis des accès (FGAC)

  Les administrateurs assemblent des portefeuilles de produits à partir de leur catalogue, ajoutent des contraintes et des balises de ressources à utiliser lors du provisionnement, puis accordent l'accès au portefeuille par le biais d'utilisateurs et de groupes AWS Identity and Access Management (IAM).
- Extensibilité et contrôle de version

  Les administrateurs peuvent ajouter un produit à un nombre quelconque de portefeuilles et le restreindre sans créer une autre copie. La mise à jour du produit vers une nouvelle version propage la mise à jour vers tous les produits dans tous les portefeuilles qui le référencent.

Pour plus d'informations, consultez la page détaillée du Service Catalog.

L'API Service Catalog fournit un contrôle programmatique sur toutes les actions de l'utilisateur final au lieu d'utiliser le. AWS Management Console Pour plus d'informations, consultez le Guide du développeur de Service Catalog.

Vidéo : Présentation de AWS Service Catalog

Cette vidéo (7:27) explique comment créer, organiser et gérer un catalogue de produits organisé, et comment partager des AWS produits avec un certain niveau d'autorisation. Par conséquent, les utilisateurs finaux peuvent rapidement fournir des ressources informatiques approuvées sans accès direct aux AWS services sous-jacents.

Introduction à AWS Service Catalog

Présentation du Service Catalog

Lorsque vous débuterez avec Service Catalog, vous aurez tout intérêt à comprendre ses composants et les flux de travail initiaux pour les administrateurs et les utilisateurs finaux.

Users

Service Catalog prend en charge les types d'utilisateurs suivants :

- Administrateurs de catalogue (administrateurs) : gérez un catalogue de produits (applications et services), organisez-les en portefeuilles et accordez l'accès aux utilisateurs finaux. Les administrateurs de catalogue préparent AWS CloudFormation des modèles, configurent les contraintes et gèrent les rôles IAM pour les produits afin de permettre une gestion avancée des ressources.
- Utilisateurs finaux : recevez les AWS informations d'identification de leur service informatique ou de leur responsable et utilisez-les AWS Management Console pour lancer les produits auxquels ils ont accès. Parfois appelés simplement utilisateurs, les utilisateurs finaux peuvent bénéficier d'autorisations différentes selon vos besoins opérationnels. Par exemple, un utilisateur peut avoir le niveau d'autorisation maximum (pour lancer et gérer toutes les ressources requises par les produits qu'il utilise) ou uniquement l'autorisation d'utiliser des fonctions de service particulières.

Produits

Un produit est un service informatique que vous souhaitez mettre à disposition pour un déploiementAWS. Un produit comprend une ou plusieurs AWS ressources, telles que des instances EC2, des volumes de stockage, des bases de données, des configurations de surveillance, des composants réseau ou des AWS Marketplace produits packagés. Un produit peut être une instance de calcul unique exécutant AWS Linux, une application Web multiniveau entièrement configurée s'exécutant dans son propre environnement, ou tout autre élément intermédiaire.

Vous créez un produit en important un AWS CloudFormation modèle. AWS CloudFormationles modèles définissent les AWS ressources requises pour le produit, les relations entre les ressources et les paramètres que les utilisateurs finaux peuvent utiliser lorsqu'ils lancent le produit pour configurer des groupes de sécurité, créer des paires de clés et effectuer d'autres personnalisations.

HashiCorp Support pour Terraform Open Source et Terraform Cloud

AWS Service Catalogpermet un provisionnement rapide en libre-service avec gouvernance de vos configurations HashiCorp Terraform Open Source et Terraform Cloud au sein de celles-ci. AWS Vous pouvez utiliser Service Catalog comme un outil unique pour organiser, gérer et distribuer vos configurations Terraform à grande échelle. AWS Vous pouvez accéder aux principales fonctionnalités de Service Catalog, notamment le catalogage de modèles Terraform standardisés et préapprouvés, le contrôle d'accès, l'attribution du moindre privilège, le versionnement, le balisage et le partage avec des milliers de comptes. AWS Vos utilisateurs finaux voient une simple liste de produits et de versions auxquels ils ont accès, et peuvent ensuite déployer ces produits en une seule action.

Pour en savoir plus et pour suivre un didacticiel sur le produit Terraform, consultez. Commencer à utiliser un produit Terraform

Produits provisionnés

AWS CloudFormationles stacks facilitent la gestion du cycle de vie de votre produit en vous permettant de provisionner, d'étiqueter, de mettre à jour et de résilier votre instance de produit en tant qu'unité unique. Une pile AWS CloudFormation comprend un modèle AWS CloudFormation écrit au format JSON ou YAML, ainsi que son ensemble associé de ressources. Un produit provisionné est une pile. Lorsqu'un utilisateur final lance un produit, l'instance du produit fournie par Service Catalog est une pile contenant les ressources nécessaires pour exécuter le produit. Pour plus d'informations, consultez le AWS CloudFormation guide de l'utilisateur.

Portefeuilles

Un portefeuille est un ensemble de produits contenant des informations de configuration. Les portefeuilles vous permettent de gérer qui peut utiliser un produit en particulier et de quelle façon. Service Catalog vous permet de créer un portefeuille personnalisé pour chaque type d'utilisateur de votre organisation et d'accorder l'accès au portefeuille approprié de manière sélective. Lorsque vous ajoutez une nouvelle version d'un produit à un portefeuille, cette version est automatiquement mise à la disposition de tous les utilisateurs actuels du portefeuille en question.

Vous pouvez également partager vos portefeuilles avec d'autres AWS comptes et autoriser l'administrateur de ces comptes à distribuer vos portefeuilles avec des contraintes supplémentaires, telles que la limitation des instances EC2 qu'un utilisateur peut créer. Grâce à l'utilisation de portefeuilles, d'autorisations, du partage et de contraintes, vous pouvez vous assurer que les utilisateurs lancent des produits qui sont correctement configurés pour les besoins et les normes de l'entreprise.

Gestion des versions

Service Catalog vous permet de gérer plusieurs versions des produits de votre catalogue. Cette approche vous permet d'ajouter de nouvelles versions de modèles et de ressources associées en fonction des mises à jour logicielles ou des modifications de configuration.

Lorsque vous créez une nouvelle version d'un produit, la mise à jour est automatiquement distribuée à tous les utilisateurs ayant accès au produit, ce qui leur permet de sélectionner la version du produit à utiliser. Les utilisateurs peuvent rapidement et facilement mettre à jour des instances du produit en cours d'exécution vers la nouvelle version.

Autorisations

Accorder l'accès à un portefeuille à un utilisateur permet à l'utilisateur en question de parcourir le portefeuille et de lancer les produits y figurant. Vous appliquez des autorisations AWS Identity and Access Management (IAM) pour contrôler qui peut consulter et modifier votre catalogue. Les autorisations IAM peuvent être attribuées aux utilisateurs, aux groupes et aux rôles IAM.

Lorsqu'un utilisateur lance un produit auquel un rôle IAM est attribué, Service Catalog utilise ce rôle pour lancer les ressources cloud du produit à l'aide AWS CloudFormation de. En attribuant un rôle IAM à chaque produit, vous pouvez éviter d'autoriser les utilisateurs à effectuer des opérations non approuvées et leur permettre de provisionner des ressources à l'aide du catalogue.

Constraints

Les contraintes contrôlent la manière dont vous pouvez déployer des AWS ressources spécifiques pour un produit. Vous pouvez les utiliser pour appliquer des limites aux produits à des fins de gouvernance ou de contrôle des coûts. Il existe différents types de contraintes AWS Service Catalog : les contraintes de lancement, les contraintes de notification et les contraintes de modèle.

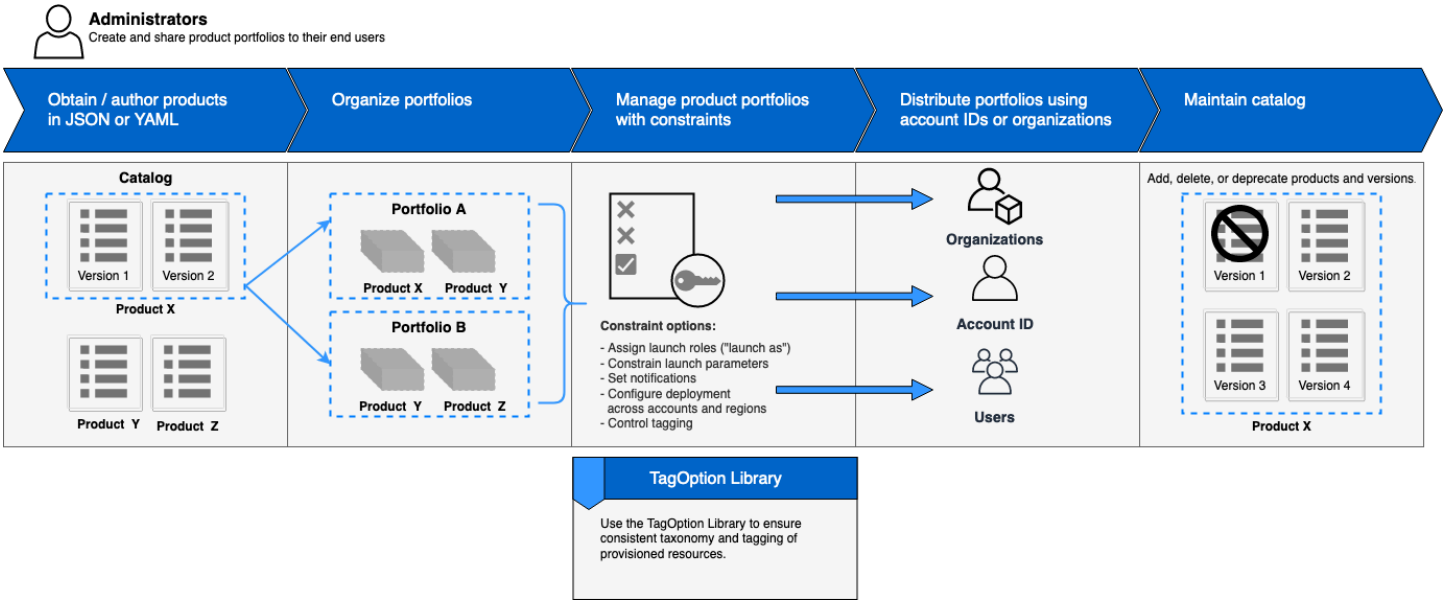
Les contraintes de lancement vous permettent de spécifier un rôle pour un produit au sein d'un portefeuille. Utilisez ce rôle pour provisionner les ressources lors du lancement, afin de limiter les autorisations des utilisateurs sans affecter la capacité des utilisateurs à approvisionner des produits à partir du catalogue.

Les contraintes de notification vous permettent de recevoir des notifications concernant des événements de stack via une rubrique Amazon SNS.

Les contraintes de modèle limitent les paramètres de configuration mis à la disposition de l'utilisateur lors du lancement du produit (par exemple, les types d'instance EC2 ou les plages d'adresses IP). Les contraintes de modèle vous permettent de réutiliser des modèles AWS CloudFormation génériques pour les produits et d'appliquer des restrictions aux modèles pour chaque produit ou portefeuille.

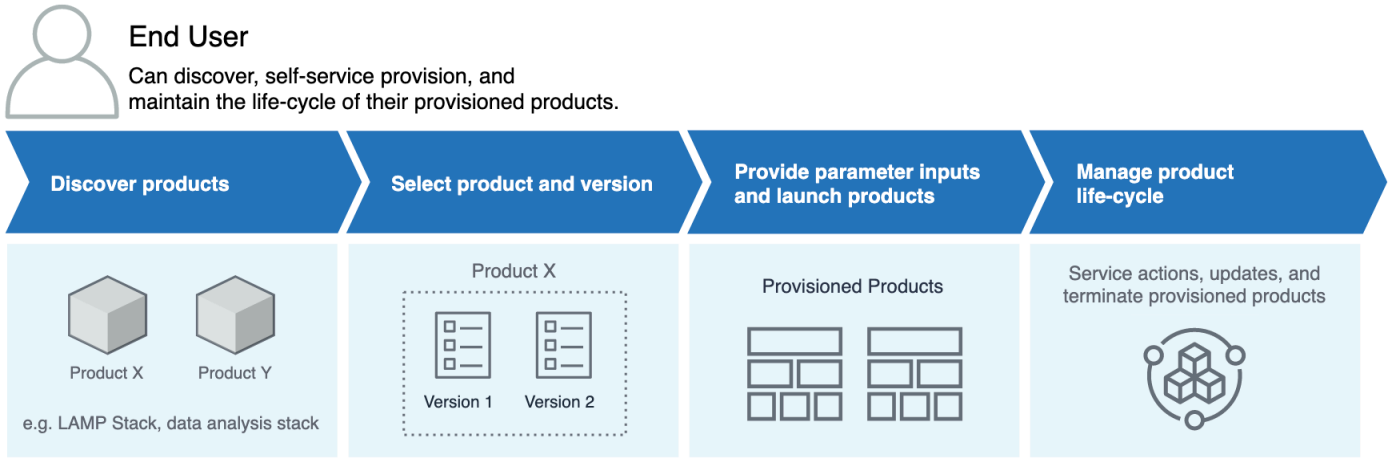
Flux de travail initial pour un administrateur

Ce diagramme montre le flux de travail initial permettant à un administrateur de créer un catalogue.



Flux de travail initial pour un utilisateur final

Ce diagramme montre le flux de travail initial d'un utilisateur final.



Quotas de service AWS Service Catalog par défaut

Votre AWS compte possède les quotas par défaut suivants pourAWS Organizations, contrainte, portefeuille, produit, produit approvisionné, région, action de service et TagOptions.

Vous pouvez l'utiliser Service Quotas pour gérer vos quotas ou pour demander une augmentation de quota. Pour plus d'informationsService Quotas, voir Qu'est-ce que les Quotas de Service ? dans le guide de Service Quotas l'utilisateur. Pour de plus amples informations sur une demande d'augmentation de quota, veuillez consulter Demande d'augmentation de quota.

AWS Organizations

- Administrateurs AWS Service Catalog délégués par organisation : 50

Quotas de contraintes

- Contraintes par produit par portefeuille : 100

Quotas de portefeuille

- Utilisateurs, groupes et rôles par portefeuille : 100
- Produits par portefeuille : 150

- Balises par portefeuille : 20
- Comptes partagés par portefeuille : 5 000
- Valeurs de balise par clé de balise : 25

Quotas de produits

- Utilisateurs, groupes et rôles par produit : 200
- Versions de produit par produit : 100
- Balises par produit : 20
- Valeurs de balise par clé de balise : 25

Quotas de produits provisionné

- Balises par produit provisionné : 50

Quotas régionaux

- Portefeuilles : 100
- Produits : 350

Quotas d'actions de service

- Actions de service par région : 200
- Associations d'actions de service par version de produit : 25

TagOptions quotas

- TagOptions par ressource : 25
- Valeurs par TagOption : 25

Configuration AWS Service Catalog

Avant de commencer AWS Service Catalog, effectuez les tâches suivantes.

Rubriques

- Inscrivez-vous pour un Compte AWS
- Création d'un utilisateur doté d'un accès administratif

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des AWS services et des ressources de ce compte. Pour des raisons de sécurité, attribuez un accès administratif à un utilisateur et utilisez uniquement l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connectez-vous en tant qu'utilisateur disposant d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.

2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

   Pour obtenir des instructions, voir Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

Pour activer l’accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

  Créez un jeu d’autorisations. Suivez les instructions de la rubrique Création d’un jeu d’autorisations du Guide de l’utilisateur AWS IAM Identity Center .

- Utilisateurs gérés dans IAM par un fournisseur d’identité :

  Créez un rôle pour la fédération d’identité. Pour plus d’informations, voir la rubrique Création d’un rôle pour un fournisseur d’identité tiers (fédération) du Guide de l’utilisateur IAM.

- Utilisateurs IAM :
  - Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique Création d’un rôle pour un utilisateur IAM du Guide de l’utilisateur IAM.
  - (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d’utilisateurs. Suivez les instructions de la rubrique Ajout d’autorisations à un utilisateur (console) du Guide de l’utilisateur IAM.

Accorder des autorisations aux AWS Service Catalog administrateurs

En tant qu'administrateur de catalogue, vous devez avoir accès à la vue de la console de l'AWS Service Catalogadministrateur et disposer des autorisations IAM qui vous permettent d'effectuer des tâches telles que les suivantes :

- Création et gestion de portefeuilles
- Création et gestion de produits

- Ajout de contraintes de modèle pour contrôler les options qui sont disponibles pour les utilisateurs finaux lorsqu'ils lancent un produit
- Ajout de contraintes de lancement pour définir les rôles IAM AWS Service Catalog assumés lorsque les utilisateurs finaux lancent des produits
- Attribution aux utilisateurs finaux d'un accès à vos produits

Vous, ou un administrateur qui gère vos autorisations IAM, devez associer à votre utilisateur, groupe ou rôle IAM les politiques requises pour suivre ce didacticiel.

Pour accorder des autorisations à un administrateur de catalogue

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, choisissez Gestion des accès, puis Utilisateurs. Si vous avez déjà créé un utilisateur IAM que vous souhaitez utiliser en tant qu'administrateur du catalogue, choisissez le nom d'utilisateur, puis choisissez Ajouter des autorisations. Sinon, créez un utilisateur comme suit :
   a. Sélectionnez Ajouter un utilisateur.
   b. Pour User name (nom d'utilisateur), saisissez **`ServiceCatalogAdmin`**.
   c. Sélectionnez Programmatic access (Accès par programme) et AWS Management Console Access (Accès).
   d. Sélectionnez Next: Permissions (Étape suivante : autorisations).
3. Choisissez Attach existing policies directly (Attacher directement les politiques existantes).
4. Choisissez Créer une politique, puis effectuez les opérations suivantes :
   a. Sélectionnez l'onglet JSON.
   b. Copiez l'exemple de politique suivant et collez-le dans le document de stratégie :

```
{
    "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. Choisissez Suivant : Balises.

d. (Facultatif) Choisissez Ajouter une balise pour associer une paire clé-valeur à la ressource. Vous pouvez ajouter un maximum de 50 balises.

> **Note**
>
> Les balises sont des paires clé-valeur que vous pouvez ajouter aux ressources. Cela permet d'identifier, d'organiser et de rechercher des ressources. Pour plus d'informations, consultez la section AWSRessources relatives au balisage dans le Guide de Références générales AWS référence.

e. Choisissez Suivant : vérification.

f. Pour Policy Name, tapez **`ServiceCatalogAdmin-AdditionalPermissions`**.

> **Important**
>
> Vous devez accorder aux administrateurs Amazon S3 des autorisations pour accéder aux modèles AWS Service Catalog stockés dans Amazon S3. Pour plus d'informations, consultez les exemples de politiques utilisateur dans le guide de l'utilisateur d'Amazon Simple Storage Service.

g. Choisissez Create Policy (Créer une politique).

5. Revenez dans la fenêtre de navigateur avec la page des autorisations, puis choisissez Refresh.
6. Dans le champ de recherche, tapez **`ServiceCatalog`** pour filtrer la liste de stratégies.
7. Cochez les cases correspondant aux **`ServiceCatalogAdmin-AdditionalPermissions`**politiques **`AWSServiceCatalogAdminFullAccess`**et, puis choisissez Suivant : Réviser.
8. Si vous mettez à jour un utilisateur, choisissez Add permissions.

   Si vous créez un utilisateur, choisissez Create user. Vous pouvez télécharger ou copier les informations d'identification, puis choisir Close.
9. Pour vous connecter en tant qu'utilisateur de catalogue, utilisez l'URL propre à votre compte. Pour trouver cette URL, choisissez Dashboard dans le volet de navigation, puis Copy Link. Collez le lien dans votre navigateur, puis utilisez le nom et le mot de passe de l'utilisateur IAM que vous avez créé ou mis à jour dans cette procédure.

Accorder des autorisations aux utilisateurs AWS Service Catalog finaux

Pour que l'utilisateur final puisse utiliser AWS Service Catalog, vous devez lui accorder l'accès à la vue de la console Utilisateur final AWS Service Catalog. Pour accorder l'accès, vous devez associer des politiques à l'utilisateur, au groupe ou au rôle IAM utilisé par l'utilisateur final. Dans la procédure suivante, nous associons la **`AWSServiceCatalogEndUserFullAccess`**politique à un groupe IAM.

Pour accorder des autorisations à un groupe d'utilisateurs finaux

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, sélectionnez User groups (Groupes d'utilisateurs).
3. Choisissez Créer un groupe et procédez comme suit :

   a. Dans Nom du groupe d'utilisateurs, tapez**`Endusers`**.

   b. Dans le champ de recherche, tapez **`AWSServiceCatalog`** pour filtrer la liste de stratégies.

   c. Cochez la case correspondant à la **`AWSServiceCatalogEndUserFullAccess`**politique. Vous avez également la possibilité de choisir **`AWSServiceCatalogEndUserReadOnlyAccess`** à la place.

   d. Choisissez Create Group.

4. Dans le panneau de navigation, choisissez utilisateurs.
5. Choisissez Ajouter des utilisateurs et procédez comme suit :

    a. Pour User name, tapez le nom de l'utilisateur.

    b. Sélectionnez Mot de passe - Accès à la console de AWS gestion.

    c. Sélectionnez Next: Permissions (Étape suivante : autorisations).

    d. Choisissez Add user to group (ajouter un utilisateur au groupe).

    e. Cochez la case en regard du groupe Endusers, puis choisissezSuivants : Balises et Suivant : Vérification.

    f. Sur la page Review (Vérification), choisissez Create user (Créer un utilisateur). Téléchargez ou copiez les informations d'identification, puis choisissez Close.

Installer et configurer le moteur de provisionnement Terraform

Pour utiliser correctement les produits Terraform avecAWS Service Catalog, vous devez installer et configurer un moteur de provisionnement Terraform dans le même compte que celui où vous allez administrer les produits Terraform. Pour commencer, vous pouvez utiliser le moteur de provisionnement Terraform fourni parAWS, qui installe et configure le code et l'infrastructure nécessaires au fonctionnement du moteur de provisionnement Terraform. AWS Service Catalog Cette configuration unique prend environ 30 minutes. AWS Service Catalogfournit un GitHub référentiel contenant des instructions sur l'installation et la configuration du moteur de provisionnement Terraform.

Détermination des files d'attente

Lorsque vous appelez une opération de provisionnement, AWS Service Catalog prépare un message de charge utile à envoyer à la file d'attente correspondante dans le moteur de provisionnement. Afin de créer l'ARN pour la file d'attente, AWS Service Catalog fait les hypothèses suivantes :

- Le moteur de provisionnement se trouve dans le compte du propriétaire du produit
- Le moteur de provisionnement est situé dans la même région que celle dans laquelle l'appel AWS Service Catalog a été effectué
- Les files d'attente du moteur de provisionnement suivent le schéma de dénomination documenté détaillé ci-dessous

Par exemple, s'il ProvisionProduct est appelé `us-east-1` depuis le compte 1111111111 à l'aide d'un produit créé par le compte 0000000000000, cela suppose que AWS Service Catalog le bon ARN SQS est. `arn:aws:sqs:us-east-1:0000000000000:ServiceCatalogTerraformOSProvisionOperationQueue`

La même logique s'applique à la fonction Lambda appelée par. `DescribeProvisioningParameters`

Ajouter Confused Deputy à votre moteur de provisionnement Terraform

Touches contextuelles adjointes confuses sur les terminaux pour restreindre l'accès aux opérations **`lambda:Invoke`**

La fonction Lambda de l'analyseur de paramètres créée AWS Service Catalog par les moteurs fournis dispose d'une politique d'accès qui accorde des autorisations `lambda:Invoke` entre comptes uniquement au principal du service : 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"
    }
  ]
}
```

Il doit s'agir de la seule autorisation nécessaire pour que l'AWS Service Catalogintégration fonctionne correctement. Toutefois, vous pouvez restreindre davantage ce paramètre à l'aide de la clé de contexte `aws:SourceAccount` Confused Deputy. When AWS Service Catalog envoie des messages à ces files d'attente, AWS Service Catalog remplit la clé avec l'ID du compte d'approvisionnement. Cela est utile lorsque vous avez l'intention de distribuer des produits via le partage de portefeuille et que vous souhaitez vous assurer que seuls des comptes spécifiques utilisent votre moteur.

Par exemple, vous pouvez restreindre votre moteur pour n'autoriser que les demandes provenant de 000000000000 et 111111111111 en utilisant la condition ci-dessous :

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

Touches contextuelles adjointes confuses sur les terminaux pour restreindre l'accès aux opérations **`sqs:SendMessage`**

Les files d'attente Amazon SQS créées AWS Service Catalog par les moteurs fournis pour les opérations de provisionnement sont soumises à une politique d'accès qui accorde des autorisations `sqs:SendMessage` entre comptes (et KMS associés) uniquement au principal du service : 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"
    }
  ]
}
```

Il doit s'agir de la seule autorisation nécessaire pour que l'AWS Service Catalogintégration fonctionne correctement. Toutefois, vous pouvez restreindre davantage ce paramètre à l'aide de la clé de contexte `aws:SourceAccount` Confused Deputy. When AWS Service Catalog envoie des messages à ces files d'attente, AWS Service Catalog remplit les clés avec l'ID du compte d'approvisionnement. Cela est utile lorsque vous avez l'intention de distribuer des produits via le partage de portefeuille et que vous souhaitez vous assurer que seuls des comptes spécifiques utilisent votre moteur.

Par exemple, vous pouvez restreindre votre moteur pour n'autoriser que les demandes provenant de 000000000000 et 111111111111 en utilisant la condition ci-dessous :

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

Démarrage

Vous pouvez commencer en AWS Service Catalog utilisant l'un des modèles de produits bien conçus de la bibliothèque de mise en route ou en suivant les étapes de l'un des didacticiels de mise en route.

Dans le didacticiel, vous effectuez des tâches en tant qu'administrateur du catalogue et utilisateur final. En tant qu'administrateur du catalogue, vous créez un portefeuille, puis un produit. En tant qu'utilisateur final, vous vérifiez que vous pouvez accéder à la console utilisateur final et lancer le produit. Le produit est l'un des suivants :

- Un environnement de développement cloud qui s'exécute sur Amazon Linux et est basé sur un AWS CloudFormation modèle qui définit les AWS ressources que le produit peut utiliser.
- Un environnement open source qui s'exécute sur un moteur de provisionnement Terraform et est basé sur un fichier de configuration tar.gz qui définit les AWS ressources que le produit peut utiliser.

> **Note**
>
> Avant de commencer, assurez-vous d'avoir terminé les actions dansConfiguration AWS Service Catalog.

Rubriques

Bibliothèque de mise en route

AWS Service Catalog fournit une bibliothèque de mise en route de modèles de produits bien architecturés pour que vous puissiez démarrer rapidement. Vous pouvez copier tous les produits de nos portefeuilles de bibliothèque de mise en route sur votre propre compte, puis les personnaliser en fonction de vos besoins.

Rubriques

Prérequis

Avant d'utiliser les modèles de notre bibliothèque de mise en route, assurez-vous que vous disposez des éléments suivants :

- Autorisations requises pour utiliser des modèles AWS CloudFormation. Pour plus d'informations, consultez Contrôle de l'accès avec AWS Identity and Access Management.
- Autorisations d'administrateur requises pour gérer AWS Service Catalog. Pour plus d'informations, consultez the section called "Gestion de l'identité et des accès".

En savoir plus

Pour plus d'informations sur le framework Well-Architected, consultez Well-ArchitectedAWS.

Commencer à utiliser un AWS CloudFormation produit

Vous pouvez commencer en AWS Service Catalog utilisant l'un des modèles de produits bien conçus de la bibliothèque de mise en route ou en suivant les étapes du didacticiel de mise en route.

Dans le didacticiel, vous effectuez des tâches en tant qu'administrateur du catalogue et utilisateur final. En tant qu'administrateur du catalogue, vous créez un portefeuille, puis un produit. En tant qu'utilisateur final, vous vérifiez que vous pouvez accéder à la console utilisateur final et lancer le produit. Le produit est un environnement de développement cloud qui s'exécute sur Amazon Linux et est basé sur un AWS CloudFormation modèle qui définit les AWS ressources que le produit peut utiliser.

> **Note**
>
> Avant de commencer, assurez-vous d'avoir terminé les actions dansConfiguration AWS Service Catalog.

Rubriques

- Étape 2 : Création d'une paire de clés
- Étape 3 : Création d'un portefeuille
- Étape 4 : Création d'un nouveau produit dans le portefeuille
- Étape 5 : ajouter une contrainte de modèle pour limiter la taille de l'instance
- Étape 6 : ajouter une contrainte de lancement pour attribuer un rôle IAM
- Étape 7 : Accorder aux utilisateurs finaux l'accès au portefeuille
- Étape 8 : Testez l'expérience de l'utilisateur final

Étape 1 : Téléchargez le AWS CloudFormation modèle

Vous pouvez utiliser des AWS CloudFormation modèles pour configurer et approvisionner des portefeuilles et des produits. Ces modèles sont des fichiers texte qui peuvent être formatés en JSON ou YAML et décrivent les ressources que vous souhaitez mettre en service. Pour plus d'informations, consultez Formats de modèle dans le Guide de l'utilisateur AWS CloudFormation. Vous pouvez utiliser l'AWS CloudFormationéditeur ou un éditeur de texte de votre choix pour créer et enregistrer des modèles. Dans ce didacticiel, nous vous proposons un modèle simple, afin que vous puissiez commencer. Le modèle lance une instance Linux unique configurée pour l'accès SSH.

> **Note**
>
> L'utilisation AWS CloudFormation de modèles nécessite des autorisations spéciales. Avant de commencer, assurez-vous que vous disposez des autorisations appropriées. Pour plus d'informations, consultez les conditions préalables dansBibliothèque de mise en route.

Téléchargement du modèle

L'exemple de modèle fourni pour ce didacticiel est disponible à l'adresse https://awsdocs.s3.amazonaws.com/servicecatalog/development-environment.template. `development-environment.template`

Présentation du modèle

Le texte de l'exemple de modèle est le suivant :

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

Ressources du modèle

Le modèle déclare les ressources à créer lorsque le produit est lancé. Il se compose des sections suivantes :

- AWSTemplateFormatVersion(facultatif) — Version du format de AWS modèle utilisée pour créer ce modèle. La dernière version du format du modèle est le 09/09/2010 et est actuellement la seule valeur valide.
- Description (facultatif) — Description du modèle.
- Paramètres (facultatif) — Les paramètres que votre utilisateur doit spécifier pour lancer le produit. Pour chaque paramètre, le modèle inclut une description et des contraintes qui doivent être satisfaites par la valeur saisie. Pour plus d'informations sur les contraintes, consultez Utilisation de contraintes AWS Service Catalog.

  Le `KeyName` paramètre vous permet de spécifier le nom d'une paire de clés Amazon Elastic Compute Cloud (Amazon EC2) que les utilisateurs finaux doivent fournir lors AWS Service Catalog du lancement de votre produit. Vous allez créer la paire de clés à l'étape suivante.
- Métadonnées (facultatif) : objets fournissant des informations supplémentaires sur le modèle. La clé AWS: : CloudFormation : :Interface définit la manière dont la vue de la console de l'utilisateur final affiche les paramètres. La propriété `ParameterGroups` définit la façon dont les paramètres

sont regroupés et les en-têtes pour ces groupes. La propriété `ParameterLabels` définit des noms de paramètre conviviaux. Lorsqu'un utilisateur spécifie des paramètres pour lancer un produit basé sur ce modèle, la vue de la console Utilisateur final affiche le paramètre étiqueté `Server size:` sous l'en-tête `Instance configuration`, et les paramètres étiquetés `Key pair:` et `CIDR range:`, sous l'en-tête `Security configuration`.

- Mappages (facultatif) : mappage de clés et de valeurs associées que vous pouvez utiliser pour spécifier des valeurs de paramètres conditionnelles, comme dans une table de recherche. Vous pouvez associer une clé à une valeur correspondante en utilisant la fonction FindInMap intrinsèque Fn : : dans les sections Ressources et Sorties. Le modèle ci-dessus inclut une liste de AWS régions et l'Amazon Machine Image (AMI) correspondant à chacune d'elles. AWS Service Catalogutilise ce mappage pour déterminer l'AMI à utiliser en fonction de la AWS région sélectionnée par l'utilisateur dans leAWS Management Console.
- Ressources (obligatoire) — Empilez les ressources et leurs propriétés. Vous pouvez faire référence aux ressources dans les sections Ressources et Sorties du modèle. Dans le modèle ci-dessus, nous indiquons une instance EC2 exécutant Amazon Linux et un groupe de sécurité qui autorise l'accès SSH à l'instance. La section Propriétés de la ressource d'instance EC2 utilise les informations saisies par l'utilisateur pour configurer le type d'instance et un nom de clé pour l'accès SSH.

  AWS CloudFormationutilise la AWS région actuelle pour sélectionner l'ID AMI parmi les mappages définis précédemment et lui assigne un groupe de sécurité. Le groupe de sécurité est configuré pour autoriser l'accès entrant sur le port 22 à partir de la plage d'adresses IP CIDR que spécifie l'utilisateur.
- Sorties (facultatif) : texte indiquant à l'utilisateur que le lancement du produit est terminé. Le modèle fourni obtient le nom DNS public de l'instance lancée et l'affiche pour l'utilisateur. L'utilisateur a besoin du nom DNS pour se connecter à l'instance à l'aide de SSH.

  Pour plus d'informations sur la page d'anatomie du modèle, reportez-vous à la section Référence du modèle dans le guide de AWS CloudFormation l'utilisateur.

Étape 2 : Création d'une paire de clés

Pour permettre à vos utilisateurs finaux de lancer le produit basé sur le modèle d'exemple de ce didacticiel, vous devez créer une paire de clés Amazon EC2. Une paire de clés est une combinaison d'une clé publique utilisée pour chiffrer les données et d'une clé privée utilisée pour déchiffrer les

données. Pour plus d'informations sur les paires de clés, assurez-vous d'être connecté à la AWS console, puis consultez les paires de clés Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

Le AWS CloudFormation modèle de ce didacticiel inclut le `KeyName` paramètre suivant : `development-environment.template`

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

Les utilisateurs finaux doivent spécifier le nom d'une paire de clés lorsqu'ils l'utilisent AWS Service Catalog pour lancer le produit basé sur le modèle.

Si vous disposez déjà dans votre compte d'une paire de clés que vous préférez utiliser, vous pouvez passez directement à Étape 3 : Création d'un portefeuille. Sinon, effectuez les étapes suivantes.

Création d’une paire de clés

1. Ouvrez la console Amazon EC2 à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sous Network & Security, choisissez Key Pairs.
3. Sur la page Key Pairs, choisissez Create Key Pair.
4. Pour Key pair name, tapez un nom facile à mémoriser, puis choisissez Create.
5. Lorsque la console vous invite à enregistrer le fichier de clé privée, enregistrez-le dans un endroit sûr.

> **Important**
>
> C’est votre seule occasion d’enregistrer le fichier de clé privée.

Étape 3 : Création d'un portefeuille

Pour fournir des produits à des utilisateurs, commencez par créer un portefeuille pour ces produits.

Pour créer un portefeuille

1. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Dans le panneau de navigation de gauche, sélectionnez Portefeuilles, puis Créer un portefeuille.
3. Entrez les valeurs suivantes :
   - Nom du portefeuille — **`Engineering Tools`**
   - Description du portefeuille — **`Sample portfolio that contains a single product.`**
   - Propriétaire — **`IT (it@example.com)`**
4. Sélectionnez Create (Créer).

Étape 4 : Création d'un nouveau produit dans le portefeuille

Après avoir créé un portefeuille, vous êtes prêt à créer un produit dans le portefeuille. Dans le cadre de ce didacticiel, vous allez créer un produit appelé Linux Desktop, un environnement de développement cloud qui s'exécute sur Amazon Linux, dans le cadre du portefeuille d'outils d'ingénierie.

Pour créer un produit au sein d'un portefeuille

1. Si vous venez de terminer l'étape précédente, la page Portfolios sera déjà affichée. Sinon, ouvrez https://console.aws.amazon.com/servicecatalog/.
2. Choisissez et ouvrez le portefeuille d'outils d'ingénierie que vous avez créé à l'étape 2.
3. Choisissez Importer un nouveau produit.
4. Sur la page Créer un produit dans la section Détails du produit, entrez les informations suivantes :
   - Nom du produit — **`Linux Desktop`**
   - Description du produit — **`Cloud development environment configured for engineering staff. Runs AWS Linux.`**
   - Propriétaire — **`IT`**
   - Distributeur — (blanc)
5. Sur la page Détails de la version, choisissez Utiliser un CloudFormation modèle. Choisissez ensuite Spécifier une URL de modèle Amazon S3 et entrez ce qui suit :

- Sélectionnez un modèle — **`https://awsdocs.s3.amazonaws.com/servicecatalog/development-environment.template`**
- Titre de la version — **`v1.0`**
- Description – **`Base Version`**

6. Dans la section Support details, saisissez les informations suivantes :

   - Contact par e-mail — **`ITSupport@example.com`**
   - Lien de support — **`https://wiki.example.com/IT/support`**
   - Description du support — **`Contact the IT department for issues deploying or connecting to this product.`**

7. Choisissez Créer un produit.

Étape 5 : ajouter une contrainte de modèle pour limiter la taille de l'instance

Les contraintes ajoutent une autre couche de contrôle sur les produits au niveau du portefeuille. Les contraintes peuvent contrôler le contexte de lancement d'un produit (contraintes de lancement), ou ajouter des règles au modèle AWS CloudFormation (contraintes de modèle). Pour plus d'informations, consultez Utilisation de contraintes AWS Service Catalog.

Ajoutez une contrainte de modèle au produit Linux Desktop qui empêche les utilisateurs de sélectionner des types d'instances volumineux au moment du lancement. Le modèle development-environment permet à l'utilisateur de choisir parmi six types d'instance ; cette contrainte limite les types d'instance valides aux deux types les plus petits, `t2.micro` et `t2.small`. Pour plus d'informations, consultez la section Instances T2 dans le guide de l'utilisateur Amazon EC2.

Pour ajouter une contrainte de modèle au produit Linux Desktop

1. Sur la page des détails du portefeuille, choisissez Contraintes, puis Créer une contrainte.
2. Sur la page Créer une contrainte, pour Produit, sélectionnez Linux Desktop. Ensuite, pour Type de contrainte, choisissez Modèle.
3. Dans la section Contrainte du modèle T, choisissez Éditeur de texte.
4. Collez le texte suivant dans l'éditeur de texte :

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

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

5. Pour Description de la contrainte, entrez**`Small instance sizes`**.
6. Sélectionnez Create (Créer).

Étape 6 : ajouter une contrainte de lancement pour attribuer un rôle IAM

Une contrainte de lancement désigne un rôle IAM qui joue un rôle AWS Service Catalog lorsqu'un utilisateur final lance un produit.

Pour cette étape, vous ajoutez une contrainte de lancement au produit Linux Desktop afin de AWS Service Catalog pouvoir utiliser les ressources IAM qui constituent le AWS CloudFormation modèle du produit.

Le rôle IAM que vous attribuez à un produit en tant que contrainte de lancement doit disposer des autorisations suivantes :

1. AWS CloudFormation
2. Services dans le AWS CloudFormation modèle du produit
3. Accès en lecture au AWS CloudFormation modèle dans un compartiment Amazon S3 appartenant au service.

Cette contrainte de lancement permet à l'utilisateur final de lancer le produit et, après le lancement, de le gérer en tant que produit provisionné. Pour plus d'informations, veuillez consulter Contraintes de lancement AWS Service Catalog.

Sans contrainte de lancement, vous devez accorder des autorisations IAM supplémentaires à vos utilisateurs finaux avant qu'ils puissent utiliser le produit Linux Desktop. Par exemple, la `ServiceCatalogEndUserAccess` politique accorde les autorisations IAM minimales requises pour accéder à la vue de la console de l'utilisateur AWS Service Catalog final.

L'utilisation d'une contrainte de lancement vous permet de suivre les meilleures pratiques IAM qui consistent à réduire au minimum les autorisations IAM des utilisateurs finaux. Pour en savoir plus, consultez Accorder le moindre privilège dans le guide de l'utilisateur IAM.

Pour ajouter une contrainte de lancement

1. Suivez les instructions pour créer de nouvelles politiques dans l'onglet JSON du guide de l'utilisateur IAM.
2. Collez le document de politique JSON suivant :

   - `cloudformation`— Autorise AWS Service Catalog toutes les autorisations nécessaires pour créer, lire, mettre à jour, supprimer, répertorier et étiqueter des AWS CloudFormation piles.
   - `ec2`— Autorise AWS Service Catalog toutes les autorisations nécessaires pour répertorier, lire, écrire, approvisionner et étiqueter les ressources Amazon Elastic Compute Cloud (Amazon EC2) qui font partie du produit. AWS Service Catalog En fonction de la AWS ressource que vous souhaitez déployer, cette autorisation peut changer.
   - `ec2`— Crée une nouvelle politique gérée pour votre AWS compte et associe la politique gérée spécifiée au rôle IAM spécifié.
   - `s3`— Permet d'accéder aux compartiments Amazon S3 détenus parAWS Service Catalog. Pour déployer le produit, AWS Service Catalog il faut accéder aux artefacts de provisionnement.
   - `servicecatalog`— Permet de AWS Service Catalog répertorier, de lire, d'écrire, de baliser et de lancer des ressources au nom de l'utilisateur final.
   - `sns`— Autorise AWS Service Catalog les autorisations nécessaires pour répertorier, lire, écrire et baliser les rubriques Amazon SNS en fonction de la contrainte de lancement.

   > **Note**
   >
   > En fonction des ressources sous-jacentes que vous souhaitez déployer, vous devrez peut-être modifier l'exemple de politique 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. Choisissez Next, Tags.
4. Choisissez Suivant, Réviser.
5. Sur la page Politique de révision, saisissez le nom**`linuxDesktopPolicy`**.
6. Choisissez Créer une politique.
7. Dans le panneau de navigation, choisissez Roles (Rôles). Choisissez ensuite Créer un rôle et procédez comme suit :

   a. Pour Sélectionner une entité de confiance, choisissez AWSservice, puis sous Cas d'utilisation pour d'autres AWS services, choisissez Service Catalog. Sélectionnez le cas d'utilisation du Service Catalog, puis choisissez Next.

b. Recherchez la linuxDesktopPolicypolitique, puis cochez la case.

c. Choisissez Suivant.

d. Pour Role name (Nom du rôle), tapez **`linuxDesktopLaunchRole`**.

e. Sélectionnez Créer un rôle.

8. Ouvrez la AWS Service Catalog console à l'adresse https://console.aws.amazon.com/servicecatalog.
9. Choisissez le portefeuille Engineering Tools.
10. Sur la page des détails du portefeuille, choisissez l'onglet Contraintes, puis sélectionnez Créer une contrainte.
11. Pour Produit, choisissez Linux Desktop, et pour Type de contrainte, choisissez Launch.
12. Choisissez Sélectionner le rôle IAM. Choisissez ensuite linuxDesktopLaunchRole, puis Create.

Étape 7 : Accorder aux utilisateurs finaux l'accès au portefeuille

Maintenant que vous avez créé un portefeuille et ajouté un produit, vous êtes prêt à accorder un accès aux utilisateurs finaux.

Prérequis

Si vous n'avez pas créé de groupe IAM pour les utilisateurs finaux, consultez. Accorder des autorisations aux utilisateurs AWS Service Catalog finaux

Pour donner accès au portefeuille

1. Sur la page des détails du portefeuille, cliquez sur l'onglet Accès.
2. Choisissez Grant access (Accorder l'accès).
3. Dans l'onglet Groupes, cochez la case correspondant au groupe IAM pour les utilisateurs finaux.
4. Choisissez Ajouter un accès.

Étape 8 : Testez l'expérience de l'utilisateur final

Pour vérifier que l'utilisateur final peut accéder correctement à la vue de la console utilisateur final et lancer votre produit, connectez-vous en AWS tant qu'utilisateur final et effectuez ces tâches.

Pour vérifier que l'utilisateur final peut accéder à la console Utilisateur final

1. Suivez les instructions pour vous connecter en tant qu'utilisateur IAM dans le guide de l'utilisateur IAM.
2. Dans la barre de menu, choisissez la AWS région dans laquelle vous avez créé le `Engineering Tools` portefeuille. Pour ce didacticiel, choisissez la région us-east-1.
3. Ouvrez la AWS Service Catalog console à l'adresse https://console.aws.amazon.com/servicecatalog/ pour voir :
   - Produits — Les produits que l'utilisateur peut utiliser.
   - Produits approvisionnés : produits provisionnés que l'utilisateur a lancés.

Pour vérifier que l'utilisateur final peut lancer le produit Linux Desktop

Notez que pour ce didacticiel, choisissez la région us-east-1.

1. Dans la section Produits de la console, choisissez Linux Desktop.
2. Choisissez Launch product pour démarrer l'assistant qui configure votre produit.
3. Sur la page Launch : Linux Desktop, entrez **`Linux-Desktop`** le nom du produit provisionné.
4. Sur la page Paramètres, entrez ce qui suit, puis choisissez Next :
   - Taille du serveur — Choisissez**`t2.micro`**.
   - Paire de clés : sélectionnez la paire de clés que vous avez créée dansÉtape 2 : Création d'une paire de clés.
   - Plage d'adresses CIDR : entrez une plage d'adresses CIDR valide pour l'adresse IP à connecter à l'instance. Vous pouvez utiliser la valeur par défaut (0.0.0.0/0) pour autoriser l'accès depuis n'importe quelle adresse IP, puis votre adresse IP, puis **`/32`** pour restreindre l'accès à votre adresse IP uniquement, ou quelque chose entre les deux.
5. Choisissez Launch product pour lancer la pile. La console affiche la page des détails de pile pour la pile Linux-Desktop. L'état initial du produit est En cours de modification. Le lancement du produit par AWS Service Catalog prend plusieurs minutes. Pour afficher l'état en cours, actualisez votre navigateur. Après le lancement du produit, le statut est « Disponible ».

Commencer à utiliser un produit Terraform

AWS Service Catalogpermet un approvisionnement rapide en libre-service avec une gouvernance intégrée de vos configurations HashiCorp Terraform. AWS Vous pouvez l'utiliser AWS Service Catalog en tant qu'outil unique pour organiser, gérer et distribuer vos configurations Terraform à grande échelle. AWS AWS Service Catalogprend en charge Terraform sur plusieurs fonctionnalités clés, notamment le catalogage de modèles Terraform standardisés et préapprouvés, le contrôle d'accès, le versionnement, le balisage et le partage avec d'autres comptes. AWS Vos utilisateurs finaux y voient une simple liste de produits et de versions auxquels ils ont accès, et peuvent ensuite déployer ces produits en une seule action. AWS Service Catalog

> **Note**
>
> Pour continuer à prendre en charge HashiCorp les technologies, à la suite des récentes modifications de licence apportées à Terraform, toutes les références précédentes à Terraform Open Source AWS Service Catalog ont été remplacées par External. Le type de produit externe inclut le support de la Terraform Community Edition, anciennement connue sous le nom de Terraform Open Source. Pour plus d'informations et d'instructions sur la migration de vos produits Open Source Terraform existants et des produits fournis vers le type de produit externe, consultez. Mise à jour des produits Open Source Terraform existants et des produits fournis vers le type de produit externe

Les étapes du didacticiel suivant vous aideront à démarrer avec un produit Terraform dans. AWS Service Catalog

En tant qu'administrateur du catalogue, vous travaillez dans un compte d'administrateur central (compte hub). Les produits Terrafrm Community Edition et Terraform Cloud nécessitent tous deux un moteur de provisionnement Terraform, sur lequel vous pouvez en savoir plus dans et. Moteur de provisionnement pour Terraform Community Edition (type de produit externe) Moteur de provisionnement pour Terraform Cloud

Au cours du didacticiel, vous devez effectuer les tâches suivantes dans le compte administrateur :

- Créez un produit Terraform en utilisant le type de produit Terraform Cloud ou External. Service Catalog utilise le type de produit externe pour prendre en charge les produits Terraform Community Edition.
- Associer le produit à un portefeuille

- Créez une contrainte de lancement pour permettre à vos utilisateurs finaux de fournir le produit
- Marquer le produit
- Partagez le portefeuille et le produit Terraform avec le compte de l'utilisateur final (compte officiel)

Dans le didacticiel, vous partagez un portfolio à l'aide de l'option de partage de l'organisation depuis le compte du hub d'administration, qui est également le compte de gestion de l'organisation. Pour plus d'informations sur le partage d'organisations, consultezPartage d'un portefeuille.

La AWS ressource contenue dans le produit Terraform que vous créez dans le didacticiel est un simple bucket Amazon S3.

> **Note**
>
> Avant de commencer, assurez-vous d'avoir terminé les actions dansConfiguration AWS Service Catalog.

Rubriques

Mise à jour des produits Open Source Terraform existants et des produits fournis vers le type de produit externe

Pour continuer à prendre en charge HashiCorp les technologies, à la suite des récentes modifications de licence apportées à Terraform, toutes les références précédentes à Terraform Open Source AWS Service Catalog ont été remplacées par External. Le type de produit externe inclut le support de Terraform Community Edition, anciennement connue sous le nom de Terraform Open Source. AWS Service Catalogne prend plus en charge Terraform Open Source en tant que type de produit valide pour les nouveaux produits ou les produits approvisionnés. Vous ne pouvez mettre à jour ou résilier que les ressources Open Source existantes de Terraform, y compris les versions des produits et les produits provisionnés.

Si vous ne l'avez pas déjà fait, vous devez faire passer tous les produits Open Source Terraform existants et les produits fournis vers des produits externes, en suivant les instructions de cette section.

1. Mettez à jour votre moteur de référence Terraform existant AWS Service Catalog pour inclure la prise en charge des types de produits externes et Terraform Open Source. Pour obtenir des instructions sur la mise à jour de votre moteur de référence Terraform, consultez notre GitHub référentiel.
2. Recréez tous les produits Open Source Terraform existants en utilisant le nouveau type de produit externe.
3. Supprimez tous les produits existants qui utilisent le type de produit Open Source Terraform.
4. Réapprovisionnez les ressources restantes pour utiliser le nouveau type de produit externe.
5. Mettez fin à tous les produits provisionnés existants qui utilisent le type de produit Open Source Terraform.

Après la transition de vos produits existants, utilisez le type de produit externe pour tous les nouveaux produits utilisant un fichier de configuration tar.gz.

AWS Service Catalogaidera les clients à effectuer ce changement selon les besoins. Si ces modifications nécessitent des efforts importants pour votre compte ou ont un impact sur les charges de travail critiques des produits, contactez votre représentant commercial pour demander de l'aide.

Prérequis : configurez votre moteur de provisionnement Terraform

Comme condition préalable à la création de produits Terraform dansAWS Service Catalog, vous devez installer et configurer un moteur de provisionnement dans votre compte administrateur Service Catalog (compte hub). Le moteur de provisionnement est requis à la fois pour les produits Terraform Community Edition (utilisant le type de produit externe) et pour les produits Terraform Cloud (utilisant le type de produit Terraform Cloud).

> **Note**
>
> La configuration du moteur est une configuration unique qui prend environ 30 minutes.

Moteur de provisionnement pour Terraform Community Edition (type de produit externe)

AWS Service Catalogutilise le type de produit externe pour prendre en charge les produits Terraform Community Edition. Le type de produit externe prend également en charge d'autres outils de provisionnement, notamment Pulumi, Ansible, Chef, etc., en fonction de la configuration du moteur de provisionnement.

Pour les AWS Service Catalog produits qui utilisent le type HashiCorp de produit externe avec Terraform Community Edition, vous devez installer et configurer un moteur de provisionnement Terraform dans votre compte AWS Service Catalog administrateur (compte hub). AWSgère ce moteur et ses ressources.

AWS Service Catalogfournit un GitHub référentiel contenant des instructions sur l'installation et la configuration du moteur de AWS provisionnement Terraform fourni. Le dépôt inclut les informations suivantes :

- Outils d'installation requis
- Élaboration du code
- Déploiement sur un AWS compte
- Informations supplémentaires sur les flux de travail de provisionnement, l'assurance qualité et les limites

Moteur de provisionnement pour Terraform Cloud

Pour les AWS Service Catalog produits qui utilisent le type de produit Terraform Cloud avec HashiCorp Terraform Cloud, vous devez installer et configurer un moteur de provisionnement Terraform dans votre AWS Service Catalog compte administrateur (compte hub). HashiCorp gère ce moteur dans un environnement distant.

HashiCorp fournit un GitHub référentiel contenant des instructions sur la configuration du moteur Terraform Cloud pour. AWS Service Catalog Le dépôt inclut les informations suivantes :

- Outils d'installation requis
- Élaboration du code
- Déploiement sur un AWS compte
- Informations supplémentaires sur les flux de travail de provisionnement, l'assurance qualité et les limites

Étape 1 : téléchargement du fichier de configuration Terraform

Vous pouvez utiliser un fichier de configuration Terraform pour créer et approvisionner des produits HashiCorp Terraform. Ces configurations sont des fichiers texte brut qui décrivent les ressources que vous souhaitez mettre en service. Vous pouvez utiliser l'éditeur de texte de votre choix pour créer, mettre à jour et enregistrer des configurations. Pour créer un produit, vous devez télécharger les configurations Terraform sous forme de fichier tar.gz. Dans ce didacticiel, AWS Service Catalog fournit un fichier de configuration simple afin que vous puissiez commencer. La configuration crée un compartiment Amazon S3.

Téléchargement du fichier de configuration

AWS Service Catalogfournit un exemple `simple-s3-bucket.tar.gz`de fichier de configuration que vous pouvez utiliser dans ce didacticiel.

Vue d'ensemble du fichier de configuration

Le texte de l'exemple de fichier de configuration est le suivant :

```
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
}
```

Ressources de configuration

Le fichier de configuration déclare les ressources à créer lors du AWS Service Catalog provisionnement du produit. Il se compose des sections suivantes :

- Variable (facultatif) — Les définitions de valeurs qu'un utilisateur administrateur (administrateur du compte hub) peut attribuer pour personnaliser la configuration. Les variables fournissent une interface cohérente pour modifier le comportement d'une configuration donnée. L'étiquette après le mot-clé de variable est le nom de la variable, qui doit être unique parmi toutes les variables d'un même module. Ce nom est utilisé pour attribuer une valeur extérieure à la variable et pour référencer la valeur de la variable depuis le module.
- Fournisseur (facultatif) — Le fournisseur de services cloud pour le provisionnement des ressources, qui est`AWS`. AWS Service Catalogne prend en charge `AWS` qu'en tant que fournisseur. Par conséquent, le moteur de provisionnement Terraform remplace tout autre fournisseur répertorié. `AWS`
- Ressource (obligatoire) — La ressource AWS d'infrastructure pour le provisionnement. Pour ce didacticiel, le fichier de configuration Terraform spécifie Amazon S3.
- Sortie (facultatif) : information ou valeur renvoyée, similaire aux valeurs renvoyées dans un langage de programmation. Vous pouvez utiliser les données de sortie pour configurer le flux de travail de l'infrastructure à l'aide d'outils d'automatisation.

Étape 2 : créer un produit Terraform

Après avoir installé le moteur de provisionnement Terraform, vous êtes prêt à créer un produit HashiCorp Terraform dans. AWS Service Catalog Dans ce didacticiel, vous allez créer un produit Terraform contenant un simple bucket Amazon S3.

Pour créer un produit Terraform

1. Ouvrez la AWS Service Catalog console à l'adresse https://console.aws.amazon.com/servicecatalog/ et connectez-vous en tant qu'utilisateur administrateur.
2. Accédez à la section Administration, puis sélectionnez Liste des produits.
3. Choisissez Créer un produit.
4. Sur la page Créer un produit dans la section Détails du produit, choisissez le type de produit externe ou Terraform Cloud. Service Catalog utilise le type de produit externe pour prendre en charge les produits Terraform Community Edition.
5. Entrez les informations suivantes sur le produit :
   - Nom du produit — **`Simple S3 bucket`**
   - Description du produit — Produit Terraform contenant un compartiment Amazon S3.
   - Propriétaire — **`IT`**
   - Distributeur — (blanc)
6. Dans le volet Détails de la version, choisissez charger un fichier modèle, puis choisissez Choisir un fichier. Sélectionnez le fichier dans lequel vous avez téléchargéÉtape 1 : téléchargement du fichier de configuration Terraform.
7. Saisissez :
   - Nom de la version — **`v1.0`**
   - Description de la version — **`Base Version`**
8. Dans la section Support details, saisissez ce qui suit, puis choisissez Create product.
   - Contact par e-mail — **`ITSupport@example.com`**
   - Lien de support — **`https://wiki.example.com/IT/support`**
   - Description du support — **`Contact the IT department for issues deploying or connecting to this product.`**
9. Choisissez Créer un produit.

Après avoir créé le produit avec succès, AWS Service Catalog affiche une bannière de confirmation sur la page du produit.

Étape 3 : Création d'un AWS Service Catalog portefeuille

Vous pouvez créer un portefeuille dans votre compte AWS Service Catalog administrateur (compte hub) pour faciliter l'organisation des produits et leur distribution aux comptes des utilisateurs finaux (comptes satellites).

Pour créer un portefeuille

1. Ouvrez la AWS Service Catalog console à l'adresse https://console.aws.amazon.com/servicecatalog/ et connectez-vous en tant qu'administrateur.
2. Dans le panneau de navigation de gauche, sélectionnez Portefeuilles, puis Créer un portefeuille.
3. Entrez les valeurs suivantes :
   - Nom du portefeuille — **`S3 bucket`**
   - Description du portefeuille — **`Sample portfolio for Terraform configurations.`**
   - Propriétaire — **`IT (it@example.com)`**
4. Sélectionnez Create (Créer).

Étape 4 : Ajouter un produit au portefeuille

Après avoir créé un portfolio, vous pouvez ajouter le produit HashiCorp Terraform que vous avez créé à l'étape 2.

Pour ajouter un produit à un portefeuille

1. Accédez à la page de liste des produits.
2. Sélectionnez le produit Terraform Simple S3 bucket que vous avez créé à l'étape 2, puis choisissez Actions. Dans le menu déroulant, choisissez Ajouter un produit au portefeuille. AWS Service Catalogaffiche le volet Ajouter un compartiment S3 simple au portefeuille.
3. Sélectionnez le portefeuille de compartiments S3, puis désactivez l'option Créer une contrainte de lancement. Vous allez créer la contrainte de lancement ultérieurement dans le didacticiel.
4. Choisissez Ajouter un produit au portefeuille.

Après avoir ajouté le produit au portefeuille avec succès, AWS Service Catalog affiche une bannière de confirmation sur la page de liste des produits.

Étape 5 : créer des rôles de lancement

Au cours de cette étape, vous allez créer un rôle IAM (rôle de lancement) spécifiant les autorisations que le moteur de provisionnement Terraform AWS Service Catalog peut assumer lorsqu'un utilisateur final lance un produit Terraform. HashiCorp

Le rôle IAM (rôle de lancement) que vous attribuerez ultérieurement à votre produit Terraform de compartiment Amazon S3 simple en tant que contrainte de lancement doit disposer des autorisations suivantes :

- Accès aux AWS ressources sous-jacentes de votre produit Terraform. Dans ce didacticiel, cela inclut l'accès aux opérations `s3:CreateBucket*` `s3:DeleteBucket*`,`s3:Get*`,`s3:List*`,, et `s3:PutBucketTagging` Amazon S3.
- Accès en lecture au modèle Amazon S3 dans un compartiment Amazon S3 AWS Service Catalog appartenant à un propriétaire
- Accès aux opérations`CreateGroup`, `ListGroupResources`,`DeleteGroup`, et aux groupes de `Tag` ressources. Ces opérations permettent de AWS Service Catalog gérer les groupes de ressources et les balises

Pour créer un rôle de lancement dans le compte AWS Service Catalog administrateur

1. Lorsque vous êtes connecté au compte AWS Service Catalog administrateur, suivez les instructions pour créer de nouvelles politiques dans l'onglet JSON du guide de l'utilisateur IAM.
2. Créez une politique pour votre simple produit Terraform contenant un compartiment Amazon S3. Cette politique doit être créée avant de créer le rôle de lancement et comprend les autorisations suivantes :
   - `s3`— Autorise AWS Service Catalog toutes les autorisations nécessaires pour répertorier, lire, écrire, approvisionner et étiqueter le produit Amazon S3.
   - `s3`— Autorise l'accès aux compartiments Amazon S3 détenus parAWS Service Catalog. Pour déployer le produit, AWS Service Catalog il faut accéder aux artefacts de provisionnement.
   - `resourcegroups`— Permet AWS Service Catalog de créer, répertorier, supprimer et étiqueterAWS Resource Groups.
   - `tag`— Autorise les autorisations AWS Service Catalog de balisage.

> **Note**
>
> En fonction des ressources sous-jacentes que vous souhaitez déployer, vous devrez peut-être modifier l'exemple de politique JSON.

Collez le document de politique JSON suivant :

```
{
    "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. Choisissez Next, Tags.
   b. Choisissez Suivant, Réviser.
   c. Sur la page Politique de révision, saisissez le nom**`S3ResourceCreationAndArtifactAccessPolicy`**.
   d. Sélectionnez Créer une politique.
4. Dans le volet de navigation, sélectionnez Rôles, puis Créer un rôle.
5. Pour Sélectionner une entité de confiance, choisissez Politique de confiance personnalisée, puis entrez la politique JSON suivante :

```
{
    "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. Choisissez Suivant.
7. Dans la liste des politiques, sélectionnez celles que `S3ResourceCreationAndArtifactAccessPolicy` vous venez de créer.
8. Choisissez Suivant.
9. Pour le Nom du rôle, saisissez **`SCLaunch-S3product`**.

> **Important**
>
> Les noms des rôles de lancement doivent commencer par « SCLaunch » suivi du nom de rôle souhaité.

10. Sélectionnez Créer un rôle.

> **Important**
>
> Après avoir créé le rôle de lancement dans votre compte d'AWS Service Catalogadministrateur, vous devez également créer un rôle de lancement identique dans le compte d'utilisateur AWS Service Catalog final. Le rôle du compte utilisateur final doit porter le même nom et inclure la même politique que le rôle du compte administrateur.

Pour créer un rôle de lancement dans le compte de l'utilisateur AWS Service Catalog final

1. Connectez-vous en tant qu'administrateur au compte de l'utilisateur final, puis suivez les instructions pour créer de nouvelles politiques dans l'onglet JSON du guide de l'utilisateur IAM.
2. Répétez les étapes 2 à 10 de la section Pour créer un rôle de lancement dans le compte AWS Service Catalog administrateur ci-dessus.

> **Note**
>
> Lorsque vous créez un rôle de lancement dans le compte de l'utilisateur AWS Service Catalog final, assurez-vous d'utiliser le même administrateur **`AccountId`** dans la politique de confiance personnalisée.

Maintenant que vous avez créé un rôle de lancement dans les comptes administrateur et utilisateur final, vous pouvez ajouter une contrainte de lancement au produit.

Étape 6 : Ajouter une contrainte de lancement à votre produit Terraform

> **Important**
>
> Vous devez créer une contrainte de lancement pour les produits HashiCorp Terraform. Sans contrainte de lancement, les utilisateurs finaux ne peuvent pas fournir le produit.

Après avoir créé un rôle de lancement dans votre compte administrateur, vous êtes prêt à associer le rôle de lancement à une contrainte de lancement sur votre produit External ou Terraform Cloud.

Cette contrainte de lancement permet à l'utilisateur final de lancer le produit et, après le lancement, de le gérer en tant que produit provisionné. Pour plus d'informations, veuillez consulter Contraintes de lancement AWS Service Catalog.

L'utilisation d'une contrainte de lancement vous permet de suivre les meilleures pratiques IAM qui consistent à réduire au minimum les autorisations IAM des utilisateurs finaux. Pour en savoir plus, consultez Accorder le moindre privilège dans le guide de l'utilisateur IAM.

Pour attribuer une contrainte de lancement au produit

1. Ouvrez la AWS Service Catalog console à l'adresse https://console.aws.amazon.com/servicecatalog.
2. Dans la console de navigation de gauche, choisissez Portfolio.
3. Choisissez le portefeuille de compartiments S3.
4. Sur la page des détails du portefeuille, choisissez l'onglet Contraintes, puis sélectionnez Créer une contrainte.
5. Pour Product, choisissez Simple S3 bucket. AWS Service Catalogsélectionne automatiquement le type de contrainte de lancement.
6. Choisissez Enter role name, puis sLaunch-S3Product.
7. Choisissez Créer.

> **Note**
>
> Le nom de rôle indiqué doit exister dans le compte qui a créé la contrainte de lancement et dans le compte de l'utilisateur qui lance un produit avec cette contrainte de lancement.

Étape 7 : Accorder l'accès à l'utilisateur final

Après avoir appliqué la contrainte de lancement à votre produit HashiCorp Terraform, vous êtes prêt à accorder l'accès aux utilisateurs finaux dans le compte Spoke.

Dans ce didacticiel, vous accordez l'accès aux utilisateurs finaux à l'aide du partage de noms principaux. Les noms principaux sont des noms de groupes, de rôles et d'utilisateurs que les administrateurs peuvent spécifier dans un portefeuille, puis partager avec le portefeuille. Lorsque vous partagez le portefeuille, AWS Service Catalog vérifiez si ces noms principaux existent déjà. S'ils existent, associe AWS Service Catalog automatiquement les principaux IAM correspondants au portefeuille partagé pour accorder l'accès aux utilisateurs finaux. Consultez la section Partage d'un portfolio pour plus d'informations.

Prérequis

Si vous n'avez pas créé de groupe IAM pour les utilisateurs finaux, consultezAccorder des autorisations aux utilisateurs AWS Service Catalog finaux.

Pour donner accès au portefeuille

1. Accédez à la page Portfolio et choisissez le portefeuille de compartiments S3.
2. Choisissez l'onglet Accès, puis choisissez Accorder l'accès.
3. Dans le volet Type d'accès, sélectionnez Nom principal.
4. Dans le volet Nom principal, sélectionnez le type de nom principal, puis entrez le nom principal de l'utilisateur final souhaité dans le compte parlé.
5. Choisissez Grant access (Accorder l'accès).

Étape 8 : partager le portefeuille avec l'utilisateur final

L'AWS Service Catalogadministrateur peut distribuer des portefeuilles avec des comptes d'utilisateurs finaux en utilisant account-to-account le partage ou AWS Organizations le partage. Dans ce didacticiel, vous partagez votre portefeuille avec l'organisation à partir du compte administrateur (compte hub), qui est également le compte de gestion de l'organisation.

Pour partager le portfolio depuis le compte du hub d'administration

1. Ouvrez la AWS Service Catalog console à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Sur la page Portfolios, sélectionnez le portefeuille de compartiments S3. Dans le menu Actions, choisissez Partager.
3. Choisissez AWS Organizations, puis filtrez dans votre structure organisationnelle.
4. Dans le volet AWSOrganisation, choisissez le compte de l'utilisateur final (compte officiel).

   Vous pouvez également sélectionner un nœud racine pour partager le portefeuille avec l'ensemble de l'organisation, une unité organisationnelle (UO) parent ou une unité organisationnelle enfant au sein de votre organisation en fonction de la structure de votre organisation. Pour plus d'informations, consultezPartage d'un portefeuille.
5. Dans le volet des paramètres de partage, choisissez Partage principal.
6. Choisissez Partager.

Après avoir partagé avec succès le portefeuille avec les utilisateurs finaux, l'étape suivante consiste à vérifier l'expérience de l'utilisateur final et à fournir le produit Terraform.

Étape 9 : Testez l'expérience de l'utilisateur final

Pour vérifier que les utilisateurs finaux peuvent accéder correctement à la vue de la console utilisateur final et lancer votre **`Simple S3 bucket`** produit, connectez-vous en AWS tant qu'utilisateur final et effectuez les tâches ci-dessous.

Pour vérifier que l'utilisateur final peut accéder à la console Utilisateur final

- Ouvrez la AWS Service Catalog console à l'adresse https://console.aws.amazon.com/servicecatalog/ pour voir :
  - Produits — Les produits que l'utilisateur peut utiliser.
  - Produits approvisionnés : produits provisionnés que l'utilisateur a lancés.

Pour vérifier que l'utilisateur final peut lancer le produit Terraform

1. Dans la section Produits de la console, choisissez Simple S3 bucket.
2. Choisissez Launch product pour démarrer l'assistant qui configure votre produit.
3. Sur la page Launch Simple S3 bucket, entrez **`Amazon S3 product`** le nom du produit provisionné.
4. Sur la page Paramètres, entrez ce qui suit, puis choisissez Next :
   - bucket_name — Fournissez un nom unique pour le compartiment Amazon S3. Par exemple, **`terraform-s3-product`**.
5. Choisissez Launch product. La console affiche la page de détails de la pile pour le lancement du produit Amazon S3. L'état initial du produit est En cours de modification. Le lancement du produit par AWS Service Catalog prend plusieurs minutes. Pour afficher l'état en cours, actualisez votre navigateur. Après un lancement de produit réussi, le statut est Disponible.

   AWS Service Catalogcrée un nouveau compartiment Amazon S3 nommé**`terraform-s3-product`**.

Étape 10 : Surveillance des opérations de provisionnement de Terraform

Si vous souhaitez surveiller les opérations de provisionnement, vous pouvez consulter les CloudWatch journaux Amazon et consulter n'importe quel flux de AWS Step Functions travail de provisionnement.

Il existe deux machines d'état pour le flux de travail de provisionnement :

- `ManageProvisionedProductStateMachine`— AWS Service Catalog invoque cette machine d'état lors du provisionnement d'un nouveau produit Terraform et lors de la mise à jour d'un produit existant provisionné par Terraform.
- `TerminateProvisionedProductStateMachine`— AWS Service Catalog invoque cette machine à états lors de la mise hors service d'un produit existant approvisionné par Terraform.

Pour exécuter la machine d'état de surveillance

1. Ouvrez la console AWS de gestion et connectez-vous en tant qu'administrateur sur le compte du hub d'administration sur lequel le moteur de provisionnement Terraform est installé.
2. Ouvrir AWS Step Functions.
3. Dans le panneau de navigation de gauche, choisissez State machines.
4. Choisissez ManageProvisionedProductStateMachine.
5. Dans la liste des exécutions, entrez l'ID de produit fourni pour localiser votre exécution.

   > **Note**
   >
   > AWS Service Catalogcrée l'ID de produit fourni lorsque vous approvisionnez le produit. L'ID de produit fourni est formaté comme suit :. **`pp-1111pwtn[ID number]`**

6. Choisissez l'ID d'exécution.

Sur la page Détails de l'exécution qui en résulte, vous pouvez consulter toutes les étapes du flux de travail de provisionnement. Vous pouvez également passer en revue les étapes ayant échoué pour identifier la cause de l'échec.

Sécurité dans AWS Service Catalog

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformitéAWS.

  Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Service Catalog, voir AWS Services concernés par programme de conformité
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation AWS Service Catalog. Les rubriques suivantes expliquent comment procéder à la configuration AWS Service Catalog pour atteindre vos objectifs de sécurité et de conformité. Vous découvrirez également d'autres AWS services qui vous aident à surveiller et à sécuriser vos AWS Service Catalog ressources.

Rubriques

Protection des données dans AWS Service Catalog

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans AWS Service Catalog. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des AWS services que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent AWS services.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec AWS Service Catalog ou d'autres AWS services utilisateurs de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données

que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Protection des données à l'aide du chiffrement

Chiffrement au repos

AWS Service Catalog utilise des compartiments Amazon S3 et des bases de données Amazon DynamoDB qui sont chiffrées au repos à l'aide de clés gérées par Amazon. Pour en savoir plus, consultez les informations sur le chiffrement au repos fournies par Amazon S3 et Amazon DynamoDB.

Chiffrement en transit

AWS Service Catalog utilise le protocole TLS (Transport Layer Security) et le chiffrement côté client des informations en transit entre l'appelant et. AWS

Vous pouvez accéder en privé aux AWS Service Catalog API depuis votre Amazon Virtual Private Cloud (Amazon VPC) en créant des points de terminaison VPC. Avec les points de terminaison VPC, le routage entre le VPC et le VPC AWS Service Catalog est géré par le AWS réseau sans avoir besoin d'une passerelle Internet, d'une passerelle NAT ou d'une connexion VPN.

La dernière génération de points de terminaison VPC utilisés par AWS Service Catalog est alimentée par AWS PrivateLink une AWS technologie permettant la connectivité privée entre les AWS services à l'aide d'interfaces réseau élastiques avec des adresses IP privées dans vos VPC.

Identity and Access Management dans AWS Service Catalog

L'accès à AWS Service Catalog nécessite des informations d'identification. Ces informations d'identification doivent être autorisées à accéder à AWS des ressources, telles qu'un AWS Service Catalog portefeuille ou un produit. AWS Service Catalog s'intègre à AWS Identity and Access Management (IAM) pour vous permettre d'accorder aux AWS Service Catalog administrateurs les autorisations dont ils ont besoin pour créer et gérer des produits, et d'accorder aux utilisateurs AWS Service Catalog finaux les autorisations dont ils ont besoin pour lancer des produits et gérer les produits provisionnés. Ces politiques sont créées et gérées par AWS ou individuellement par les

administrateurs et les utilisateurs finaux. Pour contrôler l'accès, vous devez associer ces politiques aux utilisateurs, aux groupes et aux rôles que vous utilisez avec AWS Service Catalog.

Public ciblé

Les autorisations dont vous disposez avec AWS Identity and Access Management (IAM) peuvent dépendre du rôle que vous jouez. AWS Service Catalog

Les autorisations dont vous disposez via AWS Identity and Access Management (IAM) peuvent également dépendre du rôle que vous jouez. AWS Service Catalog

Administrateur : en tant qu' AWS Service Catalog administrateur, vous avez besoin d'un accès complet à la console d'administration et d'autorisations IAM qui vous permettent d'effectuer des tâches telles que la création et la gestion de portefeuilles et de produits, la gestion des contraintes et l'octroi d'accès aux utilisateurs finaux.

Utilisateur final : avant que vos utilisateurs finaux puissent utiliser vos produits, vous devez leur accorder des autorisations leur permettant d'accéder à la console utilisateur AWS Service Catalog final. Ils peuvent également disposer d'autorisations pour lancer des produits et gérer des produits provisionnés.

Administrateur IAM : si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à. AWS Service Catalog Pour consulter des exemples de politiques AWS Service Catalog basées sur l'identité que vous pouvez utiliser dans IAM, consultez. the section called “AWS politiques gérées”

Exemples de politiques basées sur l'identité pour AWS Service Catalog

Rubriques

Accès à la console pour les utilisateurs finaux

Les stratégies **`AWSServiceCatalogEndUserFullAccess`** et **`AWSServiceCatalogEndUserReadOnlyAccess`** accordent l'accès à la vue de la console

Utilisateur final d' AWS Service Catalog . Lorsqu'un utilisateur disposant de l'une de ces politiques choisit AWS Service Catalog l'une de ces politiques AWS Management Console, la vue de la console de l'utilisateur final affiche les produits qu'il est autorisé à lancer.

Avant que les utilisateurs finaux puissent lancer avec succès un produit AWS Service Catalog auquel vous donnez accès, vous devez leur fournir des autorisations IAM supplémentaires pour leur permettre d'utiliser chacune des AWS ressources sous-jacentes du AWS CloudFormation modèle d'un produit. Par exemple, si un modèle de produit inclut Amazon Relational Database Service (Amazon RDS), vous devez accorder aux utilisateurs les autorisations Amazon RDS pour lancer le produit.

Pour savoir comment permettre aux utilisateurs finaux de lancer des produits tout en appliquant les autorisations de moindre accès aux AWS ressources, voir. the section called “Utilisation de contraintes”

Si vous appliquez la stratégie **`AWSServiceCatalogEndUserReadOnlyAccess`**, vos utilisateurs ont accès à la console Utilisateur final, mais ils n'auront pas les autorisations dont ils ont besoin pour lancer des produits et gérer des produits provisionnés. Vous pouvez accorder ces autorisations directement à un utilisateur final à l'aide d'IAM, mais si vous souhaitez limiter l'accès des utilisateurs finaux aux AWS ressources, vous devez associer la politique à un rôle de lancement. Vous pouvez ensuite AWS Service Catalog appliquer le rôle de lancement à une contrainte de lancement pour le produit. Pour plus d'informations sur l'application d'un rôle de lancement et les limitations d'un rôle de lancement, et trouver un exemple de rôle de lancement, consultez Contraintes de lancement AWS Service Catalog.

> **Note**
>
> Si vous accordez aux utilisateurs des autorisations IAM pour les AWS Service Catalog administrateurs, la vue de la console de l'administrateur s'affiche à la place. N'accordez pas ces autorisations à des utilisateurs finaux, sauf si vous voulez qu'ils aient accès à la vue de la console Administrateur.

Accès aux produits pour les utilisateurs finaux

Avant que les utilisateurs finaux puissent utiliser un produit auquel vous donnez accès, vous devez leur fournir des autorisations IAM supplémentaires pour leur permettre d'utiliser chacune des AWS ressources sous-jacentes du AWS CloudFormation modèle d'un produit. Par exemple, si un modèle

de produit inclut Amazon Relational Database Service (Amazon RDS), vous devez accorder aux utilisateurs les autorisations Amazon RDS pour lancer le produit.

Si vous appliquez la stratégie **`AWSServiceCatalogEndUserReadOnlyAccess`**, vos utilisateurs ont accès à la vue de la console Utilisateur final, mais ils n'auront pas les autorisations dont ils ont besoin pour lancer des produits et gérer des produits provisionnés. Vous pouvez accorder ces autorisations directement à un utilisateur final dans IAM, mais si vous souhaitez limiter l'accès des utilisateurs finaux aux AWS ressources, vous devez associer la politique à un rôle de lancement. Vous pouvez ensuite AWS Service Catalog appliquer le rôle de lancement à une contrainte de lancement pour le produit. Pour plus d'informations sur l'application d'un rôle de lancement et les limitations d'un rôle de lancement, et trouver un exemple de rôle de lancement, consultez Contraintes de lancement AWS Service Catalog.

Exemples de politiques pour la gestion des produits approvisionnés

Vous pouvez créer des stratégies personnalisées pour mieux répondre aux exigences de sécurité de votre organisation. Les exemples suivants expliquent comment personnaliser le niveau d'accès pour chaque action avec la prise en charge des niveaux utilisateur, rôle et compte. Vous pouvez accorder aux utilisateurs l'accès pour afficher, mettre à jour, résilier et gérer des produits provisionnés créés uniquement par ces utilisateurs, ou créés par d'autres personnes également sous leur rôle ou le compte auquel ils sont connectés. Cet accès est hiérarchique : l'octroi d'un accès au niveau du compte accorde également un accès au niveau du rôle et un accès au niveau de l'utilisateur, tandis que l'ajout d'un accès au niveau du rôle accorde également un accès au niveau utilisateur mais pas au niveau du compte. Vous pouvez spécifier ces accès dans la stratégie JSON à l'aide d'un bloc `Condition` comme `accountLevel`, `roleLevel` ou `userLevel`.

Ces exemples s'appliquent également aux niveaux d'accès pour les opérations d'écriture d' AWS Service Catalog API : `UpdateProvisionedProduct` et`TerminateProvisionedProduct`, et pour les opérations de lecture : `DescribeRecord`, `ScanProvisionedProducts`, et`ListRecordHistory`. Les opérations d'API `ScanProvisionedProducts` et `ListRecordHistory` utilisent une entrée appelée `AccessLevelFilterKey`, et les valeurs de cette clé correspondent aux niveaux du bloc `Condition` présentés ici (`accountLevel` équivaut à la valeur « Account » pour `AccessLevelFilterKey`, `roleLevel` à « Role », et `userLevel` à « User »). Pour plus d'informations, consultez le Guide du développeur du Service Catalog.

Exemples

- Accès administrateur complet aux produits approvisionnés
- Accès de l'utilisateur final aux produits fournis

- Accès administrateur partiel aux produits approvisionnés

Accès administrateur complet aux produits approvisionnés

La stratégie suivante donne un accès complet en lecture et écriture aux produits provisionnés et enregistrements au sein du catalogue au niveau compte.

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

Cette stratégie est fonctionnellement équivalente à la stratégie suivante :

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

Le fait de ne pas spécifier de `Condition` bloc dans une politique pour AWS Service Catalog revient `"servicecatalog:accountLevel"` à spécifier un accès. Notez que l'accès `accountLevel` inclut les accès `roleLevel` et `userLevel`.

Accès de l'utilisateur final aux produits fournis

La stratégie suivante restreint l'accès aux opérations de lecture et d'écriture aux seuls produits provisionnés ou enregistrements associés, créés par l'utilisateur actuel.

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

Accès administrateur partiel aux produits approvisionnés

Les deux stratégies ci-dessous, si elles sont toutes deux appliquées au même utilisateur, autorisent un type d'accès que l'on pourrait qualifier d'« accès administrateur partiel » en fournissant un accès en lecture seule complet et un accès en écriture limité. Cela signifie que l'utilisateur peut afficher

n'importe quel produit provisionné ou enregistrement associé au sein du compte du catalogue, mais qu'il ne peut exécuter aucune action sur aucun produit provisionné ou enregistrement n'appartenant pas à cet utilisateur.

La première stratégie donne à l'utilisateur l'accès aux opérations d'écriture sur les produits provisionnés créés par l'utilisateur actuel, mais pas aux produits provisionnés créés par d'autres personnes. La deuxième stratégie ajoute un accès complet aux opérations de lecture sur les produits provisionnés créés par tous (utilisateur, rôle ou compte).

```
{
    "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 politiques gérées pour AWS Service Catalog AppRegistry

AWS politique gérée : **AWSServiceCatalogAdminFullAccess**

Vous pouvez les associer `AWSServiceCatalogAdminFullAccess` à vos entités IAM. AppRegistry associe également cette politique à un rôle de service qui permet AppRegistry d'effectuer des actions en votre nom.

Cette politique accorde des autorisations *`administratives`* qui permettent un accès complet à la vue de la console de l'administrateur et accorde l'autorisation de créer et de gérer des produits et des portefeuilles.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes.

- `servicecatalog`— Permet aux principaux d'accéder à la vue de la console de l'administrateur et de créer et de gérer des portefeuilles et des produits, de gérer les contraintes, d'accorder l'accès aux utilisateurs finaux et d'effectuer d'autres tâches administratives au sein AWS Service Catalog de cette console.
- `cloudformation`— Autorise AWS Service Catalog toutes les autorisations pour répertorier, lire, écrire et étiqueter des AWS CloudFormation piles.
- `config`— Autorise des autorisations AWS Service Catalog limitées sur les portefeuilles, les produits et les produits approvisionnés via AWS Config.
- `iam`— Permet aux principaux d'accéder à toutes les autorisations nécessaires pour consulter et créer des utilisateurs de services, des groupes ou des rôles nécessaires à la création et à la gestion de produits et de portefeuilles.

- `ssm`— Permet AWS Service Catalog de AWS Systems Manager répertorier et de lire les documents de Systems Manager dans le AWS compte courant et dans AWS la région.

Consultez la politique : AWSServiceCatalogAdminFullAccess.

AWS politique gérée : **`AWSServiceCatalogAdminReadOnlyAccess`**

Vous pouvez les associer `AWSServiceCatalogAdminReadOnlyAccess` à vos entités IAM. AppRegistry associe également cette politique à un rôle de service qui permet AppRegistry d'effectuer des actions en votre nom.

Cette politique accorde des autorisations *`en lecture seule`* qui permettent un accès complet à la vue de la console de l'administrateur. Cette politique n'accorde pas l'accès pour créer ou gérer des produits et des portefeuilles.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes.

- `servicecatalog`— Permet aux principaux d'accéder en lecture seule à la vue de la console de l'administrateur.
- `cloudformation`— Autorise des autorisations AWS Service Catalog limitées pour répertorier et lire les AWS CloudFormation piles.
- `config`— Autorise des autorisations AWS Service Catalog limitées sur les portefeuilles, les produits et les produits approvisionnés via AWS Config.
- `iam`— Accorde aux principaux des autorisations limitées leur permettant de consulter les utilisateurs du service, les groupes ou les rôles nécessaires à la création et à la gestion de produits et de portefeuilles.
- `ssm`— Permet AWS Service Catalog de AWS Systems Manager répertorier et de lire les documents de Systems Manager dans le AWS compte courant et dans AWS la région.

Consultez la politique : AWSServiceCatalogAdminReadOnlyAccess.

AWS politique gérée : **`AWSServiceCatalogEndUserFullAccess`**

Vous pouvez les associer `AWSServiceCatalogEndUserFullAccess` à vos entités IAM. AppRegistry associe également cette politique à un rôle de service qui permet AppRegistry d'effectuer des actions en votre nom.

Cette politique accorde aux *contributeurs* des autorisations qui permettent un accès complet à la vue de la console de l'utilisateur final, ainsi que l'autorisation de lancer des produits et de gérer les produits provisionnés.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes.

- `servicecatalog`— Accorde aux principaux des autorisations complètes sur la vue de la console de l'utilisateur final et la possibilité de lancer des produits et de gérer les produits approvisionnés.
- `cloudformation`— Autorise AWS Service Catalog toutes les autorisations pour répertorier, lire, écrire et étiqueter des AWS CloudFormation piles.
- `config`— Autorise des autorisations AWS Service Catalog limitées pour répertorier et lire les détails des portefeuilles, des produits et des produits approvisionnés via AWS Config.
- `ssm`— Permet AWS Service Catalog de lire AWS Systems Manager les documents de Systems Manager dans le AWS compte courant et dans AWS la région.

Consultez la politique : AWSServiceCatalogEndUserFullAccess.

AWS politique gérée : **`AWSServiceCatalogEndUserReadOnlyAccess`**

Vous pouvez les associer `AWSServiceCatalogEndUserReadOnlyAccess` à vos entités IAM. AppRegistry associe également cette politique à un rôle de service qui permet AppRegistry d'effectuer des actions en votre nom.

Cette politique accorde des autorisations *en lecture seule* qui permettent un accès en lecture seule à la vue de la console de l'utilisateur final. Cette politique n'autorise pas le lancement de produits ou la gestion de produits approvisionnés.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes.

- `servicecatalog`— Autorise les principaux à accéder en lecture seule à la vue de la console de l'utilisateur final.
- `cloudformation`— Autorise des autorisations AWS Service Catalog limitées pour répertorier et lire les AWS CloudFormation piles.
- `config`— Autorise des autorisations AWS Service Catalog limitées pour répertorier et lire les détails des portefeuilles, des produits et des produits approvisionnés via AWS Config.

- `ssm`— Permet AWS Service Catalog de lire AWS Systems Manager les documents de Systems Manager dans le AWS compte courant et dans AWS la région.

Consultez la politique : AWSServiceCatalogEndUserReadOnlyAccess.

AWS politique gérée : **`AWSServiceCatalogSyncServiceRolePolicy`**

AWS Service Catalog associe cette politique au rôle `AWSServiceRoleForServiceCatalogSync` lié au service (SLR), ce qui permet de synchroniser les modèles AWS Service Catalog d'un référentiel externe avec les produits. AWS Service Catalog

Cette politique accorde des autorisations qui permettent un accès limité aux AWS Service Catalog actions (par exemple, les appels d'API) et aux autres actions de AWS service qui en AWS Service Catalog dépendent.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes.

- `servicecatalog`— Permet au rôle de synchronisation des AWS Service Catalog artefacts de limiter l'accès aux API AWS Service Catalog publiques.
- `codeconnections`— Permet au rôle de synchronisation des AWS Service Catalog artefacts de limiter l'accès aux API CodeConnections publiques.
- `cloudformation`— Permet au rôle de synchronisation des AWS Service Catalog artefacts de limiter l'accès aux API AWS CloudFormation publiques.

Consultez la politique : AWSServiceCatalogSyncServiceRolePolicy.

Détails des rôles liés au service

AWS Service Catalog utilise les informations d'autorisation ci-dessus pour le rôle `AWSServiceRoleForServiceCatalogSync` lié au service créé lorsqu'un utilisateur crée ou met à jour un AWS Service Catalog produit qui utilise. CodeConnections Vous pouvez modifier cette politique à l'aide de la AWS CLI, de l' AWS API ou de la AWS Service Catalog console. Pour plus d'informations sur la création, la modification et la suppression de rôles liés à un service, reportez-vous à la section Utilisation de rôles liés à un service (SLR) pour. AWS Service Catalog

Les autorisations incluses dans le rôle `AWSServiceRoleForServiceCatalogSync` lié au service permettent d' AWS Service Catalog effectuer les actions suivantes pour le compte du client.

- `servicecatalog:ListProvisioningArtifacts`— Permet au rôle de synchronisation des AWS Service Catalog artefacts de répertorier les artefacts d'approvisionnement pour un AWS Service Catalog produit donné qui sont synchronisés avec un fichier modèle dans un référentiel.
- `servicecatalog:DescribeProductAsAdmin`— Permet au rôle de synchronisation des AWS Service Catalog artefacts d'utiliser l'`DescribeProductAsAdmin`API pour obtenir des informations sur un AWS Service Catalog produit et ses artefacts provisionnés associés, qui sont synchronisés avec un fichier modèle dans un référentiel. Le rôle de synchronisation des artefacts utilise le résultat de cet appel pour vérifier la limite de quota de service du produit pour le provisionnement des artefacts.
- `servicecatalog:DeleteProvisioningArtifact`— Permet au rôle de synchronisation des AWS Service Catalog artefacts de supprimer un artefact provisionné.
- `servicecatalog:ListServiceActionsForProvisioningArtifact`— Permet au rôle de synchronisation des AWS Service Catalog artefacts de déterminer si des actions de service sont associées à un artefact de provisionnement et de garantir que l'artefact de provisionnement n'est pas supprimé si une action de service est associée.
- `servicecatalog:DescribeProvisioningArtifact`— Permet au rôle de synchronisation des AWS Service Catalog artefacts de récupérer les détails de l'`DescribeProvisioningArtifact`API, y compris l'ID de validation, qui est fourni dans la `SourceRevisionInfo` sortie.
- `servicecatalog:CreateProvisioningArtifact`— Permet au rôle de synchronisation des AWS Service Catalog artefacts de créer un nouvel artefact provisionné si une modification est détectée (par exemple, un git-push est validé) dans le fichier modèle source dans le référentiel externe.
- `servicecatalog:UpdateProvisioningArtifact`— Permet au rôle de synchronisation des AWS Service Catalog artefacts de mettre à jour l'artefact provisionné pour un produit connecté ou synchronisé.
- `codeconnections:UseConnection`— Permet au rôle de synchronisation des AWS Service Catalog artefacts d'utiliser la connexion existante pour mettre à jour et synchroniser un produit.
- `cloudformation:ValidateTemplate`— Autorise un accès limité au rôle de synchronisation des AWS Service Catalog artefacts AWS CloudFormation pour valider le format du modèle utilisé dans un référentiel externe et vérifier s'il AWS CloudFormation est compatible avec le modèle.

AWS politique gérée : **AWSServiceCatalogOrgsDataSyncServiceRolePolicy**

AWS Service Catalog attache cette politique au rôle `AWSServiceRoleForServiceCatalogOrgsDataSync` lié au service (SLR), permettant AWS Service Catalog la synchronisation avec. AWS Organizations

Cette politique accorde des autorisations qui permettent un accès limité aux AWS Service Catalog actions (par exemple, les appels d'API) et aux autres actions de AWS service qui en AWS Service Catalog dépendent.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes.

- `organizations`— Permet au rôle de synchronisation AWS Service Catalog des données de limiter l'accès aux API AWS Organizations publiques.

Consultez la politique : AWSServiceCatalogOrgsDataSyncServiceRolePolicy.

Détails des rôles liés au service

AWS Service Catalog utilise les informations d'autorisation ci-dessus pour le rôle `AWSServiceRoleForServiceCatalogOrgsDataSync` lié au service créé lorsqu'un utilisateur active l'accès au portefeuille AWS Organizations partagé ou crée un partage de portefeuille. Vous pouvez modifier cette politique à l'aide de la AWS CLI, de l' AWS API ou de la AWS Service Catalog console. Pour plus d'informations sur la création, la modification et la suppression de rôles liés à un service, reportez-vous à la section Utilisation de rôles liés à un service (SLR) pour. AWS Service Catalog

Les autorisations incluses dans le rôle `AWSServiceRoleForServiceCatalogOrgsDataSync` lié au service permettent d' AWS Service Catalog effectuer les actions suivantes pour le compte du client.

- `organizations:DescribeAccount`— Permet au rôle AWS Service Catalog Organizations Data Sync de AWS Organizations récupérer les informations associées au compte spécifié.
- `organizations:DescribeOrganization`— Permet au rôle AWS Service Catalog Organizations Data Sync de récupérer des informations sur l'organisation à laquelle appartient le compte de l'utilisateur.

- `organizations:ListAccounts`— Permet au rôle AWS Service Catalog Organizations Data Sync de répertorier les comptes de l'organisation de l'utilisateur.
- `organizations:ListChildren`— Permet au rôle AWS Service Catalog Organizations Data Sync de répertorier toutes les unités organisationnelles (UO) ou tous les comptes contenus dans l'unité d'organisation parent ou racine spécifiée.
- `organizations:ListParents`— Permet au rôle AWS Service Catalog Organizations Data Sync de répertorier la racine ou les unités d'organisation qui servent de parent immédiat à l'unité d'organisation ou au compte enfant spécifié.
- `organizations:ListAWSServiceAccessForOrganization`— Permet au rôle AWS Service Catalog Organizations Data Sync de récupérer la liste des AWS services que l'utilisateur a autorisés à intégrer à son organisation.

Politiques déconseillées

Les stratégies gérées obsolètes sont les suivantes :

- ServiceCatalogAdminFullAccess— Utilisez AWSServiceCatalogAdminFullAccessplutôt.
- ServiceCatalogAdminReadOnlyAccess— Utilisez AWSServiceCatalogAdminReadOnlyAccessplutôt.
- ServiceCatalogEndUserFullAccess— Utilisez AWSServiceCatalogEndUserFullAccessplutôt.
- ServiceCatalogEndUserAccess— Utilisez AWSServiceCatalogEndUserReadOnlyAccessplutôt.

Utilisez la procédure suivante pour vous assurer que les autorisations sont accordées à vos administrateurs et à vos utilisateurs finaux à l'aide des stratégies actuelles.

Pour migrer des politiques obsolètes vers les politiques actuelles, consultez la section Ajouter et supprimer des autorisations d'identité IAM dans AWS Identity and Access Management le Guide de l'utilisateur.

AppRegistry mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées AppRegistry depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page Historique du AppRegistry document.

Modification	Description	Date
AWSServiceCatalogSyncServiceRolePolicy— Mettre à jour la politique gérée	AWS Service Catalog a mis à jour la `AWSServiceCatalogSyncServiceRolePolicy` politique pour `codestar-connections` la remplacer par`codeconnections` .	7 mai 2024
AWSServiceCatalogAdminFullAccess— Mettre à jour la politique gérée	AWS Service Catalog a mis à jour la `AWSServiceCatalogAdminFullAccess` politique afin d'inclure les autorisations requises pour que l' AWS Service Catalog administrateur puisse créer le rôle `AWSServiceRoleForServiceCatalogOrgsDataSync` lié au service (SLR) dans son compte.	14 avril 2023
AWSServiceCatalogOrgsDataSyncServiceRolePolicy— Nouvelle politique gérée	AWS Service Catalog a ajouté le`AWSServiceCatalogOrgsDataSyncServiceRolePolicy` , qui est attaché au rôle `AWSServiceRoleForServiceCatalogOrgsDataSync` lié au service (SLR), AWS Service Catalog permettant la synchronisation avec. AWS Organizations Cette politique permet un accès limité aux AWS Service Catalog actions (par exemple, les appels d'API) et aux autres actions	14 avril 2023

Modification	Description	Date
	de AWS service qui en AWS Service Catalog dépendent.	
AWSServiceCatalogAdminFullAccess— Mettre à jour la politique gérée	AWS Service Catalog a mis à jour la `AWSServiceCatalogAdminFullAccess` politique afin d'inclure toutes les autorisations pour l' AWS Service Catalog administrateur et de créer une compatibilité avec AppRegistry.	12 janvier 2023
AWSServiceCatalogSyncServiceRolePolicy— Nouvelle politique gérée	AWS Service Catalog a ajouté la `AWSServiceCatalogSyncServiceRolePolicy` politique, qui est attachée au rôle `AWSServiceRoleForServiceCatalogSync` lié au service (SLR). Cette politique permet AWS Service Catalog de synchroniser les modèles d'un référentiel externe avec les AWS Service Catalog produits.	18 novembre 2022

Modification	Description	Date
AWSServiceRoleForServiceCatalogSync— Nouveau rôle lié au service	AWS Service Catalog a ajouté le rôle `AWSServiceRoleForServiceCatalogSync` lié au service (SLR). Ce rôle est requis AWS Service Catalog pour utiliser CodeConnections et créer, mettre à jour et décrire les artefacts de AWS Service Catalog provisionnement pour un produit.	18 novembre 2022

Modification	Description	Date
AWSServiceCatalogAdminFullAccess— Politique gérée mise à jour	AWS Service Catalog a mis à jour la `AWSServiceCatalogAdminFullAccess` politique afin d'inclure toutes les autorisations requises pour un AWS Service Catalog administrateur. La politique identifie les actions spécifiques que l'administrateur peut effectuer sur toutes les AWS Service Catalog ressources, telles que créer, décrire, supprimer, etc. En outre, la politique a été modifiée pour prendre en charge une fonctionnalité récemment lancée, le contrôle d'accès basé sur les attributs (ABAC) pour AWS Service Catalog. ABAC vous permet d'utiliser la `AWSServiceCatalogAdminFullAccess` politique comme modèle pour autoriser ou refuser des actions sur les AWS Service Catalog ressources en fonction de balises. Pour plus d'informations sur l'ABAC, voir À quoi sert l'ABAC dans. AWSAWS Identity and Access Management	30 septembre 2022

Modification	Description	Date
AppRegistry a commencé à suivre les modifications	AppRegistry a commencé à suivre les modifications apportées AWS à ses politiques gérées.	15 septembre 2022

Utilisation des rôles liés aux services pour AWS Service Catalog

AWS Service Catalog utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. AWS Service Catalog Les rôles liés au service sont prédéfinis par AWS Service Catalog et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration AWS Service Catalog car vous n'avez pas à ajouter manuellement les autorisations nécessaires. AWS Service Catalog définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul AWS Service Catalog peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos AWS Service Catalog ressources car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services prenant en charge les rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM et recherchez les services présentant la mention Yes (Oui) dans la colonne Service-linked roles (Rôles liés à un service). Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations des rôles liés à un service pour **`AWSServiceRoleForServiceCatalogSync`**

AWS Service Catalog peut utiliser le rôle lié au service nommé **`AWSServiceRoleForServiceCatalogSync`**— Ce rôle lié au service est requis pour utiliser CodeConnections et créer, mettre AWS Service Catalog à jour et décrire les artefacts de AWS Service Catalog provisionnement pour un produit.

Le rôle lié à un service `AWSServiceRoleForServiceCatalogSync` approuve les services suivants pour endosser le rôle :

- `sync.servicecatalog.amazonaws.com`

La politique d'autorisations de rôle nommée AWSServiceCatalogSyncServiceRolePolicy AWS Service Catalog permet d'effectuer les actions suivantes sur les ressources spécifiées :

- Action : `Connection` sur `CodeConnections`
- Action : `Create, Update, and Describe` activée `ProvisioningArtifact` pour un AWS Service Catalog produit

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création du rôle lié à un service **`AWSServiceRoleForServiceCatalogSync`**

Il n'est pas nécessaire de créer manuellement le rôle `AWSServiceRoleForServiceCatalogSync` lié à un service. AWS Service Catalog crée automatiquement le rôle lié au service pour vous lorsque vous l'établissez CodeConnections dans AWS Management Console, dans ou dans l' AWS CLI API. AWS

> **Important**
>
> Ce rôle lié à un service peut apparaître dans votre compte si vous avez effectué une action dans un autre service qui utilise les fonctions prises en charge par ce rôle. De plus, si vous utilisiez le AWS Service Catalog service avant le 18 novembre 2022, date à laquelle il a commencé à prendre en charge les rôles liés au service, vous avez AWS Service Catalog créé le `AWSServiceRoleForServiceCatalogSync` rôle dans votre compte. Pour en savoir plus, consultez Un nouveau rôle est apparu dans mon compte IAM.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez CodeConnections, AWS Service Catalog crée à nouveau le rôle lié au service pour vous.

Vous pouvez également utiliser la console IAM pour créer un rôle lié à un service avec le cas d'utilisation des produits synchronisés AWS Service Catalog . Dans l'API AWS CLI ou dans l' AWS API, créez un rôle lié à un service avec le nom du `sync.servicecatalog.amazonaws.com` service. Pour plus d'informations, consultez Création d'un rôle lié à un service dans le Guide de l'utilisateur IAM. Si vous supprimez ce rôle lié à un service, vous pouvez utiliser ce même processus pour créer le rôle à nouveau.

Autorisations des rôles liés à un service pour **`AWSServiceRoleForServiceCatalogOrgsDataSync`**

AWS Service Catalog peut utiliser le rôle lié au service nommé **`AWSServiceRoleForServiceCatalogOrgsDataSync`**— Ce rôle lié au service est obligatoire pour que les AWS Service Catalog organisations puissent rester synchronisées avec. AWS Organizations

Le rôle lié à un service `AWSServiceRoleForServiceCatalogOrgsDataSync` approuve les services suivants pour endosser le rôle :

- `orgsdatasync.servicecatalog.amazonaws.com`

Le rôle `AWSServiceRoleForServiceCatalogOrgsDataSync` lié à un service nécessite que vous utilisiez la politique de confiance suivante en plus de la politique `AWSServiceCatalogOrgsDataSyncServiceRolePolicy` gérée :

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

La politique d'autorisations de rôle nommée AWSServiceCatalogOrgsDataSyncServiceRolePolicy AWS Service Catalog permet d'effectuer les actions suivantes sur les ressources spécifiées :

- Action : `DescribeAccountDescribeOrganization`, et ainsi de `ListAWSServiceAccessForOrganization` suite `Organizations accounts`
- Action : `ListAccountsListChildren`, et ainsi de `ListParent` suite `Organizations accounts`

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création du rôle lié à un service **`AWSServiceRoleForServiceCatalogOrgsDataSync`**

Il n'est pas nécessaire de créer manuellement le rôle `AWSServiceRoleForServiceCatalogOrgsDataSync` lié à un service. AWS Service Catalog considère que votre action consiste à activer Partage avec AWS Organizations ou Partage d'un portefeuille AWS Service Catalog à autoriser la création d'un reflex en arrière-plan en votre nom.

AWS Service Catalog crée automatiquement le rôle lié au service pour vous lorsque vous le AWS Management Console demandez `EnableAWSOrganizationsAccess` ou `CreatePortfolioShare` dans AWS CLI l' AWS API.

> **Important**
>
> Ce rôle lié à un service peut apparaître dans votre compte si vous avez effectué une action dans un autre service qui utilise les fonctions prises en charge par ce rôle. Pour en savoir plus, consultez Un nouveau rôle est apparu dans mon compte IAM.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous demandez `EnableAWSOrganizationsAccess` ou créez `CreatePortfolioShare` à AWS Service Catalog nouveau le rôle lié au service pour vous.

Modification d'un rôle lié à un service pour AWS Service Catalog

AWS Service Catalog ne vous permet pas de modifier les rôles `AWSServiceRoleForServiceCatalogSync` ou les rôles

`AWSServiceRoleForServiceCatalogOrgsDataSync` liés à un service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS Service Catalog

Vous pouvez utiliser la console IAM, la AWS CLI ou l' AWS API pour supprimer manuellement le `AWSServiceRoleForServiceCatalogSync` ou le `AWSServiceRoleForServiceCatalogOrgsDataSync` SLR. Pour ce faire, vous devez d'abord supprimer manuellement toutes les ressources qui utilisent le rôle lié au service (par exemple, tout AWS Service Catalog produit synchronisé avec un référentiel externe), puis le rôle lié au service peut être supprimé manuellement.

Régions prises en charge pour les rôles liés à un service AWS Service Catalog

AWS Service Catalog prend en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez Régions et points de terminaison AWS.

Nom de la région	Identité de la région	Support dans AWS Service Catalog
US East (Virginie du Nord)	us-east-1	Oui
USA Est (Ohio)	us-east-2	Oui
USA Ouest (Californie du Nord)	us-west-1	Oui
USA Ouest (Oregon)	us-west-2	Oui
Afrique (Le Cap)	af-south-1	Oui
Asie-Pacifique (Hong Kong)	ap-east-1	Oui
Asie-Pacifique (Jakarta)	ap-southeast-3	Oui
Asie-Pacifique (Mumbai)	ap-south-1	Oui
Asie-Pacifique (Osaka)	ap-northeast-3	Oui

Nom de la région	Identité de la région	Support dans AWS Service Catalog
Asie-Pacifique (Séoul)	ap-northeast-2	Oui
Asie-Pacifique (Singapour)	ap-southeast-1	Oui
Asie-Pacifique (Sydney)	ap-southeast-2	Oui
Asie-Pacifique (Tokyo)	ap-northeast-1	Oui
Canada (Centre)	ca-central-1	Oui
Europe (Francfort)	eu-central-1	Oui
Europe (Irlande)	eu-west-1	Oui
Europe (Londres)	eu-west-2	Oui
Europe (Milan)	eu-south-1	Oui
Europe (Paris)	eu-west-3	Oui
Europe (Stockholm)	eu-north-1	Oui
Moyen-Orient (Bahreïn)	me-south-1	Oui
Amérique du Sud (São Paulo)	sa-east-1	Oui
AWS GovCloud (USA Est)	us-gov-east-1	Non
AWS GovCloud (US-Ouest)	us-gov-west-1	Non

Résolution des problèmes AWS Service Catalog d'identité et d'accès

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec AWS Service Catalog IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans AWS Service Catalog

- Je ne suis pas autorisé à effectuer iam:PassRole
- Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes AWS Service Catalog ressources

Je ne suis pas autorisé à effectuer une action dans AWS Service Catalog

S'il vous AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni vos informations de connexion. L'exemple d'erreur suivant se produit lorsque l'utilisateur de mateojackson essaie d'utiliser la console pour afficher les détails d'une my-example-widget ressource fictive mais ne dispose pas des autorisations fictives`aws:GetWidget`.

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

Dans ce cas, Mateo demande à son administrateur de mettre à jour ses politiques pour lui permettre d'accéder à la ressource `my-example-widget` à l'aide de l'action `aws:GetWidget`.

Je ne suis pas autorisé à effectuer **`iam:PassRole`**

Si vous recevez un message d'erreur selon lequel vous n'êtes pas autorisé à exécuter l'action `iam:PassRole`, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni votre nom d'utilisateur et votre mot de passe. Demandez à cette personne de mettre à jour vos politiques pour vous permettre de transmettre un rôle à AWS Service Catalog.

Certains AWS services vous permettent de transmettre un rôle existant à ce service, au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur nommé marymajor essaie d'utiliser la console pour effectuer une action dans AWS Service Catalog. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction du service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

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

Dans ce cas, Mary demande à son administrateur de mettre à jour ses politiques pour lui permettre d'exécuter l'PassRole action iam :.

Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes AWS Service Catalog ressources

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si ces fonctionnalités sont prises AWS Identity and Access ManagementAWS Service Catalog en AWS Service Catalog charge, consultez le Guide de AWS Service Catalog l'administrateur.
- Pour savoir comment fournir un accès à vos ressources sur les AWS comptes que vous possédez, consultez la section Fournir un accès à un utilisateur IAM sur un autre AWS compte que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des AWS comptes tiers, consultez la section Fournir un accès aux AWS comptes détenus par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès entre comptes, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Contrôle de l'accès

un AWS Service Catalog portefeuille donne à vos administrateurs un certain niveau de contrôle d'accès pour vos groupes d'utilisateurs finaux. Lorsque vous ajoutez des utilisateurs à un portefeuille, ceux-ci peuvent parcourir et lancer n'importe lequel des produits du portefeuille. Pour plus d'informations, consultez the section called "Gestion des portefeuilles".

Constraints

Les contraintes déterminent les règles qui sont appliquées à vos utilisateurs finaux lors du lancement d'un produit à partir d'un portefeuille spécifique. Vous les utilisez pour appliquer des limites aux produits à des fins de contrôle de la gouvernance ou des coûts. Pour plus d'informations sur les contraintes, consultez the section called “Utilisation de contraintes”.

AWS Service Catalog les contraintes de lancement vous permettent de mieux contrôler les autorisations requises par un utilisateur final. Lorsque votre administrateur crée une contrainte de lancement pour un produit d'un portefeuille, cette dernière associe un ARN de rôle qui est utilisé lorsque vos utilisateurs finaux lancent le produit à partir de ce portefeuille. À l'aide de ce modèle, vous pouvez contrôler l'accès à la création de AWS ressources. Pour plus d’informations, consultez the section called “Contraintes de lancement”.

Connexion et surveillance AWS Service Catalog

AWS Service Catalog s'intègre AWS CloudTrailà un service qui capture tous les appels d' AWS Service Catalog API et fournit les fichiers journaux à un compartiment Amazon S3 que vous spécifiez. Pour plus d'informations, consultez la section Journalisation des appels d' AWS Service Catalog API avec CloudTrail.

Vous pouvez également utiliser les contraintes de notification pour configurer les notifications Amazon SNS concernant les événements de stack. Pour plus d’informations, consultez the section called “Contraintes de notification”.

Validation de conformité pour AWS Service Catalog

Des auditeurs tiers évaluent la sécurité et la conformité dans AWS Service Catalog le cadre de plusieurs programmes de AWS conformité, notamment les suivants :

- System and Organization Controls (SOC)
- Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)
- Federal Risk and Authorization Management Program (FedRAMP)
- Health Insurance Portability and Accountability Act (HIPAA)

Pour obtenir la liste des AWS services concernés par des programmes de conformité spécifiques, consultez la section Services AWS concernés par programme de conformité. Pour des informations générales, consultez Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, consultez Downloading Reports (Téléchargement des rapports) dans AWS Artifact.

Votre responsabilité en matière de conformité lors de l'utilisation AWS Service Catalog dépend de la sensibilité de vos données, des objectifs de conformité de votre entreprise et des lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur la sécurité et la conformité sur. AWS
- Livre blanc sur l'architecture pour la sécurité et la conformité HIPAA — Ce livre blanc décrit comment les entreprises peuvent créer des applications conformes à la loi HIPAA. AWS
- AWS Ressources relatives à la conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Config— Ce AWS service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Ce AWS service fournit une vue complète de l'état de votre sécurité interne, AWS ce qui vous permet de vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité.

Résilience dans AWS Service Catalog

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

Outre l'infrastructure AWS globale, AWS Service Catalog propose des actions AWS Service Catalog en libre-service. Grâce aux actions en libre-service, les clients peuvent réduire la maintenance administrative et la formation des utilisateurs finaux tout en respectant les mesures de conformité et de sécurité. Grâce aux actions en libre-service, en tant qu'administrateur vous pouvez autoriser les utilisateurs finaux à exécuter des tâches opérationnelles, notamment la sauvegarde et la restauration, résoudre des problèmes, exécuter des commandes approuvés et demander des autorisations dans AWS Service Catalog. Pour en savoir plus, veuillez consulter la section the section called “Utilisation des actions de service”.

Sécurité de l'infrastructure dans AWS Service Catalog

En tant que service géré, AWS Service Catalog il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder AWS Service Catalog via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l’aide d’un ID de clé d’accès et d’une clé d’accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d’identification de sécurité temporaires et signer les demandes.

Avec AWS Service Catalog, vous pouvez contrôler les régions dans lesquelles les données sont stockées. Les portefeuilles et les produits sont uniquement disponibles dans les régions dans lesquelles vous les avez mis à disposition. Vous pouvez utiliser l'API `CopyProduct` pour copier un produit dans une autre région.

Bonnes pratiques en matière de sécurité pour AWS Service Catalog

AWS Service Catalog fournit un certain nombre de fonctionnalités de sécurité à prendre en compte lors de l'élaboration et de la mise en œuvre de vos propres politiques de sécurité. Les bonnes pratiques suivantes doivent être considérées comme des instructions générales et ne représentent pas une solution de sécurité complète. Étant donné que ces bonnes pratiques peuvent ne pas être appropriées ou suffisantes pour votre environnement, considérez-les comme des remarques utiles plutôt que comme des recommandations.

Vous pouvez définir des règles qui limitent les valeurs de paramètre qu'un utilisateur peut saisir lors du lancement d'un produit. Ces règles sont appelées « contraintes de gabarit » car elles restreignent le déploiement du gabarit AWS CloudFormation pour le produit. Il vous suffit d'utiliser un simple éditeur pour créer des contraintes de gabarit et de les appliquer à chaque produit.

AWS Service Catalog applique des contraintes lors de l'approvisionnement d'un nouveau produit ou de la mise à jour d'un produit déjà utilisé. Il applique toujours la contrainte la plus restrictive parmi celles mises en œuvre pour le portefeuille et le produit. Par exemple, imaginez un scénario dans lequel le produit autorise le lancement de toutes les instances Amazon EC2 et où le portefeuille est soumis à deux contraintes : l'une autorise le lancement de toutes les instances EC2 de type autre que le GPU et l'autre autorise uniquement le lancement des instances EC2 t1.micro et m1.small. Dans cet exemple, AWS Service Catalog applique la deuxième contrainte, plus restrictive (t1.micro et m1.small).

Vous pouvez limiter l'accès des utilisateurs finaux aux AWS ressources lorsque vous associez une politique IAM à un rôle de lancement. Vous pouvez ensuite AWS Service Catalog créer une contrainte de lancement pour utiliser le rôle lors du lancement du produit.

Pour en savoir plus sur les politiques gérées pour AWS Service Catalog, consultez la section Politiques AWS gérées pour AWS Service Catalog.

Gestion des catalogues

AWS Service Catalog fournit une interface pour la gestion des portefeuilles, des produits et des contraintes à partir d'une console Administrateur.

> **Note**
>
> Pour effectuer des tâches de cette section, vous devez disposer des autorisations d'administrateur pour AWS Service Catalog. Pour plus d’informations, consultez Identity and Access Management dans AWS Service Catalog.

Tâches

- Gestion des portefeuilles
- Gestion des produits
- Utilisation de contraintes AWS Service Catalog
- Actions de serviceAWS Service Catalog
- Ajout de produits AWS Marketplace à votre portefeuille
- En utilisant AWS CloudFormation StackSets
- Gestion des budgets

Gestion des portefeuilles

Vous pouvez créer, consulter et mettre à jour des portefeuilles sur la page Portefeuilles de la AWS Service Catalog console d'administration.

Tâches

- Création, affichage et suppression de portefeuilles
- Affichage des détails d'un portefeuille
- Création et suppression de portefeuilles
- Ajouter des produits
- Ajout de contraintes
- Octroi d'accès à des utilisateurs
- Partage d'un portefeuille

- Partage et importation de portefeuilles

Création, affichage et suppression de portefeuilles

La page Portefeuilles affiche la liste des portefeuilles que vous avez créés dans la région actuelle. Utilisez cette page pour créer de nouveaux portefeuilles, afficher les détails d'un portefeuille ou supprimer des portefeuilles de votre compte.

Pour consulter la page Portfolios

1. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Sélectionnez une autre région, si nécessaire.
3. Si vous utilisez AWS Service Catalog pour la première fois, la page de démarrage de AWS Service Catalog s'affiche. Sélectionnez Get started pour créer un portefeuille. Suivez les instructions pour créer votre premier portfolio, puis passez à la page Portfolios.

Pendant l'utilisationAWS Service Catalog, vous pouvez revenir à la page Portfolios à tout moment ; choisissez Service Catalog dans la barre de navigation, puis Portefeuilles.

Affichage des détails d'un portefeuille

Sur la console Administrateur AWS Service Catalog, la page Portfolio details répertorie les paramètres associés à un portefeuille. Utilisez cette page pour gérer les produits du portefeuille, autoriser les utilisateurs à accéder aux produits TagOptions et appliquer des contraintes.

Pour afficher la page Portfolio details

1. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Choisissez le portefeuille que vous souhaitez gérer.

Création et suppression de portefeuilles

Utilisez la page Portefeuilles pour créer et supprimer des portefeuilles.

Pour créer un nouveau portefeuille

1. Dans le menu de navigation de gauche, choisissez Portfolios.

2. Choisissez Créer un portefeuille.
3. Sur la page Créer un portfolio, entrez les informations demandées.
4. Choisissez Créer. AWS Service Catalog crée le portefeuille et affiche les détails du portefeuille.

Pour supprimer un portefeuille

> **Note**
>
> Vous ne pouvez supprimer que des portefeuilles locaux. Vous pouvez supprimer des portefeuilles importés (partagés), mais vous ne pouvez pas supprimer des portefeuilles importés.

Avant de pouvoir supprimer un portefeuille, vous devez supprimer tous ses produits, contraintes, groupes, rôles, utilisateurs, partages et TagOptions. Pour ce faire, ouvrez un portefeuille pour afficher les détails du portefeuille. Choisissez ensuite un onglet pour les supprimer.

> **Note**
>
> Pour éviter les erreurs, supprimez les contraintes du portefeuille avant de supprimer des produits.

1. Dans le menu de navigation de gauche, choisissez Portfolios.
2. Sélectionnez le portefeuille que vous souhaitez supprimer.
3. Sélectionnez Delete (Supprimer). Vous ne pouvez supprimer que des portefeuilles locaux. Si vous essayez de supprimer un portefeuille importé (partagé), le menu Actions n'est pas disponible.
4. Dans la fenêtre de confirmation, choisissez Delete.

Ajouter des produits

Vous pouvez ajouter des produits à un portefeuille en téléchargeant un nouveau produit directement dans un portefeuille existant ou en associant un produit existant de votre catalogue au portefeuille.

> **Note**
>
> Lorsque vous créez un AWS Service Catalog produit, vous pouvez télécharger un AWS CloudFormation modèle ou un fichier de configuration Terraform. Le AWS CloudFormation modèle est stocké dans un compartiment Amazon Simple Storage Service (Amazon S3) et le nom du compartiment commence par « cf-templates- ». Vous devez également être autorisé à récupérer des objets dans des compartiments supplémentaires lors de l'approvisionnement d'un produit. Pour plus d'informations, consultez la section Création de produits.

Ajouter un nouveau produit

Vous pouvez ajouter de nouveaux produits directement depuis la page des détails du portefeuille. Lorsque vous créez un produit à partir de cette page, AWS Service Catalog l'ajoute au portefeuille que vous avez sélectionné.

Pour ajouter un nouveau produit

1. Accédez à la page Portefeuilles, puis choisissez le nom du portefeuille auquel vous souhaitez ajouter le produit.
2. Sur la page des détails du portefeuille, développez la section Produits, puis choisissez Télécharger un nouveau produit.
3. Pour Enter product details, entrez les informations suivantes :

   - Nom du produit : nom du produit.
   - Description du produit (facultatif) — Description du produit. Cette description figure dans la liste des produits pour vous aider à choisir le bon produit.
   - Description — Description complète. Cette description figure dans la liste des produits pour vous aider à choisir le bon produit.
   - Propriétaire ou distributeur : nom ou adresse e-mail du propriétaire. Les coordonnées du distributeur sont facultatives.
   - Fournisseur (facultatif) : nom de l'éditeur de l'application. Ce champ permet de trier la liste des produits pour faciliter la recherche de produits.
4. Sur la page Version details, entrez ce qui suit :

   - Choisissez un modèle : pour les AWS CloudFormation produits, choisissez votre propre fichier modèle, un AWS CloudFormation modèle provenant d'un lecteur local ou une URL pointant

vers un modèle stocké dans Amazon S3, un modèle AWS CloudFormation Stack ARN existant ou un fichier modèle stocké dans un référentiel externe.

Pour les produits Teraform, choisissez votre propre fichier modèle, un fichier de configuration tar.gz provenant d'un lecteur local ou une URL pointant vers un modèle stocké dans Amazon S3, ou un fichier de configuration tar.gz stocké dans un référentiel externe.

- Nom de la version (facultatif) — Le nom de la version du produit (par exemple, « v1 », « v2beta »). Les espaces ne sont pas autorisés.
- Description (facultatif) — Description de la version du produit, indiquant en quoi cette version diffère de la version précédente.

5. Pour Enter support details, entrez les informations suivantes :

   - Contact par e-mail (facultatif) : adresse e-mail utilisée pour signaler les problèmes liés au produit.
   - Lien d'assistance (facultatif) : URL d'un site où les utilisateurs peuvent trouver des informations d'assistance ou déposer des tickets. L'URL doit commencer par `http://` ou `https://`. Les administrateurs sont responsables du maintien de l'exactitude et de l'accès aux informations d'assistance.
   - Description du support (facultatif) — Description de la manière dont vous devez utiliser le contact par e-mail et le lien d'assistance.

6. Choisissez Créer un produit.

Ajouter un produit existant

Vous pouvez ajouter des produits existants à un portefeuille à partir de trois emplacements : la liste des portefeuilles, la page des détails du portefeuille ou la page de la liste des produits.

Pour ajouter un produit existant à un portefeuille

1. Accédez à la page Portfolios.
2. Choisissez un portefeuille. Choisissez ensuite Actions - Ajouter un produit au portefeuille.
3. Choisissez un produit, puis choisissez Ajouter un produit au portefeuille.

Supprimer un produit d'un portefeuille

Lorsque vous ne souhaitez plus utiliser un produit, supprimez-le d'un portefeuille. Le produit est toujours disponible dans votre catalogue depuis la page Produits, et vous pouvez toujours l'ajouter à d'autres portefeuilles. Vous pouvez supprimer plusieurs produits d'un portefeuille en une seule fois.

Pour supprimer un produit d'un portefeuille

1. Accédez à la page Portefeuilles, puis choisissez le portefeuille contenant le produit. La page des détails du portefeuille s'ouvre.
2. Développez la section Produits.
3. Choisissez un ou plusieurs produits, puis sélectionnez Supprimer.
4. Confirmez votre choix.

Ajout de contraintes

Vous devez ajouter des contraintes pour contrôler la manière dont les utilisateurs interagissent avec les produits. Pour plus d'informations sur les types de contraintes prises en charge par AWS Service Catalog, consultez Utilisation de contraintes AWS Service Catalog.

Vous ajoutez des contraintes à des produits une fois qu'ils ont été placés dans un portefeuille.

Pour ajouter une contrainte à un produit

1. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Choisissez Portefeuilles, puis sélectionnez un portefeuille.
3. Sur la page des détails du portefeuille, développez la section Créer une contrainte et choisissez Ajouter des contraintes.
4. Pour Produit, sélectionnez le produit auquel appliquer la contrainte.
5. Pour Type de contrainte, choisissez l'une des options suivantes :

   Lancer : vous permet d'attribuer un rôle IAM au produit utilisé pour approvisionner les AWS ressources. Pour plus d’informations, consultez Contraintes de lancement AWS Service Catalog.

   Notification : vous permet de diffuser des notifications de produits sur une rubrique Amazon SNS. Pour plus d’informations, consultez Contraintes de notification AWS Service Catalog.

Modèle : vous permet de limiter les options disponibles pour les utilisateurs finaux lorsqu'ils lancent le produit. Un modèle consiste en un fichier texte au format JSON qui contient une ou plusieurs règles. Les règles sont ajoutées au modèle AWS CloudFormation utilisé par le produit. Pour plus d'informations, consultez Règles de contrainte de modèle.

Stack Set — Vous permet de configurer le déploiement du produit sur plusieurs comptes et régions à l'aide de AWS CloudFormation StackSets. Pour plus d'informations, consultez Contraintes d'ensemble de piles AWS Service Catalog.

Mise à jour des balises : vous permet de mettre à jour les balises une fois le produit approvisionné. Pour plus d'informations, consultez la section Contraintes de mise à jour des AWS Service Catalog balises.

6. Choisissez Continuer et entrez les informations requises.

Pour modifier une contrainte

1. Connectez-vous à la console d'administration AWS Management Console et AWS Service Catalog ouvrez-la à l'adresse https://console.aws.amazon.com/catalog/.
2. Choisissez Portefeuilles, puis sélectionnez un portefeuille.
3. Sur la page des détails du portefeuille, développez la section Créer une contrainte et sélectionnez la contrainte à modifier.
4. Choisissez Modifier les contraintes.
5. Modifiez la contrainte selon vos besoins, puis choisissez Enregistrer.

Octroi d'accès à des utilisateurs

Donnez aux utilisateurs l'accès aux portefeuilles par le biais de groupes ou de rôles. La meilleure façon de fournir un accès au portefeuille à de nombreux utilisateurs est de placer les utilisateurs dans un groupe IAM et d'accorder l'accès à ce groupe. Ainsi, vous pouvez simplement ajouter et supprimer des utilisateurs dans le groupe pour gérer l'accès au portefeuille. Pour plus d'informations, consultez la section Utilisateurs et groupes IAM dans le Guide de l'utilisateur IAM.

Outre l'accès à un portefeuille, les utilisateurs doivent également avoir accès à la console de l'utilisateur AWS Service Catalog final. Vous accordez l'accès à la console en appliquant des autorisations dans IAM. Pour plus d'informations, consultez Identity and Access Management dans AWS Service Catalog.

Si vous souhaitez partager un portefeuille et ses principaux avec d'autres comptes, vous pouvez associer des noms principaux (groupes, rôles ou utilisateurs) au portefeuille. Les noms principaux sont partagés avec le portefeuille et utilisés dans les comptes des destinataires pour accorder l'accès aux utilisateurs finaux.

Pour accorder l'accès à un portefeuille à des utilisateurs ou des groupes

1. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Dans le volet de navigation, choisissez Administration, puis Portfolios.
3. Choisissez un portefeuille auquel vous souhaitez accorder l'accès à des groupes, des rôles ou des utilisateurs. AWS Service Catalogdirige vers la page des détails du portefeuille.
4. Sur la page des détails du portefeuille, choisissez l'onglet Accès.
5. Sous Accès au portefeuille, choisissez Accorder l'accès.
6. Pour Type, choisissez Nom principal, puis sélectionnez le groupe/, role/ ou utilisateur/, Type. Vous pouvez ajouter jusqu'à 9 noms principaux.
7. Choisissez Accorder l'accès pour associer le principal au portefeuille actuel.

Pour supprimer l'accès à un portefeuille

1. Sur la page des détails du portefeuille, choisissez un groupe, un rôle ou un nom d'utilisateur.
2. Choisissez Supprimer l'accès.

Partage d'un portefeuille

Pour permettre à AWS Service Catalog l'administrateur d'un autre AWS compte de distribuer vos produits aux utilisateurs finaux, partagez votre AWS Service Catalog portefeuille avec eux en utilisant account-to-account le partage ouAWS Organizations.

Lorsque vous partagez un portefeuille à l'aide du account-to-account partage ou d'Organizations, vous partagez une référence de ce portefeuille. Les produits et les contraintes du portefeuille importé restent synchronisés avec les modifications que vous apportez au portefeuille partagé, le portefeuille d'origine que vous avez partagé.

Le destinataire ne peut pas modifier les produits ou les contraintes, mais peut ajouter AWS Identity and Access Management un accès pour les utilisateurs finaux.

> **Note**
>
> Vous ne pouvez pas partager une ressource partagée. Cela inclut les portefeuilles contenant un produit partagé.

Un ccount-to-account partage

Pour effectuer ces étapes, vous devez obtenir l'identifiant du AWS compte cible. Vous pouvez trouver l'identifiant sur la page Mon compte AWS Management Console du compte cible.

Pour partager un portefeuille avec un AWS compte

1. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Dans le menu de navigation de gauche, choisissez Portefeuilles, puis sélectionnez le portefeuille que vous souhaitez partager. Dans le menu Actions, sélectionnez Partager.
3. Dans Entrez l'identifiant du compte, entrez l'identifiant du AWS compte avec lequel vous partagez. (Facultatif) Sélectionnez TagOption Partage. Choisissez ensuite Partager.
4. Envoyez l'URL à l'administrateur AWS Service Catalog du compte cible. L'URL ouvre la page Importer le portefeuille avec l'ARN du portefeuille partagé automatiquement fourni.

Importation d'un portefeuille

Si AWS Service Catalog l'administrateur d'un autre AWS compte partage un portefeuille avec vous, importez ce portefeuille dans votre compte afin de pouvoir distribuer ses produits à vos utilisateurs finaux.

Il n'est pas nécessaire d'importer un portefeuille s'il a été partagé viaAWS Organizations.

Pour importer le portefeuille, vous devez obtenir l'identifiant du portefeuille auprès de l'administrateur.

Pour afficher tous les portfolios importés, ouvrez la AWS Service Catalog console à l'adresse https://console.aws.amazon.com/servicecatalog/. Sur la page Portefeuilles, sélectionnez l'onglet Importé. Consultez le tableau des portefeuilles importés.

Partage avec AWS Organizations

Vous pouvez partager des portefeuilles AWS Service Catalog à l'aide d'AWS Organizations.

Tout d'abord, vous devez décider si vous partagez à partir du compte de gestion ou d'un compte d'administrateur délégué. Si vous ne souhaitez pas partager depuis votre compte de gestion, créez un compte d'administrateur délégué que vous pouvez utiliser pour le partage. Pour plus d'informations, veuillez consulter la rubrique Enregistrer un administrateur délégué dans le Guide de l'utilisateur AWS CloudFormation.

Ensuite, vous devez décider avec qui le partager. Vous pouvez le partager avec les entités suivantes :

- Un compte d'organisation.
- Une unité d'organisation (UO).
- L'organisation elle-même. Dans ce cas, le partage se fait avec chaque compte de l'organisation.

Partage depuis un compte de gestion

Vous pouvez partager un portefeuille avec une organisation en utilisant votre structure organisationnelle ou en saisissant l'ID d'un nœud d'organisation.

Pour partager un portefeuille avec une organisation en utilisant la structure organisationnelle

1. Ouvrez la AWS Service Catalog console à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Sur la page Portefeuilles, sélectionnez le portefeuille que vous souhaitez partager. Dans le menu Actions, sélectionnez Partager.
3. Sélectionnez AWS Organizationset filtrez dans votre structure organisationnelle.

   Vous pouvez sélectionner le nœud racine pour partager le portefeuille avec l'ensemble de votre organisation, une unité organisationnelle (UO) parent, une unité organisationnelle enfant ou un AWS compte au sein de votre organisation.

   Le partage avec une unité d'organisation mère partage le portefeuille entre tous les comptes et les unités d'organisation enfants au sein de cette unité d'organisation mère.

   Vous pouvez sélectionner Afficher AWS les comptes uniquement pour afficher la liste de tous les AWS comptes de votre organisation.

Pour partager un portefeuille avec une organisation en saisissant l'ID du nœud organisationnel

1. Ouvrez la AWS Service Catalog console à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Sur la page Portefeuilles, sélectionnez le portefeuille que vous souhaitez partager. Dans le menu Actions, sélectionnez Partager.
3. Sélectionnez Organization Node.

   Indiquez si vous souhaitez partager avec l'ensemble de votre organisation, un AWS compte au sein de votre organisation ou une unité d'organisation.

   Entrez l'ID du nœud organisationnel que vous avez sélectionné, que vous pouvez trouver dans la AWS Organizations console à l'adresse https://console.aws.amazon.com/organizations/.

Partage à partir d'un compte administrateur délégué

Le compte de gestion d'une organisation peut enregistrer ou désenregistrer d'autres comptes en tant qu'administrateurs délégués de l'organisation.

Un administrateur délégué peut partager AWS Service Catalog les ressources de son organisation de la même manière qu'un compte de gestion. Ils sont autorisés à créer, supprimer et partager des portefeuilles.

Pour enregistrer ou désenregistrer un administrateur délégué, vous devez utiliser l'API ou la CLI depuis le compte de gestion. Pour plus d'informations, veuillez consulter les sections RegisterDelegatedAdministrator et DeregisterDelegatedAdministrator (français non garanti) de la Référence d'API AWS Organizations.

> **Note**
>
> Avant de pouvoir désigner un délégué, l'administrateur doit appeler `EnableAWSOrganizationsAccess`.

La procédure de partage d'un portefeuille à partir d'un compte d'administrateur délégué est identique à celle du partage à partir d'un compte de gestion, comme indiqué ci-dessus dansthe section called “Partage depuis un compte de gestion”.

Si un membre est désenregistré en tant qu'administrateur délégué, les événements suivants se produisent :

- Les actions de portefeuille créées à partir de ce compte sont supprimées.
- Il ne peut plus créer d'actions de portefeuille.

> **Note**
>
> Si le portefeuille et les actions créés par un administrateur délégué ne sont pas supprimés après la désinscription de l'administrateur délégué, enregistrez et désenregistrez à nouveau l'administrateur délégué. Cette action supprime le portefeuille et les actions créés par ce compte.

Déplacer des comptes au sein de votre organisation

Si vous déplacez un compte au sein de votre organisation, les AWS Service Catalog portefeuilles partagés avec ce compte peuvent changer.

Les comptes ont uniquement accès aux portefeuilles partagés avec leur organisation ou unité organisationnelle de destination.

Partage TagOptions lors du partage de portefeuilles

En tant qu'administrateur, vous pouvez créer un partage à inclure TagOptions. TagOptions sont des paires clé-valeur qui permettent aux administrateurs de :

- Définissez et appliquez la taxonomie des balises.
- Définissez les options de balise et associez-les aux produits et aux portefeuilles.
- Partagez les options de tag associées aux portefeuilles et aux produits avec d'autres comptes.

Lorsque vous ajoutez ou supprimez des options de balise dans le compte principal, les modifications apparaissent automatiquement dans les comptes des destinataires. Dans les comptes destinataires, lorsqu'un utilisateur final approvisionne un produit TagOptions, il doit choisir des valeurs pour les balises qui deviennent des balises sur le produit approvisionné.

Dans les comptes des destinataires, les administrateurs peuvent associer des TagOptions éléments locaux supplémentaires à leur portefeuille importé afin d'appliquer les règles de balisage spécifiques à ce compte.

> **Note**
>
> Pour partager un portefeuille, vous avez besoin de l'identifiant de AWS compte du consommateur. Trouvez l'identifiant du AWS compte dans Mon compte de la console.

> **Note**
>
> Si TagOption a une valeur unique, applique AWS automatiquement cette valeur pendant le processus de provisionnement.

À partager TagOptions lors du partage de portefeuilles

1. Dans le menu de navigation de gauche, choisissez Portfolios.
2. Dans Portefeuilles locaux, choisissez et ouvrez un portefeuille.
3. Choisissez Partager dans la liste ci-dessus, puis cliquez sur le bouton Partager.
4. Choisissez de partager avec un autre AWS compte ou une autre organisation.
5. Entrez le numéro d'identification du compte à 12 chiffres, sélectionnez Activer, puis sélectionnez Partager.

   Le compte que vous avez partagé apparaît dans la section Comptes partagés avec. Il indique si elles TagOptions ont été activées.

Vous pouvez également mettre à jour une part de portefeuille pour l'inclure TagOptions. Tout TagOptions ce qui appartient au portefeuille et au produit est désormais partagé sur ce compte.

Pour mettre à jour une part de portefeuille afin d'inclure TagOptions

1. Dans le menu de navigation de gauche, choisissez Portfolios.
2. Dans Portefeuille local, choisissez et ouvrez un portefeuille.
3. Choisissez Partager dans la liste ci-dessus.

4. Dans Comptes partagés avec, choisissez un identifiant de compte, puis sélectionnez Actions.
5. Sélectionnez Mettre à jour, annuler le partage ou Annuler le partage.

   Lorsque vous sélectionnez Mettre à jour et annuler le partage, choisissez Activer pour lancer le partage TagOptions. Le compte que vous avez partagé apparaît dans la section Comptes partagés avec.

   Lorsque vous sélectionnez Annuler le partage, confirmez que vous ne souhaitez plus partager le compte.

Partage des principaux noms lors du partage de portefeuilles

En tant qu'administrateur, vous pouvez créer un partage de portefeuille qui inclut les noms principaux. Les noms principaux sont des noms de groupes, de rôles et d'utilisateurs que les administrateurs peuvent spécifier dans un portefeuille, puis partager avec le portefeuille. Lorsque vous partagez le portefeuille, AWS Service Catalog vérifiez si ces noms principaux existent déjà. S'ils existent, associe AWS Service Catalog automatiquement les principaux IAM correspondants au portefeuille partagé pour accorder l'accès aux utilisateurs.

> **Note**
>
> Lorsque vous associez un principal à un portefeuille, une escalade des privilèges peut potentiellement se produire si ce portefeuille est ensuite partagé avec d'autres comptes. Pour un utilisateur d'un compte destinataire qui n'est pas AWS Service Catalog administrateur, mais qui est toujours en mesure de créer des principaux (utilisateurs/rôles), cet utilisateur peut créer un directeur IAM correspondant à une association de noms principaux pour le portefeuille. Bien que cet utilisateur ne sache pas quels noms de principaux sont associés par le biais de AWS Service Catalog, il peut être en mesure de deviner l'identité de l'utilisateur. Si cette escalade potentielle pose problème, AWS Service Catalog recommande d'utiliser `PrincipalType` comme `IAM`. Avec cette configuration, le `PrincipalARN` doit déjà exister sur le compte destinataire avant de pouvoir être associé.

Lorsque vous ajoutez ou supprimez des noms principaux dans le compte principal, ces modifications sont AWS Service Catalog automatiquement appliquées au compte destinataire. Les utilisateurs du compte destinataire peuvent ensuite effectuer des tâches en fonction de leur rôle :

- Les utilisateurs finaux peuvent approvisionner, mettre à jour et résilier le produit du portefeuille.

- Les administrateurs peuvent associer des IAM Principals supplémentaires à leur portefeuille importé pour accorder l'accès aux utilisateurs finaux spécifiques à ce compte.

> **Note**
>
> Le partage de nom principal n'est disponible que pourAWS Organizations.

Pour partager les noms principaux lors du partage de portefeuilles

1. Dans le menu de navigation de gauche, choisissez Portfolios.
2. Dans Portefeuilles locaux, choisissez le portefeuille que vous souhaitez partager.
3. Dans le menu Actions, choisissez Partager.
4. Sélectionnez une organisation dansAWS Organizations.
5. Sélectionnez la racine de l'organisation dans son intégralité, une unité organisationnelle (UO) ou un membre de l'organisation.
6. Dans les paramètres de partage, activez l'option de partage principal.

Vous pouvez également mettre à jour un partage de portefeuille pour inclure le partage du nom principal. Cela permet de partager tous les noms principaux appartenant à ce portefeuille avec le compte du destinataire.

Pour mettre à jour une part de portefeuille afin d'activer ou de désactiver les noms principaux

1. Dans le menu de navigation de gauche, choisissez Portfolios.
2. Dans Portefeuille local, choisissez le portefeuille que vous souhaitez mettre à jour.
3. Choisissez l'onglet Partager.
4. Sélectionnez le partage que vous souhaitez mettre à jour, puis choisissez Partager.
5. Choisissez Mettre à jour le partage, puis sélectionnez Activer pour lancer le partage principal. AWS Service Catalogpartage ensuite les noms principaux dans les comptes des destinataires.

Désactivez le partage principal si vous souhaitez arrêter de partager les noms principaux avec les comptes des destinataires.

Utilisation de caractères génériques lors du partage de noms principaux

AWS Service Catalogpermet d'accorder l'accès au portefeuille aux principaux noms IAM (utilisateur, groupe ou rôle) avec des caractères génériques, tels que « * » ou « ? ». L'utilisation de modèles génériques vous permet de couvrir plusieurs noms principaux IAM à la fois. Le chemin ARN et le nom principal autorisent un nombre illimité de caractères génériques.

Exemples d'un ARN générique acceptable :

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

Exemples d'un ARN générique inacceptable :

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

Dans le format IAM Principal ARN (**`arn:partition:iam:::resource-type/resource-path/resource-name`**), les valeurs valides incluent user/, group/ ou role/. Le « ? » et « * » ne sont autorisés qu'après le type de ressource dans le segment resource-id. Vous pouvez utiliser des caractères spéciaux n'importe où dans l'identifiant de ressource.

Le caractère « * » correspond également au caractère «/», ce qui permet de former des chemins dans l'identifiant de ressource. Par exemple :

`arn:aws:iam:::role/*/ResourceName_?`correspond aux deux **`arn:aws:iam:::role/pathA/pathB/ResourceName_1`** et**`arn:aws:iam:::role/pathA/ResourceName_1`**.

Partage et importation de portefeuilles

Pour mettre vos AWS Service Catalog produits à la disposition d'utilisateurs qui ne font pas partie de la vôtreComptes AWS, tels que les utilisateurs appartenant à d'autres organisations ou Comptes AWS à d'autres membres de votre organisation, vous partagez vos portefeuilles avec eux. Vous pouvez partager de différentes manières, notamment le account-to-account partage, le partage organisationnel et le déploiement de catalogues à l'aide d'ensembles de piles.

Avant de partager vos produits et portefeuilles avec d'autres comptes, vous devez décider si vous souhaitez partager une référence du catalogue ou déployer une copie du catalogue dans chaque compte destinataire. Notez que si vous déployez une copie, vous devez effectuer un nouveau déploiement en cas de mises à jour que vous souhaitez propager aux comptes destinataires.

Vous pouvez utiliser des ensembles de piles pour déployer votre catalogue dans de nombreux comptes en même temps. Si vous souhaitez partager une référence (une version importée de votre portfolio qui reste synchronisée avec l'original), vous pouvez utiliser le account-to-account partage ou le partager en utilisantAWS Organizations.

Pour utiliser des ensembles de piles pour déployer une copie de votre catalogue, consultez Comment configurer un catalogue multirégional et multi-comptes de produits standard AWS Service Catalog de l'entreprise.

Lorsque vous partagez un portefeuille en utilisant le account-to-account partage ouAWS Organizations, vous autorisez AWS Service Catalog l'administrateur d'un autre AWS compte à importer votre portefeuille dans son compte et à distribuer les produits aux utilisateurs finaux via ce compte.

Ce portefeuille importé n'est pas une copie indépendante. Les produits et les contraintes du portefeuille importé restent synchronisés avec les modifications que vous apportez au portefeuille partagé, le portefeuille d'origine que vous avez partagé. L'administrateur destinataire, l'administrateur avec lequel vous partagez un portefeuille, ne peut pas modifier les produits ou les contraintes, mais peut ajouter un accès AWS Identity and Access Management (IAM) pour les utilisateurs finaux. Pour plus d’informations, consultez Octroi d'accès à des utilisateurs.

L'administrateur destinataire peut distribuer les produits aux utilisateurs finaux associés à son AWS compte de la manière suivante :

- En ajoutant des utilisateurs, des groupes et des rôles au portefeuille importé.
- En ajoutant des produits du portefeuille importé à un portefeuille local, un portefeuille distinct créé par l'administrateur du destinataire et appartenant à son AWS compte. L'administrateur du destinataire ajoute ensuite des utilisateurs, des groupes et des rôles à ce portefeuille local. Toutes les contraintes initialement appliquées aux produits du portefeuille partagé sont également présentes dans le portefeuille local. L'administrateur local du destinataire du portefeuille peut ajouter des contraintes supplémentaires, mais ne peut pas supprimer les contraintes initialement importées depuis le portefeuille partagé.

Lorsque vous ajoutez des produits ou des contraintes au portefeuille partagé, ou que vous supprimez des produits ou des contraintes de celui-ci, la modification est propagée à toutes les instances importées du portefeuille. Par exemple, si vous supprimez un produit du portefeuille partagé, ce produit est également supprimé du portefeuille importé. Il est également supprimé de tous les portefeuilles locaux auxquels le produit importé a été ajouté. Si un utilisateur final a lancé un produit

avant que vous ne le supprimiez, le produit provisionné de l'utilisateur final continue de s'exécuter, mais le produit devient indisponible pour les futurs lancements.

Si vous appliquez une contrainte de lancement à un produit dans un portefeuille partagé, celle-ci est propagée à toutes les instances importées du produit. Pour remplacer cette contrainte de lancement, l'administrateur destinataire ajoute le produit dans un portefeuille local, puis applique une contrainte de lancement différente à ce produit. La contrainte de lancement en vigueur définit un rôle de lancement pour le produit.

Un rôle de lancement est un rôle IAM AWS Service Catalog utilisé pour fournir des AWS ressources (telles que des instances Amazon EC2 ou des bases de données Amazon RDS) lorsqu'un utilisateur final lance le produit. En tant qu'administrateur, vous pouvez choisir de désigner un ARN de rôle de lancement spécifique ou un nom de rôle local. Si vous utilisez le rôle ARN, celui-ci sera utilisé même si l'utilisateur final appartient à un AWS compte différent de celui qui possède le rôle de lancement. Si vous utilisez un nom de rôle local, le rôle IAM portant ce nom dans le compte de l'utilisateur final est utilisé.

Pour plus d'informations sur les contraintes de lancement et les rôles de lancement, consultez Contraintes de lancement AWS Service Catalog. Le compte AWS qui possède le rôle de lancement provisionne les ressources AWS, et les coûts d'utilisation sont facturés à ce compte pour ces ressources. Pour plus d’informations, consultez Tarification d’AWS Service Catalog.

Cette vidéo vous montre comment partager des portefeuilles entre différents comptes dansAWS Service Catalog.

Partagez (https://www.youtube.com/embed/BVSohYOppjk%22%3EShare) Portefeuilles entre comptes dans AWS Service Catalog.

> **Note**
>
> Vous ne pouvez pas repartager des produits à partir d'un portefeuille qui a été importé ou partagé.

> **Note**
>
> Les importations de portefeuille doivent avoir lieu dans la même région entre le compte de gestion et le compte dépendant.

Relation entre des portefeuilles partagés et des portefeuilles importés

Ce tableau résume la relation entre un portefeuille importé et un portefeuille partagé, ainsi que les actions qu'un administrateur qui importe un portefeuille peut et ne peut pas effectuer avec ce portefeuille et les produits qu'il contient.

Élément de portefeuille partagé	Relation avec un portefeuille importé	L'administrateur destinataire peut	L'administrateur destinataire ne peut pas
Produits et versions de produit	Héritées. Si le créateur du portefeuille ajoute des produits ou supprime des produits dans le portefeuille partagé, la modification est propagée vers le portefeuille importé.	Ajouter des produits importés à portefeuilles locaux. Les produits restent synchronisés avec le portefeuille partagé.	Télécharger ou ajouter des produits au portefeuille importé, ou supprimer des produits du portefeuille importé.
Contraintes de lancement	Héritées. Si le créateur du portfolio ajoute des contraintes de lancement ou supprime des contraintes de lancement d'un produit partagé, la modification se propage à toutes les instances importées du produit. Si l'administrateur du destinataire ajoute	Dans un portefeuille local, l'administrateur peut appliquer des contraintes de lancement qui affectent le lancement local du produit.	Ajouter des contraintes de lancement au portefeuille importé ou en supprimer.

Élément de portefeuille partagé	Relation avec un portefeuille importé	L'administrateur destinataire peut	L'administrateur destinataire ne peut pas
	un produit importé à son portefeuille local, cette contrainte de lancement importée n'est pas répercutée sur le portefeuille partagé.		
Contraintes de modèle	Héritées. Si le créateur du portefeuille ajoute une contrainte de modèle ou supprime des contraintes de modèle dans un produit partagé, la modification est propagée à toutes les instances importées du produit. Si l'administrateur du destinataire ajoute un produit importé à un portefeuille local, les contraintes du modèle importé ne sont pas répercutées sur le portefeuille local.	Dans un portefeuille local, l'administrateur peut ajouter des contraintes de modèle qui limitent le produit local.	Supprimer les contraintes de modèle importées.

Élément de portefeuille partagé	Relation avec un portefeuille importé	L'administrateur destinataire peut	L'administrateur destinataire ne peut pas
Utilisateurs, groupes et rôles	Non héritée.	Ajoutez des utilisateurs, des groupes et des rôles figurant dans le AWS compte de l'administrateur.	Non applicable.

Gestion des produits

Vous pouvez créer des produits, mettre à jour des produits en créant une nouvelle version basée sur un modèle mis à jour et regrouper les produits dans des portefeuilles afin de les distribuer aux utilisateurs.

Les nouvelles versions de produits sont propagées vers tous les utilisateurs qui ont accès au produit grâce à un portefeuille. Lorsque vous distribuez une mise à jour, les utilisateurs finaux peuvent mettre à jour les produits provisionnés existants.

Tâches

- Affichage de la page des produits
- Création de produits
- Ajouter des produits aux portefeuilles
- Mise à jour des produits
- Synchronisation de produits avec des modèles de fichiers provenant GitHub d' GitHub Enterprise ou de Bitbucket
- Supprimer des produits
- Gestion des versions

Affichage de la page des produits

Vous gérez les produits depuis la page Liste des produits de la console AWS Service Catalog d'administration.

Pour consulter la page de liste des produits

1. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Choisissez la liste des produits.

Création de produits

Vous créez des produits à partir de la page Produits dans la console Administrateur AWS Service Catalog.

> **Note**
>
> La création de produits Terraform nécessite une configuration supplémentaire, notamment un moteur de provisionnement Terraform et un rôle de lancement. Pour plus d'informations, consultezCommencer à utiliser un produit Terraform.

Pour créer un nouveau produit AWS Service Catalog

1. Accédez à la page de liste des produits.
2. Choisissez Créer un produit, puis choisissez Créer un produit.
3. Détails du produit : vous permet de choisir le type de produit que vous souhaitez créer. AWS Service Catalogprend en chargeAWS CloudFormation, Terraform Cloud et types de produits externes (prend en charge Terraform Community Edition). Les détails du produit contiennent également les métadonnées qui apparaissent lorsque vous recherchez et consultez des produits dans une liste ou une page détaillée. Saisissez :
   - Nom du produit : nom du produit.
   - Description du produit — La description apparaît dans la liste des produits pour vous aider à choisir le bon produit.
   - Propriétaire : personne ou organisation qui publie ce produit. Le propriétaire peut être le nom de votre organisation informatique ou celui de votre administrateur.
   - Distributeur (facultatif) : nom de l'éditeur de l'application. Ce champ permet de trier la liste des produits pour faciliter la recherche de produits.
4. Les détails de version vous permettent d'ajouter votre fichier modèle et de créer votre produit. Saisissez :

- Choisir une méthode — Il existe quatre méthodes pour ajouter un fichier modèle.
  - Utiliser un fichier modèle local - Téléchargez un AWS CloudFormation modèle ou un fichier de configuration Terraform tar.gz à partir d'un lecteur local.
  - Utiliser une URL Amazon S3 : spécifiez une URL qui pointe vers un AWS CloudFormation modèle ou un fichier de configuration Terraform tar.gz stocké dans Amazon S3. Si vous spécifiez une URL Amazon S3, elle doit commencer par`https://`.
  - Utiliser un référentiel externe : spécifiez votre référentiel de code GitHub, GitHub Enterprise ou Bitbucket. AWS Service Catalogvous permet de synchroniser des produits avec des fichiers modèles. Pour les produits Terraform, le format de fichier modèle doit être un seul fichier archivé dans Tar et compressé dans Gzip.
  - Utiliser une CloudFormation pile existante : entrez l'ARN d'une CloudFormation pile existante. Cette méthode ne prend pas en charge les produits Terraform Cloud ou externes.
- Nom de la version (facultatif) — Le nom de la version du produit (par exemple, « v1 », « v2beta »). Les espaces ne sont pas autorisés.
- Description (facultatif) — Description de la version du produit, notamment en quoi cette version diffère des autres versions.
- Conseils — Géré dans l'onglet Versions de la page de détails d'un produit. Lorsqu'une version de produit est créée, pendant le processus de création du produit, les instructions relatives à cette version sont définies par défaut. Pour en savoir plus sur les conseils, consultez la section Gestion des versions.

5. Les informations relatives au support identifient l'organisation au sein de votre entreprise et fournissent un point de contact pour l'assistance. Saisissez :

   - Contact par e-mail (facultatif) : adresse e-mail utilisée pour signaler les problèmes liés au produit.
   - Lien d'assistance (facultatif) : URL d'un site où les utilisateurs peuvent trouver des informations d'assistance ou déposer des tickets. L'URL doit commencer par `http://` ou `https://`. Les administrateurs sont responsables du maintien de l'exactitude et de l'accès aux informations d'assistance.
   - Description du support (facultatif) — Description de la manière dont vous devez utiliser le contact par e-mail et le lien d'assistance.

6. Gérer les balises (facultatif) — En plus d'utiliser des balises pour classer vos ressources, vous pouvez également les utiliser pour authentifier vos autorisations de création de cette ressource.

7. Créer un produit — Lorsque vous avez rempli le formulaire, sélectionnez Créer un produit. Après quelques secondes, le produit apparaît sur la page de liste des produits. Vous pouvez avoir besoin d'actualiser votre navigateur pour voir le produit.

Vous pouvez également l'utiliser CodePipeline pour créer et configurer un pipeline afin de déployer votre modèle de produit AWS Service Catalog et d'apporter les modifications que vous avez apportées à votre référentiel source. Pour plus d'informations, consultez Didacticiel : Création d'un pipeline qui se déploie dans AWS Service Catalog.

Vous pouvez définir les propriétés des paramètres dans votre modèle AWS CloudFormation ou dans celui de Terraform et appliquer ces règles lors du provisionnement. Ces propriétés peuvent définir la longueur minimale et maximale, les valeurs minimales et maximales, les valeurs autorisées et une expression régulière pour la valeur. AWS Service Catalogémet un avertissement lors du provisionnement si la valeur fournie ne respecte pas la propriété du paramètre. Pour en savoir plus sur les propriétés des paramètres, consultez la section Paramètres du guide de AWS CloudFormation l'utilisateur.

Résolution des problèmes

Vous devez être autorisé à récupérer des objets depuis des compartiments Amazon S3. Dans le cas contraire, vous risquez de rencontrer l'erreur suivante lors du lancement ou de la mise à jour d'un produit.

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

Si vous recevez ce message, assurez-vous d'être autorisé à récupérer des objets dans les compartiments suivants :

- Le compartiment dans lequel le modèle d'artefact de provisionnement est stocké.
- Le bucket qui commence par « cf-templates-* » et dans lequel est stocké le modèle d'artefact d'AWS Service Catalogapprovisionnement.
- Le compartiment interne qui commence par « sc-* » et où AWS Service Catalog stocke les métadonnées. Vous ne pourrez pas voir ce compartiment depuis votre compte.

L'exemple de politique suivant indique les autorisations minimales requises pour récupérer des objets dans les compartiments mentionnés précédemment.

```
{
```

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

Ajouter des produits aux portefeuilles

Vous pouvez ajouter des produits à autant de portefeuilles que vous le souhaitez. Lorsqu'un produit est mis à jour, tous les portefeuilles (y compris les portefeuilles partagés) contenant le produit reçoivent automatiquement la nouvelle version.

Ajout d'un produit à un portefeuille à partir de votre catalogue

1. Accédez à la page de liste des produits.
2. Sélectionnez un produit, puis sélectionnez Actions. Dans le menu déroulant, choisissez Ajouter un produit au portefeuille. Vous êtes redirigé vers la page Ajouter ***name-of-product*** au portfolio.
3. Choisissez un portefeuille, puis choisissez Ajouter un produit au portefeuille.

Lors de l'ajout d'un produit Terraform à un portefeuille, le produit nécessite une contrainte de lancement. Vous devez sélectionner un rôle IAM dans votre compte, saisir un ARN de rôle IAM ou saisir un nom de rôle. Si vous spécifiez un nom de rôle et si un compte utilise la contrainte de lancement, le compte utilise ce nom pour le rôle IAM. Cela permet aux contraintes relatives aux rôles de lancement d'être indépendantes du compte, ce qui vous permet de créer moins de ressources par compte partagé. Pour plus de détails et des instructions, consultez Étape 6 : Ajouter une contrainte de lancement à votre produit Terraform

Un portefeuille peut contenir de nombreux produits qui sont une combinaison de types AWS CloudFormation de produits Terraform.

Mise à jour des produits

Lorsque vous mettez à jour le modèle d'un produit, vous créez une nouvelle version du produit. Les nouvelles versions du produit sont automatiquement disponibles pour tous les utilisateurs qui ont accès à un portefeuille contenant le produit.

> **Note**
>
> Lors de la mise à jour d'un produit existant, vous ne pouvez pas modifier le type de produit (AWS CloudFormationni Teraform). Par exemple, si vous mettez à jour un AWS CloudFormation produit, vous ne pouvez pas remplacer le AWS CloudFormation modèle existant par un fichier de configuration Terraform tar.gz. Vous devez mettre à jour le fichier AWS CloudFormation modèle existant avec un nouveau fichier AWS CloudFormation modèle.

Les utilisateurs finaux qui exécutent actuellement un produit provisionné de la version précédente du produit peuvent mettre à jour leur produit provisionné vers la nouvelle version. Lorsqu'une nouvelle version d'un produit est disponible, les utilisateurs peuvent utiliser la commande Mettre à jour le produit provisionné sur les pages de liste des produits provisionnés ou de détails des produits provisionnés.

Avant de créer une nouvelle version d'un produit, il est AWS Service Catalog recommandé de tester les mises à jour de votre produit dans AWS CloudFormation ou dans le moteur Terraform pour vous assurer qu'elles fonctionnent correctement.

Pour créer une nouvelle version de produit

1. Accédez à la page de liste des produits.
2. Choisissez le produit que vous souhaitez mettre à jour. Vous êtes redirigé vers la page de détails du produit.
3. Sur la page des détails du produit, développez l'onglet Versions, puis choisissez Créer une nouvelle version.
4. Sous Détails de la version, effectuez les opérations suivantes :

   - Choisir un modèle — Il existe quatre méthodes pour ajouter un fichier modèle.

Utiliser un fichier modèle local - Téléchargez un AWS CloudFormation modèle ou un fichier de configuration Terraform tar.gz à partir d'un lecteur local.

Utiliser une URL Amazon S3 : spécifiez une URL qui pointe vers un AWS CloudFormation modèle ou un fichier de configuration Terraform tar.gz stocké dans Amazon S3. Si vous spécifiez une URL Amazon S3, elle doit commencer par https ://.

Utiliser un référentiel externe : spécifiez votre référentiel de code GitHub, GitHub Enterprise ou Bitbucket. AWS Service Catalogvous permet de synchroniser des produits avec des fichiers modèles. Pour les produits Terraform, le format de fichier modèle doit être un seul fichier archivé dans Tar et compressé dans Gzip.

Utiliser une CloudFormation pile existante : entrez l'ARN d'une CloudFormation pile existante. Cette méthode ne prend pas en charge les produits Terraform Cloud ou externes.

- Titre de la version : nom de la version du produit (par exemple, « v1 », « v2beta »). Les espaces ne sont pas autorisés.
- Description (facultatif) — Description de la version du produit, indiquant en quoi cette version diffère de la version précédente.

5. Choisissez Créer une version du produit.

Vous pouvez également l'utiliser CodePipeline pour créer et configurer un pipeline dans lequel déployer votre modèle de AWS Service Catalog produit et transférer vos modifications dans votre référentiel source. Pour plus d'informations, consultez Didacticiel : Création d'un pipeline qui se déploie dans AWS Service Catalog.

Synchronisation de produits avec des modèles de fichiers provenant GitHub d' GitHub Enterprise ou de Bitbucket

AWS Service Catalog vous permet de synchroniser les produits avec des fichiers modèles gérés par le biais d'un fournisseur de référentiel externe. AWS Service Catalog désigne les produits dotés de ce type de connexion au modèle en tant que produits synchronisés avec Git. Les options de référentiel incluent GitHub GitHub Enterprise ou Bitbucket. Une fois que vous vous êtes autorisé Compte AWS avec un compte de référentiel externe, vous pouvez créer de nouveaux AWS Service Catalog produits ou mettre à jour des produits existants pour les synchroniser avec un fichier modèle du référentiel. Lorsque des modifications sont apportées au fichier modèle et validées dans le référentiel

(par exemple, à l'aide de git-push), les modifications sont AWS Service Catalog automatiquement détectées et une nouvelle version du produit (artefact) est créée.

Rubriques

Autorisations requises pour synchroniser les produits avec des fichiers modèles externes

Vous pouvez utiliser la politique AWS Identity and Access Management (IAM) suivante comme modèle pour permettre aux AWS Service Catalog administrateurs de synchroniser des produits avec des fichiers modèles provenant d'un référentiel externe. Cette politique inclut les autorisations requises de la part de CodeConnections et AWS Service Catalog. AWS Service Catalog vous recommande de copier le modèle de politique ci-dessous et d'utiliser également la politique AWS Service Catalog`AWSServiceCatalogAdminFullAccess` gérée lors de l'activation de produits synchronisés avec le référentiel.

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

Création d'une connexion à un compte

Avant de synchroniser un fichier modèle avec un AWS Service Catalog produit, vous devez créer et autoriser une account-to-account connexion unique. Vous utilisez cette connexion pour spécifier les détails du référentiel contenant le fichier modèle souhaité. Vous pouvez créer une connexion à l'aide de la AWS Service Catalog CodeConnections console, de la console AWS Command Line Interface (CLI) ou CodeConnections des API.

Après avoir établi une connexion, vous pouvez utiliser la AWS Service Catalog console, l' AWS Service Catalog API ou la CLI pour créer un AWS Service Catalog produit synchronisé. AWS Service Catalog les administrateurs peuvent créer de nouveaux produits ou mettre à jour AWS Service Catalog des produits existants sur la base d'un fichier modèle dans un référentiel ou une branche. Si une modification est validée dans le référentiel, la détecte AWS Service Catalog automatiquement et crée une nouvelle version du produit. Les versions précédentes du produit sont maintenues jusqu'à la limite de versions prescrite et sont considérées comme obsolètes.

En outre, crée AWS Service Catalog automatiquement un rôle lié à un service (SLR) une fois la connexion créée. Ce SLR permet AWS Service Catalog de détecter toute modification de fichier modèle validée dans le référentiel. Le SLR permet également de AWS Service Catalog créer

automatiquement de nouvelles versions de produits pour les produits synchronisés. Pour plus d'informations sur les autorisations et les fonctionnalités du SLR, reportez-vous à la section Rôles liés à un service pour. AWS Service Catalog

Pour créer un nouveau produit synchronisé avec Git

1. Dans le panneau de navigation de gauche, choisissez Liste des produits, puis sélectionnez Créer un produit.
2. Entrez les détails du produit.
3. Dans Détails de la version, choisissez Spécifiez votre référentiel de code à l'aide d'un AWS CodeStar fournisseur, puis choisissez le lien Créer une nouvelle AWS CodeStar connexion.
4. Après avoir créé la connexion, actualisez la liste des connexions, puis sélectionnez la nouvelle connexion. Spécifiez les détails du référentiel, notamment le chemin du référentiel, de la branche et du fichier modèle.

   Pour plus d'informations sur l'utilisation d'un fichier de configuration Terraform, consultez. Synchronisation des produits Terraform avec des modèles de fichiers depuis GitHub Enterprise GitHub ou Bitbucket

   a. (Facultatif lors de la création d'une nouvelle ressource de AWS Service Catalog produit) Dans la section Support Details, ajoutez des métadonnées pour le produit.
   b. (Facultatif lors de la création d'une nouvelle ressource de AWS Service Catalog produit) Dans la section Balises, choisissez Ajouter une nouvelle balise et entrez les paires clé et valeur.
5. Choisissez Créer un nouveau produit.

Pour créer plusieurs produits synchronisés avec Git

1. Dans le panneau de navigation de gauche de la AWS Service Catalog console, choisissez Liste des produits, puis sélectionnez Créer plusieurs produits gérés par git.
2. Entrez les détails courants du produit.
3. Dans Détails du référentiel externe, sélectionnez une AWS CodeStar connexion, puis spécifiez le référentiel et la branche.
4. Dans le volet Ajouter des produits, entrez le chemin du fichier modèle et le nom du produit. Choisissez Ajouter un nouvel article et continuez à ajouter des produits comme vous le souhaitez.

5. Après avoir ajouté tous les produits souhaités, choisissez Créer des produits en bloc.

Pour connecter un AWS Service Catalog produit existant à un référentiel externe

1. Dans le panneau de navigation de gauche de la AWS Service Catalog console, sélectionnez Liste des produits, puis sélectionnez Connecter les produits à un référentiel externe.
2. Sur la page Sélectionner des produits, sélectionnez les produits que vous souhaitez connecter à un référentiel externe, puis choisissez Suivant.
3. Sur la page Spécifier les détails de la source, sélectionnez une AWS CodeStar connexion existante, puis spécifiez le référentiel, la branche et le chemin du fichier modèle.
4. Choisissez Suivant.
5. Sur la page Vérifier et envoyer, vérifiez les détails de connexion, puis choisissez Connect products to an external repository.

Affichage des connexions de produits synchronisées avec Git

Vous pouvez utiliser la AWS Service Catalog console, l'API ou AWS CLI pour afficher les détails de connexion au référentiel. Pour les AWS Service Catalog produits liés à un fichier modèle, vous pouvez récupérer les informations relatives à la connexion au référentiel et à la dernière synchronisation du modèle avec le produit à partir de l'état de la dernière synchronisation.

> **Note**
>
> Vous pouvez consulter les informations du référentiel et le statut de la dernière synchronisation au niveau du produit. Les utilisateurs doivent disposer d'autorisations IAM dans les CodeConnections API pour consulter les détails du référentiel. Reportez-vous à la section Autorisations requises pour synchroniser les AWS Service Catalog produits avec les fichiers modèles pour plus d'informations sur la politique requise pour ces autorisations IAM.

Pour afficher les détails de la connexion et du référentiel à l'aide de AWS Management Console

1. Dans le panneau de navigation de gauche, sélectionnez Liste des produits.
2. Sélectionnez le produit dans la liste.
3. Sur la page Produit, accédez à la section Informations sur la source du produit.

4. Pour afficher l'ID de révision source d'une version du produit, cliquez sur le lien Dernière version créée. La section Détails de la version affiche l'ID de révision de la source.

Pour afficher les détails de la connexion et du référentiel à l'aide de AWS CLI

À partir de AWS CLI, exécutez les commandes suivantes :

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

$ aws servicecatalog describe-provisioning-artifact

$ aws servicecatalog search-product-as-admin

$ aws servicecatalog list-provisioning-artifacts
```

Mise à jour des connexions aux produits synchronisées avec Git

Vous pouvez mettre à jour les connexions de compte existantes et les produits synchronisés avec Git à l'aide de la AWS Service Catalog console, de l' AWS Service Catalog API ou. AWS CLI

Pour savoir comment connecter un AWS Service Catalog produit existant à un fichier modèle, reportez-vous à la section Création de nouvelles connexions de produits synchronisées avec Git.

Pour mettre à jour les produits existants vers des produits synchronisés avec Git

1. Dans le panneau de navigation de gauche, choisissez Liste des produits, puis choisissez l'une des options suivantes :
   - Pour mettre à jour un seul produit, sélectionnez le produit, accédez à la section Détails de la source du produit, puis choisissez Modifier les détails.
   - Pour mettre à jour plusieurs produits, choisissez Connect products to a external repository, sélectionnez jusqu'à dix produits, puis cliquez sur Next.
2. Dans la section Informations sur la source du produit, effectuez les mises à jour suivantes :
   - Spécifiez la connexion.
   - Spécifiez le référentiel.
   - Spécifiez la branche.
   - Nommez le fichier modèle.
3. Sélectionnez Enregistrer les modifications.

> **Note**
>
> Pour les produits qui ne sont pas encore connectés à un référentiel externe, vous pouvez utiliser l'option Connect to an external repository affichée dans l'alerte en haut de la page d'informations du produit après avoir sélectionné le produit.

Vous pouvez également utiliser la AWS Service Catalog console ou AWS CLI

- Connect un AWS Service Catalog produit existant à un fichier modèle dans un référentiel externe
- Mettez à jour les métadonnées du produit, notamment le nom, la description et les balises du produit.
- Reconfigurez (mettez à jour la synchronisation pour utiliser une autre source de référentiel) une connexion pour un AWS Service Catalog produit précédemment connecté.

Pour mettre à jour les informations de connexion et de référentiel à l'aide de AWS Service Catalog la console

1. Dans le panneau de navigation de gauche de la AWS Service Catalog console, choisissez Liste des produits, puis sélectionnez un produit actuellement connecté à un référentiel externe.
2. Dans la section Détails de la source du produit, choisissez Modifier la source du produit.
3. Dans la section Détails de la source du produit, spécifiez le nouveau référentiel souhaité.
4. Sélectionnez Enregistrer les modifications.

Pour mettre à jour les informations de connexion et de référentiel à l'aide de AWS CLI

À partir des `$ aws servicecatalog update-provisioning-artifact` commandes AWS CLI Exécuter `$ aws servicecatalog update-product` et.

Suppression des connexions de produits synchronisées avec Git

Vous pouvez supprimer une connexion entre un AWS Service Catalog produit et un fichier modèle à l'aide de la AWS Service Catalog console, de CodeConnections l'API ou AWS CLI. Lorsque vous déconnectez un produit d'un fichier modèle, le AWS Service Catalog produit synchronisé passe à un produit géré régulièrement. Après avoir déconnecté le produit, si le fichier modèle est modifié et validé dans le référentiel précédemment connecté, les modifications ne sont pas reflétées. Pour reconnecter un AWS Service Catalog produit à un fichier modèle dans un référentiel externe,

reportez-vous à la section Mise à jour des connexions et des produits synchronisés AWS Service Catalog.

Pour déconnecter un produit synchronisé avec Git à l'aide de la console AWS Service Catalog

1. Dans le AWS Management Console, choisissez Liste des produits dans le panneau de navigation de gauche.
2. Sélectionnez un produit dans la liste.
3. Sur la page Produit, accédez à la section Informations sur la source du produit.
4. Choisissez Déconnecter.
5. Confirmez l'action, puis choisissez Déconnecter.

Pour déconnecter un produit synchronisé avec Git à l'aide de AWS CLI

À partir du AWS CLI, exécutez la `$ aws servicecatalog update-product` commande. Dans l'`ConnectionParameters`entrée, supprimez la connexion spécifiée.

Pour supprimer une connexion à l'aide de l' CodeConnections API ou AWS CLI

Dans l' CodeConnections API ou AWS CLI exécutez la `$ aws codestar-connections delete-connection` commande.

Synchronisation des produits Terraform avec des modèles de fichiers depuis GitHub Enterprise GitHub ou Bitbucket

Lors de la création d'un produit synchronisé avec Git à l'aide d'un fichier de configuration Terraform, le chemin du fichier accepte uniquement le format tar.gz. Les formats de dossiers Terraform ne sont pas acceptés dans le chemin du fichier.

Région AWS support pour les produits synchronisés avec Git

AWS Service Catalog prend en charge les produits synchronisés avec Git Régions AWS comme indiqué dans le tableau ci-dessous.

Région AWS nom	Région AWS identité	Support pour les produits synchronisés avec Git
US East (Virginie du Nord)	us-east-1	Oui

Région AWS nom	Région AWS identité	Support pour les produits synchronisés avec Git
USA Est (Ohio)	us-east-2	Oui
USA Ouest (Californie du Nord)	us-west-1	Oui
USA Ouest (Oregon)	us-west-2	Oui
Afrique (Le Cap)	af-south-1	Non
Asie-Pacifique (Hong Kong)	ap-east-1	Non
Asie-Pacifique (Jakarta)	ap-southeast-3	Non
Asie-Pacifique (Mumbai)	ap-south-1	Oui
Asie-Pacifique (Osaka)	ap-northeast-3	Non
Asie-Pacifique (Séoul)	ap-northeast-2	Oui
Asie-Pacifique (Singapour)	ap-southeast-1	Oui
Asie-Pacifique (Sydney)	ap-southeast-2	Oui
Asie-Pacifique (Tokyo)	ap-northeast-1	Oui
Canada (Centre)	ca-central-1	Oui
Europe (Francfort)	eu-central-1	Oui
Europe (Irlande)	eu-west-1	Oui
Europe (Londres)	eu-west-2	Oui
Europe (Milan)	eu-south-1	Non
Europe (Paris)	eu-west-3	Oui
Europe (Stockholm)	eu-north-1	Oui
Moyen-Orient (Bahreïn)	me-south-1	Non

Région AWS nom	Région AWS identité	Support pour les produits synchronisés avec Git
Amérique du Sud (São Paulo)	sa-east-1	Oui
AWS GovCloud (USA Est)	us-gov-east-1	Non
AWS GovCloud (US-Ouest)	us-gov-west-1	Non

Supprimer des produits

Lorsque vous supprimez un produit, AWS Service Catalog toutes les versions du produit sont supprimées de chaque portefeuille contenant le produit.

AWS Service Catalogvous permet de supprimer un produit à l'aide de la AWS Service Catalog console ouAWS CLI. Pour réussir à supprimer un produit, vous devez d'abord dissocier toutes les ressources associées au produit. Les associations de ressources entre produits et ressources incluent les associations de portefeuilles TagOptions, les budgets et les actions de service.

> **Important**
>
> Vous ne pouvez pas récupérer un produit une fois qu'il a été supprimé.

Pour supprimer un produit à l'aide de la AWS Service Catalog console

1. Accédez à la page Portefeuilles et sélectionnez le portefeuille contenant le produit que vous souhaitez supprimer.
2. Sélectionnez le produit que vous souhaitez supprimer, puis choisissez Supprimer dans le coin supérieur droit du volet du produit.
3. Pour les produits sans ressources associées, confirmez le produit que vous souhaitez supprimer en saisissant Supprimer dans la zone de texte, puis en choisissant Supprimer.

   Pour les produits associés aux ressources, passez à l'étape 4.
4. Dans la fenêtre Supprimer le produit, consultez le tableau des associations, qui affiche toutes les ressources associées au produit. AWS Service Catalogtente de dissocier ces ressources lorsque vous supprimez le produit.

5. Confirmez que vous souhaitez supprimer le produit et toutes les ressources associées en saisissant Supprimer dans la zone de texte.
6. Choisissez Dissocier et supprimer.

S'il n'AWS Service Catalogest pas possible de dissocier toutes les ressources du produit, celui-ci n'est pas supprimé. La fenêtre Supprimer le produit affiche le nombre de dissociations ayant échoué et une description de chaque échec. Pour plus d'informations sur la résolution des dissociations de ressources ayant échoué lors de la suppression d'un produit, voir Résolution des dissociations de ressources ayant échoué lors de la suppression d'un produit ci-dessous.

Rubriques

- Suppression de produits à l'aide du AWS CLI
- Résolution des dissociations de ressources échouées lors de la suppression d'un produit

Suppression de produits à l'aide du AWS CLI

AWS Service Catalogvous permet d'utiliser le AWS Command Line Interface(AWS CLI) pour supprimer des produits de votre portefeuille. L'AWS CLI est un outil à code source libre qui vous permet d'interagir avec les services AWS à l'aide des commandes du shell de ligne de commande. La fonction AWS Service Catalog force-delete nécessite un AWS CLIalias, c'est-à-dire un raccourci que vous pouvez créer dans le AWS CLI pour raccourcir les commandes ou les scripts que vous utilisez fréquemment.

Prérequis

- Installation et configuration de l'AWS CLI. Pour plus d'informations, consultez la section Installation ou mise à jour de la dernière version des principes de base de la configuration AWS CLI et de la configuration. Utilisez une AWS CLI version minimale de 1.11.24 ou 2.0.0.
- L'alias CLI de suppression du produit nécessite un terminal compatible avec bash et le processeur JSON de ligne de commande JQ. Pour plus d'informations sur l'installation du processeur JSON en ligne de commande, consultez Download jq.
- Créez un AWS CLI alias pour les appels d'`Disassociation`API par lots, ce qui vous permet de supprimer un produit en une seule commande.

Pour réussir à supprimer un produit, vous devez d'abord dissocier toutes les ressources associées au produit. Parmi les exemples d'associations de ressources de produits, citons les associations

de portefeuilles, les budgets, les options de balise et les actions de service. Lorsque vous utilisez la CLI pour supprimer un produit, l'`force-delete-product`alias de la CLI vous permet d'appeler l'`Disassociate`API pour dissocier toutes les ressources susceptibles d'empêcher l'`DeleteProduct`API. Cela permet d'éviter un appel distinct à des dissociations individuelles.

> **Note**
>
> Les chemins de fichiers indiqués dans les procédures ci-dessous peuvent varier en fonction du système d'exploitation que vous utilisez pour effectuer ces actions.

Création d'un AWS CLI alias pour supprimer AWS Service Catalog des produits

Lorsque vous utilisez le AWS CLI pour supprimer un AWS Service Catalog produit, l'`force-delete-product`alias CLI vous permet d'appeler l'`Disassociate`API pour dissocier toutes les ressources susceptibles d'empêcher l'`DeleteProduct`appel.

Créez un **`alias`** fichier dans votre dossier AWS CLI de configuration

1. Dans la AWS CLI console, accédez au dossier de configuration. Par défaut, le chemin du dossier de configuration est `~/.aws/` sous Linux et macOS, ou `%USERPROFILE%\.aws\` sous Windows.
2. Créez un sous-dossier nommé à `cli` l'aide de la navigation dans les fichiers ou en saisissant la commande suivante dans votre terminal préféré :

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

   Le chemin par défaut du `cli` dossier obtenu est `~/.aws/cli/` sous Linux et macOS, ou `%USERPROFILE%\.aws\cli` sous Windows.
3. Dans le nouveau `cli` dossier, créez un fichier texte nommé `alias` sans extension de fichier. Vous pouvez créer le `alias` fichier à l'aide de la navigation dans les fichiers ou en saisissant la commande suivante dans le terminal de votre choix :

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

4. Entrez `[toplevel]` sur la première ligne.
5. Enregistrez le fichier.

Vous pouvez ensuite ajouter l' force-delete-product alias à votre `alias` fichier en collant manuellement le script d'alias dans le fichier ou en utilisant une commande dans la fenêtre du terminal.

Ajoutez manuellement l' force-delete-product alias à votre **`alias`** fichier

1. Dans la AWS CLI console, accédez à votre dossier AWS CLI de configuration et ouvrez le `alias` fichier.
2. Entrez l'alias de code suivant dans le fichier, sous la `[toplevel]` ligne :

```
            [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. Enregistrez le fichier.

Utilisez la fenêtre du terminal pour ajouter l' force-delete-product alias à votre **`alias`** fichier

1. Ouvrez la fenêtre de votre terminal et exécutez la commande suivante

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

2. Collez le script d'alias dans la fenêtre du terminal, puis appuyez sur CTRL+D pour quitter la `cat` commande.

Appelez l' force-delete-product alias

1. Dans la fenêtre de votre terminal, exécutez la commande suivante pour appeler l'alias de produit de suppression

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

   L'exemple ci-dessous montre la commande `force-delete-product` alias et la réponse qui en résulte

   ```
   $ 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. Entrez y pour confirmer que vous souhaitez supprimer le produit.

Une fois le produit supprimé avec succès, la fenêtre du terminal affiche les résultats suivants

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

Ressources supplémentaires

Pour plus d'informations sur AWS CLI l'utilisation d'alias et la suppression de AWS Service Catalog produits, consultez les ressources suivantes :

- Création et utilisation d'AWS CLIalias dans le guide de l'utilisateur AWS Command Line Interface(CLI).
- AWS CLIdépôt d'alias dépôt git.
- Supprimer AWS Service Catalog des produits.
- AWSre:Invent 2016 : L'AWS CLIutilisateur efficace sur. YouTube

Résolution des dissociations de ressources échouées lors de la suppression d'un produit

Si votre précédente tentative de suppression d'un produit a échoué en raison d'exceptions liées à la dissociation des ressources, consultez la liste des exceptions et leurs solutions ci-dessous.

> **Note**
>
> Si vous avez fermé la fenêtre Supprimer des produits avant de recevoir le message d'échec de la dissociation des ressources, vous pouvez suivre les étapes 1 à 3 de la section Supprimer un produit pour ouvrir à nouveau la fenêtre.

Pour résoudre un échec de dissociation des ressources

Dans la fenêtre Supprimer le produit, consultez la colonne État du tableau des associations. Identifiez l'exception de dissociation des ressources qui a échoué et les solutions suggérées :

Type d'exception de statut	Cause	Résolution
Produit prod-****	AWS Service CatalogIm possible de supprimer le produit car le produit est toujours associé à des budgets TagOptions, dont au moins un `ProvisioningArtifact` avec des actions associées, le produit est toujours affecté à un portefeuille, le produit a des utilisateurs ou le produit est soumis à des contraintes.	Essayez à nouveau de supprimer le produit.
Utilisateur : n'`username`est pas autorisé à effectuer :	L'utilisateur qui tente de supprimer le produit ne dispose pas des autorisations nécessaires pour dissocier les ressources du produit.	AWS Service Catalogre commande de contacter l'administrateur de votre compte pour plus d'informations sur la dissociation des ressources de produits que vous n'êtes pas actuellement autorisé à dissocier.

Gestion des versions

Vous attribuez les versions de produit lorsque vous créez un produit, et vous pouvez les mettre à jour à tout moment.

Les versions ont un modèle AWS CloudFormation, un titre, une description, un état et un guide de version.

État de la version

Une version peut avoir l'un des trois états suivants :

- Active - Une version active apparaît dans la liste des versions et permet aux utilisateurs de la lancer.
- Inactive - Une version inactive est masquée dans la liste des versions. Les produits provisionnés existants lancés à partir de cette version ne seront pas affectés.
- Supprimé : une version supprimée est supprimée de la liste des versions. La suppression d'une version ne peut pas être annulée.

Guide de version

Vous pouvez définir un guide de version pour fournir des informations aux utilisateurs finaux sur la version du produit. Le guide de version ne concerne que les versions actives du produit.

Il existe deux options pour le guide de version :

- Aucune : par défaut, les versions du produit ne contiennent aucun guide. Les utilisateurs finaux peuvent utiliser cette version pour mettre à jour et lancer les produits provisionnés.
- Obsolète : les utilisateurs ne peuvent pas lancer de nouveaux produits provisionnés à l'aide d'une version de produit obsolète. Si un produit provisionné p lancé précédemment utilise une version désormais obsolète, les utilisateurs peuvent uniquement mettre à jour ce produit provisionné en utilisant la version existante ou une nouvelle version.

Mise à jour des versions

Vous attribuez les versions de produit lorsque vous créez un produit, et vous pouvez aussi les mettre à jour à tout moment. Pour plus d'informations sur la création d'un produit, consultez Création de produits.

Pour mettre à jour une version de produit

1. Dans la console AWS Service Catalog, choisissez Products (Produits).
2. Dans la liste des produits, choisissez le produit dont vous souhaitez mettre à jour la version.
3. Sur la page Product details (Détails du produit), choisissez l'onglet Versions, puis choisissez la version à mettre à jour.

4. Sur la page Version details (Détails de la version), modifiez la version du produit, puis choisissez Save changes (Enregistrer les modifications).

Utilisation de contraintes AWS Service Catalog

Vous appliquez des contraintes pour contrôler les règles appliquées à un produit dans un portefeuille spécifique lorsque les utilisateurs finaux le lancent. Lorsque les utilisateurs finaux lancent le produit, ils voient les règles que vous avez appliquées à l'aide de contraintes. Vous pouvez appliquer des contraintes à un produit une fois que celui-ci est placé dans un portefeuille. Les contraintes sont actives dès que vous les créez. Elles sont appliquées à toutes les versions actuelles d'un produit qui n'ont pas été lancées.

Constraints

- Contraintes de lancement AWS Service Catalog
- Contraintes de notification AWS Service Catalog
- Contraintes de mise à jour des balises AWS Service Catalog
- Contraintes d'ensemble de piles AWS Service Catalog
- Contraintes de modèle AWS Service Catalog

Contraintes de lancement AWS Service Catalog

Une contrainte de lancement spécifie le rôle AWS Identity and Access Management (IAM) AWS Service Catalog assumé lorsqu'un utilisateur final lance, met à jour ou met fin à un produit. Un rôle IAM est un ensemble d'autorisations qu'un utilisateur ou un AWS service peut assumer temporairement pour utiliser les AWS services. Pour un exemple d'introduction, voir :

- AWS CloudFormationtype de produit : Étape 6 : ajouter une contrainte de lancement pour attribuer un rôle IAM
- Type de produit Terraform Open Source ou Terraform Cloud : Étape 5 : créer des rôles de lancement

Les contraintes de lancement s'appliquent aux produits du portefeuille (association produit-portefeuille). Les contraintes de lancement ne s'appliquent pas au niveau du portefeuille ou à un produit de tous les portefeuilles. Pour associer une contrainte de lancement à tous les produits

d'un portefeuille, vous devez appliquer la contrainte de lancement à chaque produit, de manière individuelle.

Sans contrainte de lancement, les utilisateurs finaux doivent lancer et gérer les produits à l'aide de leurs propres informations d'identification IAM. Pour ce faire, ils doivent disposer d'autorisations pour AWS CloudFormation les AWS services utilisés par les produits, etAWS Service Catalog. En utilisant un rôle de lancement, vous pouvez plutôt limiter les autorisations des utilisateurs finaux au minimum dont ils ont besoin pour ce produit. Pour plus d'informations sur les autorisations des utilisateurs finaux, consultez Identity and Access Management dans AWS Service Catalog.

Pour créer et attribuer des rôles IAM, vous devez disposer des autorisations administratives IAM suivantes :

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

Configuration d'un rôle de lancement

Le rôle IAM que vous attribuez à un produit en tant que contrainte de lancement doit être autorisé à utiliser les éléments suivants :

Pour les produits Cloudformation

- La politique `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess` AWS CloudFormation gérée
- Services dans le AWS CloudFormation modèle du produit
- Accès en lecture au AWS CloudFormation modèle dans un compartiment Amazon S3 appartenant au service.

Pour les produits Terraform

- Services du modèle Amazon S3 pour le produit
- Accès en lecture au modèle Amazon S3 dans un compartiment Amazon S3 appartenant au service.

- `resource-groups:Tag`pour le balisage dans une instance Amazon EC2 (pris en charge par le moteur de provisionnement Terraform lors des opérations de provisionnement)
- `resource-groups:CreateGroup`pour le balisage des groupes de ressources (supposé par AWS Service Catalog créer des groupes de ressources et attribuer des balises)

La politique de confiance du rôle IAM doit permettre AWS Service Catalog d'assumer le rôle. Dans la procédure ci-dessous, la politique de confiance sera définie automatiquement lorsque vous sélectionnez AWS Service Catalog le type de rôle. Si vous n'utilisez pas la console, consultez la section Création de politiques de confiance pour les AWS services qui assument des rôles dans Comment utiliser les politiques de confiance avec les rôles IAM.

> **Note**
>
> Les autorisations `servicecatalog:ProvisionProduct`, `servicecatalog:TerminateProvisionedProduct` et `servicecatalog:UpdateProvisionedProduct` ne peuvent pas être attribuées à un rôle de lancement. Vous devez utiliser des rôles IAM, comme indiqué dans les étapes de politique intégrées dans la section Accorder des autorisations aux utilisateurs AWS Service Catalog finaux.

> **Note**
>
> Pour consulter les produits et ressources Cloudformation fournis dans la AWS Service Catalog console, les utilisateurs finaux ont besoin d'un accès en AWS CloudFormation lecture. L'affichage des produits et ressources provisionnés dans la console n'utilise pas le rôle de lancement.

Pour créer un rôle de lancement

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.

   Les produits Terraform nécessitent des configurations de rôles de lancement supplémentaires. Pour plus d'informations, consultez Étape 5 : Création de rôles de lancement dans Getting Started with a Terraform Open Source product.
2. Sélectionnez Roles (Rôles).

3. Choisissez Create New Role (Créer un nouveau rôle).
4. Entrez un nom de rôle, puis choisissez Next Step.
5. Sous Rôles de AWS service à côté de AWS Service Catalog, choisissez Sélectionner.
6. Sur la page Attach Policy, choisissez Next Step.
7. Pour créer le rôle, choisissez Create Role.

Pour attacher une stratégie au nouveau rôle

1. Choisissez le rôle que vous avez créé pour afficher la page des détails du rôle.
2. Choisissez l'onglet Permissions et développez la section Inline Policies. Puis, choisissez click here.
3. Choisissez Custom Policy, puis Select.
4. Entrez un nom pour la stratégie et collez ce qui suit dans l'éditeur Policy Document :

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

> **Note**
>
> Lorsque vous configurez un rôle de lancement pour une contrainte de lancement, vous devez utiliser cette chaîne :`"s3:ExistingObjectTag/servicecatalog:provisioning":"true"`.

5. Ajoutez une ligne à la politique pour chaque service supplémentaire utilisé par le produit. Par exemple, pour ajouter une autorisation pour Amazon Relational Database Service (Amazon RDS), entrez une virgule à la fin de la dernière ligne de `Action` la liste, puis ajoutez la ligne suivante :

   ```
   "rds:*"
   ```

6. Choisissez Apply Policy (Appliquer la stratégie).

Application d'une contrainte de lancement

Après avoir configuré le rôle de lancement, attribuez-le au produit en tant que contrainte de lancement. Cette action indique AWS Service Catalog d'assumer le rôle lorsqu'un utilisateur final lance le produit.

Pour attribuer le rôle à un produit

1. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Choisissez le portefeuille qui contient le produit.
3. Cliquez sur l'onglet Constraints (Contraintes) puis sur Create constraint (Créer une contrainte).
4. Choisissez le produit dans Product (Produit), puis Launch (Lancement) sous Constraint type (Type de contrainte). Choisissez Continuer.
5. Dans la section Contrainte de lancement, vous pouvez sélectionner un rôle IAM dans votre compte et saisir un ARN de rôle IAM, ou saisir le nom du rôle.

   Si vous spécifiez le nom du rôle et si un compte utilise la contrainte de lancement, le compte utilise ce nom pour le rôle IAM. Cette approche permet aux contraintes relatives aux rôles de lancement d'être indépendantes du compte, ce qui vous permet de créer moins de ressources par compte partagé.

   > **Note**
   >
   > Le nom de rôle indiqué doit exister dans le compte qui a créé la contrainte de lancement et dans le compte de l'utilisateur qui lance un produit avec cette contrainte de lancement.

6. Après avoir spécifié le rôle IAM, choisissez Create (Créer).

Ajouter un adjoint confus à la contrainte de lancement

AWS Service Catalogprend en charge la protection Confused Deputy pour les API qui s'exécutent avec une demande Assume Role. Lorsque vous ajoutez une contrainte de lancement, vous pouvez restreindre l'accès au rôle de lancement en utilisant `sourceArn` les conditions `sourceAccount` et la politique de confiance du rôle de lancement. Cela garantit que le rôle de lancement est appelé par une source fiable.

Dans l'exemple suivant, l'AWS Service Catalogutilisateur final appartient au compte 111111111111. Lorsque l'AWS Service Catalogadministrateur crée un rôle `LaunchConstraint` pour un produit, l'utilisateur final peut spécifier les conditions suivantes dans la politique de confiance du rôle de lancement afin de restreindre le rôle d'assumer le rôle au compte 111111111111.

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

}
```

Un utilisateur qui approvisionne un produit avec le `LaunchConstraint` doit avoir le même `AccountId` (1111111111). Dans le cas contraire, l'opération échoue avec une `AccessDenied` erreur, empêchant ainsi toute utilisation abusive du rôle de lancement.

Les AWS Service Catalog API suivantes sont sécurisées pour la protection de Confused Deputy :

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

La `sourceArn` protection pour AWS Service Catalog ne prend en charge que les ARN modèles, tels que « `arn:<aws-partition>:servicecatalog:<region>:<accountId>:` ». Elle ne prend pas en charge les ARN de ressources spécifiques.

Vérification de la contrainte de lancement

Pour vérifier qu'il AWS Service Catalog utilise le rôle pour lancer le produit et qu'il approvisionne correctement le produit, lancez le produit depuis la AWS Service Catalog console. Pour tester une contrainte avant sa publication pour des utilisateurs, créez un portefeuille test qui contient les mêmes produits et testez les contraintes avec ce portefeuille.

Pour lancer le produit

1. Dans le menu de la AWS Service Catalog console, choisissez Service Catalog, End user.
2. Choisissez le produit pour ouvrir la page de détails du produit. Dans le tableau des options de lancement, vérifiez que le nom de ressource Amazon (ARN) du rôle apparaît.
3. Choisissez Launch product.
4. Poursuivez les étapes de lancement en indiquant les informations requises.
5. Vérifiez que le produit démarre correctement.

Contraintes de notification AWS Service Catalog

> **Note**
>
> AWS Service Catalogne prend pas en charge les contraintes de notification pour les produits Terraform Open Source ou Terraform Cloud.

Une contrainte de notification spécifie une rubrique Amazon SNS pour recevoir des notifications concernant les événements liés à la pile.

Utilisez la procédure suivante pour créer une rubrique SNS et vous y abonner.

Pour créer une rubrique SNS et un abonnement

1. Ouvrez la console Amazon SNS à partir de l'adresse https://console.aws.amazon.com/sns/v3/home.
2. Choisissez Créer une rubrique.

3. Saisissez un nom de rubrique puis choisissez Create topic.
4. Choisissez Créer un abonnement.
5. Pour Protocol, sélectionnez Email. Pour Endpoint, saisissez une adresse e-mail que vous pouvez utiliser pour recevoir les notifications. Choisissez Créer un abonnement.
6. Vous recevrez un e-mail de confirmation avec la ligne d'objet `AWS Notification - Subscription Confirmation`. Ouvrez l'e-mail et suivez les instructions pour terminer votre abonnement.

Utilisez la procédure suivante pour appliquer une contrainte de notification utilisant la rubrique SNS que vous avez créée à l'aide de la procédure précédente.

Pour appliquer une contrainte de notification à un produit

1. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Choisissez le portefeuille qui contient le produit.
3. Développez Contraintes et choisissez Ajouter des contraintes.
4. Choisissez le produit dans Produit et définissez le type de contrainte sur Notification. Choisissez Continuer.
5. Choisissez Choisir une rubrique dans votre compte et sélectionnez la rubrique SNS que vous avez créée dans Nom de la rubrique.
6. Sélectionnez Envoyer.

Contraintes de mise à jour des balises AWS Service Catalog

> **Note**
>
> AWS Service Catalogne prend pas en charge les contraintes de mise à jour des balises pour les produits Open Source Terraform.

Avec les contraintes de mise à jour des balises, AWS Service Catalog les administrateurs peuvent autoriser ou interdire aux utilisateurs finaux de mettre à jour les balises sur les ressources associées à un produit provisionné. Si la mise à jour des balises est autorisée, les nouvelles balises associées au produit ou au portefeuille seront appliquées aux ressources provisionnées lors d'une mise à jour de produit provisionnée.

Pour activer la mise à jour des balises pour un produit

1. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Choisissez le portefeuille qui contient le produit que vous souhaitez mettre à jour.
3. Cliquez sur l'onglet Contraintes, puis sur Ajouter des contraintes.
4. Sous Constraint type (Type de contrainte), choisissez Tag Update (Mise à jour des balises).
5. Choisissez le produit à partir de Product (Produit), puis cliquez sur Continue (Continuer).
6. Sur la page des mises à jour de balises, sélectionnez Enable Tag Updates (Activer les mises à jour des balises).
7. Sélectionnez Envoyer.

Contraintes d'ensemble de piles AWS Service Catalog

> **Note**
>
> - AWS Service Catalogne prend pas en charge les contraintes de stack pour les produits Open Source Terraform.
> - AutoTags ne sont actuellement pas pris en charge avec AWS CloudFormation StackSets.

Une contrainte d'ensemble de piles vous permet de configurer les options de déploiement du produit à l'aide de AWS CloudFormation StackSets. Vous pouvez spécifier plusieurs comptes et régions pour le lancement de produit. Les utilisateurs finaux peuvent gérer ces comptes et déterminer où les produits sont déployés et l'ordre de déploiement.

Pour appliquer une contrainte d'ensemble de piles à un produit

1. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Choisissez le portefeuille contenant le produit que vous souhaitez.
3. Choisissez l'onglet Contraintes, puis sélectionnez Créer des contraintes.
4. Dans Produit, sélectionnez le produit. Dans Type de contrainte, choisissez Stack Set.
5. Configurez les comptes, les régions et les autorisations en fonction des contraintes de votre stack set.

- Dans les paramètres du compte, identifiez les comptes sur lesquels vous souhaitez créer des produits.
- Dans les paramètres régionaux, choisissez les régions géographiques dans lesquelles les produits seront déployés et l'ordre dans lequel vous souhaitez que ces produits soient déployés dans ces régions.
- Dans Autorisations, choisissez un rôle d' StackSetadministrateur IAM pour gérer vos comptes cibles. Si vous ne choisissez aucun rôle, StackSets utilise l'ARN par défaut. En savoir plus sur la configuration d'autorisations d'ensemble de piles.

6. Sélectionnez Create (Créer).

Contraintes de modèle AWS Service Catalog

> **Note**
>
> AWS Service Catalogne prend pas en charge les contraintes de modèle pour les produits Terraform Open Source ou Terraform Cloud.

Pour limiter les options qui sont à disposition des utilisateurs finaux lorsqu'ils lancent un produit, vous appliquez des contraintes de modèle. Appliquez des contraintes de modèle pour vous assurer que les utilisateurs finaux peuvent utiliser des produits sans violer les exigences de conformité de votre organisation. Vous appliquez des contraintes de modèle à un produit d'un AWS Service Catalog portefeuille. Un portefeuille doit contenir un ou plusieurs produits pour que vous puissiez définir des contraintes de modèle.

Une contrainte de modèle se compose d'une ou plusieurs règles qui restreignent les valeurs autorisées pour des paramètres définis dans le modèle AWS CloudFormation sous-jacent du produit. Les paramètres d'un modèle AWS CloudFormation définissent l'ensemble de valeurs que les utilisateurs peuvent spécifier lorsqu'ils créent une pile. Par exemple, un paramètre peut définir les différents types d'instance que les utilisateurs peuvent choisir lors du lancement d'une pile incluant des instances EC2.

Si l'ensemble de valeurs de paramètre dans un modèle est trop large pour le public cible de votre portefeuille, vous pouvez définir des contraintes de modèle pour limiter les valeurs que les utilisateurs peuvent choisir lors du lancement d'un produit. Par exemple, si les paramètres de modèle incluent des types d'instance EC2 qui sont trop volumineux pour des utilisateurs qui doivent utiliser

uniquement des types d'instance de petite taille (par exemple, `t2.micro` ou `t2.small`), vous pouvez ajouter une contrainte de modèle pour limiter les types d'instance que les utilisateurs finaux peuvent choisir. Pour plus d'informations sur les paramètres de modèle AWS CloudFormation, consultez Paramètres dans le Guide de l'utilisateur AWS CloudFormation.

Les contraintes de modèle sont liées au sein d'un portefeuille. Si vous appliquez des contraintes de modèle à un produit dans un portefeuille et si vous ajoutez ensuite le produit à un autre portefeuille, les contraintes ne s'appliquent pas au produit dans le deuxième portefeuille.

Si vous appliquez une contrainte de modèle à un produit qui a déjà été partagé avec des utilisateurs, la contrainte est active immédiatement pour tous les lancements de produit suivants et pour toutes les versions du produit dans le portefeuille.

Vous définissez des règles de contrainte de modèle en utilisant un éditeur de règles ou en écrivant les règles sous forme d'un texte JSON dans la console Administrateur AWS Service Catalog. Pour plus d'informations sur les règles, y compris la syntaxe et des exemples, consultez Règles de contrainte de modèle.

Pour tester une contrainte avant sa publication pour des utilisateurs, créez un portefeuille test qui contient les mêmes produits et testez les contraintes avec ce portefeuille.

Pour appliquer des contraintes de modèle à un produit

1. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Sur la page Portefeuilles, choisissez le portefeuille contenant le produit auquel vous souhaitez appliquer une contrainte de modèle.
3. Développez la section Contraintes et choisissez Ajouter des contraintes.
4. Dans la fenêtre Sélectionner le produit et le type, dans Produit, sélectionnez le produit pour lequel vous souhaitez définir les contraintes du modèle. Ensuite, pour Type de contrainte, choisissez Modèle. Choisissez Continuer.
5. Sur la page Générateur de contraintes du modèle, modifiez les règles de contrainte à l'aide de l'éditeur JSON ou de l'interface du générateur de règles.

   - Pour modifier le code JSON de la règle, choisissez l'onglet Constraint Text Editor. Plusieurs exemples sont fournis sur cet onglet pour vous aider à démarrer.

     Pour créer les règles à l'aide d'une interface de création de règles, choisissez l'onglet Générateur de règles. Sur cet onglet, vous pouvez choisir n'importe quel paramètre spécifié

dans le modèle pour le produit, ainsi que les valeurs autorisées pour ce paramètre. En fonction du type du paramètre, vous spécifiez les valeurs autorisées en choisissant des éléments dans une liste de contrôle, en spécifiant un nombre ou en indiquant un ensemble de valeurs dans une liste séparée par des virgules.

Lorsque vous avez fini de créer une règle, choisissez Ajouter une règle. La règle apparaît dans le tableau de l'onglet Générateur de règles. Pour consulter et modifier la sortie JSON, choisissez l'onglet Constraint Text Editor.

6. Lorsque vous avez terminé de modifier les règles de votre contrainte, choisissez Soumettre. Pour voir la contrainte, rendez-vous sur la page des détails du portefeuille et développez Contraintes.

Règles de contrainte de modèle

Les règles qui définissent les contraintes du modèle dans un AWS Service Catalog portefeuille décrivent à quel moment les utilisateurs finaux peuvent utiliser le modèle et quelles valeurs ils peuvent spécifier pour les paramètres déclarés dans le AWS CloudFormation modèle utilisé pour créer le produit qu'ils tentent d'utiliser. Les règles sont utiles pour empêcher les utilisateurs finaux de spécifier par inadvertance une valeur incorrecte. Par exemple, vous pouvez ajouter une règle pour vérifier si les utilisateurs finaux ont spécifié un sous-réseau valide dans un VPC donné ou utilisé des types d'instance `m1.small` pour des environnements de test. AWS CloudFormation utilise des règles pour valider des valeurs de paramètre avant de créer les ressources pour le produit.

Chaque règle se compose de deux propriétés : une condition de règle (facultative) et des assertions (obligatoire). La condition de règle détermine si une règle prend effet. Les assertions décrivent les valeurs que les utilisateurs peuvent spécifier pour un paramètre particulier. Si vous ne définissez pas de condition de règle, les assertions de la règle prennent toujours effet. Pour définir une condition de règle et des assertions, vous utilisez des fonctions intrinsèques spécifiques aux règles qui sont des fonctions qui peuvent uniquement être utilisées dans la section `Rules` d'un modèle. Vous pouvez imbriquer des fonctions, mais le résultat final d'une condition de règle ou d'une assertion doit avoir la valeur true (vrai) ou false (faux).

Par exemple, supposons que vous avez déclaré un VPC et un paramètre de sous-réseau dans la section `Parameters`. Vous pouvez créer une règle qui vérifie qu'un sous-réseau donné est dans un VPC particulier. Par conséquent, quand un utilisateur spécifie un VPC, AWS CloudFormation évalue l'assertion pour vérifier si la valeur du paramètre de sous-réseau est dans ce VPC avant de créer ou mettre à jour la pile. Si la valeur du paramètre n'est pas valide, AWS CloudFormation arrête

immédiatement de créer ou mettre à jour la pile. Si des utilisateurs ne spécifient pas de VPC, AWS CloudFormation ne vérifie pas la valeur du paramètre de sous-réseau.

Syntaxe

La section `Rules` d'un modèle se compose du nom de clé `Rules`, suivi d'un seul signe deux points. Toutes les déclarations de règle sont placées entre des accolades. Si vous déclarez plusieurs règles, celles-ci sont séparées par des virgules. Pour chaque règle, vous déclarez un nom logique entre guillemets, suivi d'un signe deux points et d'accolades qui entourent la condition de règle et les assertions.

Une règle peut inclure une propriété `RuleCondition` et doit inclure une propriété `Assertions`. Pour chaque règle, vous ne pouvez définir qu'une seule condition de règle ; vous pouvez définir une ou plusieurs assertions au sein de la propriété `Assertions`. Vous définissez une condition et des assertions de règle à l'aide de fonctions intrinsèques spécifiques aux règles, comme illustré dans le pseudo-modèle suivant :

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

Le pseudo-modèle montre une section `Rules` contenant deux règles nommées `Rule01` et `Rule02`. `Rule01` inclut une condition de règle et deux assertions. Si la fonction dans la condition de règle a la valeur true, les deux fonctions de chaque assertion sont évaluées et appliquées. Si la condition a la valeur false, la règle ne prend pas effet. `Rule02` prend toujours effet, car il n'y a pas de condition de règle, ce qui signifie qu'une assertion est toujours évaluée et appliquée.

Pour plus d'informations sur les fonctions intrinsèques spécifiques aux règles permettant de définir les conditions et les assertions des règles, consultez la section Fonctions des AWS règles dans le guide de l'AWS CloudFormationutilisateur.

Exemple : Vérification conditionnelle d'une valeur de paramètre

Les deux règles suivantes vérifient la valeur du paramètre `InstanceType`. En fonction de la valeur du paramètre d'environnement (`test` ou `prod`), l'utilisateur doit spécifier `m1.small` ou `m1.large` pour le paramètre `InstanceType`. Les paramètres `InstanceType` et `Environment` doivent être déclarés dans la section `Parameters` du même modèle.

```
"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"
```

```
      }
    ]
  }
}
```

Actions de serviceAWS Service Catalog

> **Note**
>
> AWS Service Catalogne prend pas en charge les actions de service pour les produits Terraform Open Source ou Terraform Cloud.

AWS Service Catalog vous permet de réduire la maintenance administrative et la formation des utilisateurs finaux, tout en respectant les mesures de conformité et de sécurité. Grâce aux actions de service, en tant qu'administrateur vous pouvez autoriser les utilisateurs finaux à exécuter des tâches opérationnelles, résoudre des problèmes, exécuter des commandes approuvés ou demander des autorisations dans AWS Service Catalog. Vous utilisez des documents AWS Systems Manager pour définir les actions de service. Les AWS Systems Managerdocuments donnent accès à des actions prédéfinies qui mettent en œuvre les AWS meilleures pratiques, telles que l'arrêt et le redémarrage d'Amazon EC2, et vous pouvez également définir des actions personnalisées.

Dans ce didacticiel, vous permettez aux utilisateurs finaux de redémarrer une instance Amazon EC2. Vous ajoutez les autorisations nécessaires, définissez l'action de service, associez l'action de service à un produit et tester l'expérience de l'utilisateur final à l'aide de l'action avec un produit provisionné.

Prérequis

Ce didacticiel suppose que vous disposez de l'ensemble des autorisations administrateur AWS, que vous connaissez AWS Service Catalog et que vous disposez déjà d'un ensemble de produits, de portefeuilles et d'utilisateurs. Si vous ne connaissez pas AWS Service Catalog, exécutez les tâches Configuration et Démarrage avant d'utiliser ce didacticiel.

Rubriques

- Étape 4 : Tester l'expérience de l'utilisateur final
- Étape 5 : Gestion des actions de service avec AWS CloudFormation
- Étape 6 : Résolution des problèmes

Étape 1 : Configurer les autorisations des utilisateurs finaux

Les utilisateurs finaux doivent disposer des autorisations nécessaires pour consulter et exécuter des actions de service spécifiques. Dans cet exemple, l'utilisateur final doit être autorisé à accéder à la fonctionnalité d'actions de AWS Service Catalog service et à redémarrer Amazon EC2.

Pour mettre à jour les autorisations

1. Ouvrez la console AWS Identity and Access Management (IAM) à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le menu, localisez les groupes d'utilisateurs.
3. Choisissez les groupes que les utilisateurs finaux utiliseront pour accéder aux AWS Service Catalog ressources. Dans cet exemple, nous sélectionnons le groupe de l'utilisateur final. Dans votre propre implémentation, choisissez le groupe utilisé par les utilisateurs finaux pertinents.
4. Dans l'onglet Autorisations de la page de détails de votre groupe, vous créez une nouvelle stratégie ou modifier une existante. Dans cet exemple, nous ajoutons des autorisations à la stratégie existante en sélectionnant la personnalisée créée pour les autorisations de provisionner et de supprimer d'AWS Service Catalog du groupe.
5. Sur la page Stratégie, choisissez Modifier la stratégie pour ajouter les autorisations nécessaires. Vous pouvez utiliser l'éditeur visuel ou JSON pour modifier la stratégie. Dans cet exemple, nous utilisons l'éditeur JSON pour ajouter les autorisations. Pour ce didacticiel, ajoutez les autorisations suivantes à la stratégie :

```
{
 "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. Après avoir modifié la stratégie, examinez et validez les modifications apportées à la stratégie. Les utilisateurs du groupe d'utilisateurs finaux disposent désormais des autorisations nécessaires pour effectuer l'action de redémarrage d'Amazon EC2 dans. AWS Service Catalog

Étape 2 : Créer une action de service

Ensuite, vous créez une action de service pour redémarrer les instances Amazon EC2.

1. Ouvrez la AWS Service Catalog console à l'adresse https://console.aws.amazon.com/sc/.
2. Dans le menu, choisissez Actions du service.
3. Sur la page Actions de service, choisissez Créer une action.
4. Sur la page Action creation (Création d'une action), choisissez un document AWS Systems Manager pour définir l'action de service. L'action de redémarrage de l'instance Amazon EC2 étant définie par un AWS Systems Manager document, nous conservons l'option par défaut dans le menu déroulant, Amazon documents.
5. Recherchez et choisissez l'action AWS-Restartec2Instance.
6. Indiquez un nom et une description pour l'action. Ils doivent être pertinents pour votre environnement et votre équipe. Comme cette description s’adresse à l’utilisateur final, choisissez un nom et une description qui faciliteront sa compréhension de l'action.
7. Sous Configuration du paramètre et de la cible, choisissez le paramètre du document SSM qui sera la cible de l'action (par exemple, l'ID d'instance), puis choisissez la cible du paramètre. Choisissez Ajouter un paramètre pour ajouter des paramètres supplémentaires.
8. Sous Autorisations, choisissez un rôle. Pour cet exemple, nous utilisons les autorisations par défaut. D'autres configurations d'autorisation sont possibles et définies sur cette page.

9. Après avoir vérifié la configuration, choisissez Créer une action.
10. Sur la page suivante, un message de confirmation s'affiche lorsque l'action a été créée et est prête à être utilisée.

Étape 3 : Associer l'action de service à une version de produit

Après avoir défini une action, vous devez associer un produit à cette action.

1. Sur la page Actions de service, choisissez AWS-Restartec2Instance, puis choisissez Associer une action.
2. Sur la page Associate action (Associer une action), choisissez le produit sur lequel vous souhaitez que vos utilisateurs finaux exécutent une action de service. Dans cet exemple, choisissez Bureau Linux.
3. Sélectionnez une version de produit. Remarque : vous pouvez utiliser la case à cocher la plus haute pour sélectionner toutes les versions.
4. Choisissez Action d'association.
5. Sur la page suivante, un message de confirmation s'affiche.

Vous avez désormais créé l'action de service dans AWS Service Catalog. L'étape suivante de ce didacticiel consiste à utiliser l'action du service en tant qu'utilisateur final.

Étape 4 : Tester l'expérience de l'utilisateur final

Les utilisateurs finaux peuvent effectuer des actions de service sur les produits provisionnés. Pour les besoins de ce didacticiel, l'utilisateur final doit posséder au moins un produit provisionné. Le produit provisionné doit être lancé à partir de la version de produit associée à l'action de service de l'étape précédente.

Pour accéder à l'action de service en tant qu'utilisateur final

1. Connectez-vous à la console AWS Service Catalog en tant qu'utilisateur final.
2. Sur le tableau de bord AWS Service Catalog, dans le panneau de navigation, choisissez Liste des produits provisionnés. La liste répertorie les produits provisionnés pour le compte de l'utilisateur final.
3. Sur la page Liste des produits provisionnés, choisissez l'instance provisionnée.

4. Sur la page des détails du produit provisionné, choisissez Actions dans le coin supérieur droit, puis choisissez l'action AWS-Restartec2Instance.
5. Confirmez que vous souhaitez exécuter l'action personnalisée. Vous recevrez une confirmation du lancement de l'action.

Étape 5 : Gestion des actions de service avec AWS CloudFormation

Vous pouvez créer des actions de service et leurs associations avec AWS CloudFormation des ressources. Pour plus d'informations, consultez les rubriques suivantes dans le Guide de l'utilisateur AWS CloudFormation :

- AWS::ServiceCatalog::CloudFormationProduit ProvisioningArtifactProperties
- AWS::ServiceCatalog::ServiceActionAssociation

> **Note**
>
> Si vous gérez des associations d'actions de service avec AWS CloudFormation des ressources, n'ajoutez ni ne supprimez d'actions de service via le AWS Command Line Interface ouAWS Management Console. Lorsque vous effectuez une mise à jour de la pile, toutes les modifications apportées aux actions de service effectuées en dehors de AWS CloudFormation sont remplacées.

Étape 6 : Résolution des problèmes

Si l'exécution de votre action de service échoue, vous trouverez le message d'erreur dans la section Outputs (Sorties) de l'événement d'exécution de l'action de service sur la page Provisioned product (Produit provisionné). Des explications concernant les messages d'erreur courants sont fournies ci-dessous.

> **Note**
>
> Le texte exact du message d'erreur peut changer, il convient donc d'éviter de l'utiliser dans des processus automatisés.

Internal failure (Échec interne)

AWS Service Catalog a rencontré une erreur interne. Réessayez ultérieurement. Si le problème persiste, contactez le support client.

Une erreur s'est produite (ThrottlingException) lors de l'appel de l' StartAutomationExecution opération

L'exécution de l'action de service a été limitée par le service principal, tel que SSM.

Access denied while assuming the role (Accès refusé en assumant le rôle)

AWS Service Catalog n’a pas pu assumer le rôle spécifié dans la définition de l'action de service. Assurez-vous que le principal servicecatalog.amazonaws.com, ou un directeur régional tel que servicecatalog.us-east-1.amazonaws.com, est autorisé dans la politique de confiance du rôle.

Une erreur s'est produite (AccessDeniedException) lors de l'appel de l' StartAutomationExecution opération : L'utilisateur n'est pas autorisé à effectuer : ssm : StartAutomationExecution sur la ressource.

Le rôle spécifié dans la définition de l'action de service n'est pas autorisé à invoquer ssm :StartAutomationExecution. Assurez-vous que le rôle dispose des autorisations SSM appropriées.

Impossible de trouver des ressources dont le type est ***`TargetType`***un produit provisionné

Le produit provisionné ne contient aucune ressource correspondant au type de cible spécifié dans le document SSM, telle que ::EC2 AWS : :Instance. Vérifiez la présence de ces ressources dans votre produit provisionné ou confirmez que le document est correct.

Document with that name does not exist (Il n’existe aucun document portant ce nom)

Le document spécifié dans la définition de l'action de service n'existe pas.

Failed to describe SSM Automation document (La description du document SSM Automation a échoué)

AWS Service Cataloga rencontré une exception inconnue de SSM lors de la tentative de description du document spécifié.

Failed to retrieve credentials for role (La récupération des informations d'identification pour le rôle a échoué)

AWS Service Catalog a rencontré une erreur inconnue en assumant le rôle spécifié.

La valeur du paramètre ***InvalidValue***« » est introuvable dans ***{ValidValue1}, {ValidValue2}***

La valeur du paramètre transmise à SSM ne figure pas dans la liste des valeurs autorisées pour le document. Vérifiez que les paramètres fournis sont valides et réessayez.

Erreur de type de paramètre. La valeur fournie pour n'***ParameterName***est pas une chaîne valide.

La valeur du paramètre transmis à SSM n'est pas valide pour le type du document.

Parameter is not defined in service action definition (Le paramètre n'est pas défini dans la définition de l'action de service)

Un paramètre qui n'est pas défini dans la définition de l'action de service a été transmis à AWS Service Catalog. Vous pouvez uniquement utiliser des paramètres définis dans la définition de l'action de service.

L'étape échoue lorsqu'elle exécute/annule une action. ***Message d'erreur.*** Reportez-vous au guide de dépannage du service d'automatisation pour plus de détails sur le diagnostic.

Une étape du document d'automatisation SSM a échoué. Consultez l'erreur dans le message pour dépanner ultérieurement.

Les valeurs suivantes pour le paramètre ne sont pas autorisées car elles ne figurent pas dans le produit approvisionné : ***InvalidResourceId***

L'utilisateur a demandé une action sur une ressource qui ne se trouve pas dans le produit provisionné.

TargetType non défini pour le document SSM Automation

Les actions de service nécessitent que les documents d'automatisation SSM soient TargetType définis. Consultez votre document d'automatisation SSM.

Ajout de produits AWS Marketplace à votre portefeuille

Vous pouvez ajouter des produits AWS Marketplace à vos portefeuilles pour mettre ces produits à disposition de vos utilisateurs finaux AWS Service Catalog.

AWS Marketplace est une boutique en ligne dans laquelle vous trouverez un vaste choix de logiciels et services, auxquels vous pouvez vous abonner et que vous pouvez commencer à utiliser immédiatement. Les types de produits dans AWS Marketplace incluent des bases de données,

des serveurs d'applications, des outils de test, des outils de surveillance, des outils de gestion de contenu et des logiciels d'intelligence métier. AWS Marketplace est disponible à l'adresse https://aws.amazon.com/marketplace. Notez que vous ne pouvez pas ajouter de produits SaaS (Software as a Service) de AWS Marketplace àAWS Service Catalog.

Vous distribuez un AWS Marketplace produit aux utilisateurs AWS Service Catalog finaux en copiant le produit avec le AWS CloudFormation modèleAWS Service Catalog, puis en l'ajoutant à un portefeuille.

> **Note**
>
> AWS Service Catalogne prend pas en charge la distribution de AWS Marketplace produits aux utilisateurs AWS Service Catalog finaux à l'aide d'un modèle de produit Terraform Open Source ou Terraform Cloud.

AWS Marketplace prend en charge AWS Service Catalog directement, ou vous pouvez vous abonner et ajouter des produits à l'aide de l'option manuelle. Nous vous recommandons d'ajouter des produits à l'aide de la fonctionnalité spécialement conçue pour AWS Service Catalog.

Gestion des produits AWS Marketplace à l'aide d'AWS Service Catalog

Vous pouvez ajouter les produits AWS Marketplace auxquels vous êtes abonné directement à AWS Service Catalog à l'aide de l'interface personnalisée. Dans AWS Marketplace, choisissez Catalogue des services. Pour plus d'informations, consultez la section Copier des produits vers AWS Service Catalog dans l'AWS Marketplaceaide et la FAQ.

Gestion et ajout de produits AWS Marketplace à l'aide de l'option manuelle

Procédez comme suit pour vous abonner à un AWS Marketplace produit, définir ce produit dans un AWS CloudFormation modèle et ajouter le modèle à un AWS Service Catalog portefeuille.

Pour vous abonner à un produit AWS Marketplace

1. Accédez à AWS Marketplace à l'adresse https://aws.amazon.com/marketplace.
2. Parcourez les produits ou recherchez le produit que vous souhaitez ajouter à votre portefeuille AWS Service Catalog. Choisissez le produit pour afficher la page des détails du produit.
3. Choisissez Continuer pour afficher la page d'expédition, puis cliquez sur l'onglet Lancement manuel.

Les informations figurant sur la page d'expédition incluent les types d'instances Amazon Elastic Compute Cloud (Amazon EC2) pris en charge, les types d'instances Régions AWS pris en charge et l'ID Amazon Machine Image (AMI) que le produit utilise pour chaque région. AWS Veuillez noter que certains choix ont une incidence sur les coûts. Vous utiliserez ces informations pour personnaliser le modèle AWS CloudFormation dans des étapes ultérieures.

4. Choisissez Accept Terms pour vous abonner au produit.

   Une fois que vous vous êtes abonné à un produit, vous pouvez à tout moment accéder aux informations sur la page d'approvisionnement de produit dans AWS Marketplace, en choisissant Votre logiciel puis le produit.

Pour définir votre produit AWS Marketplace dans un modèle AWS CloudFormation

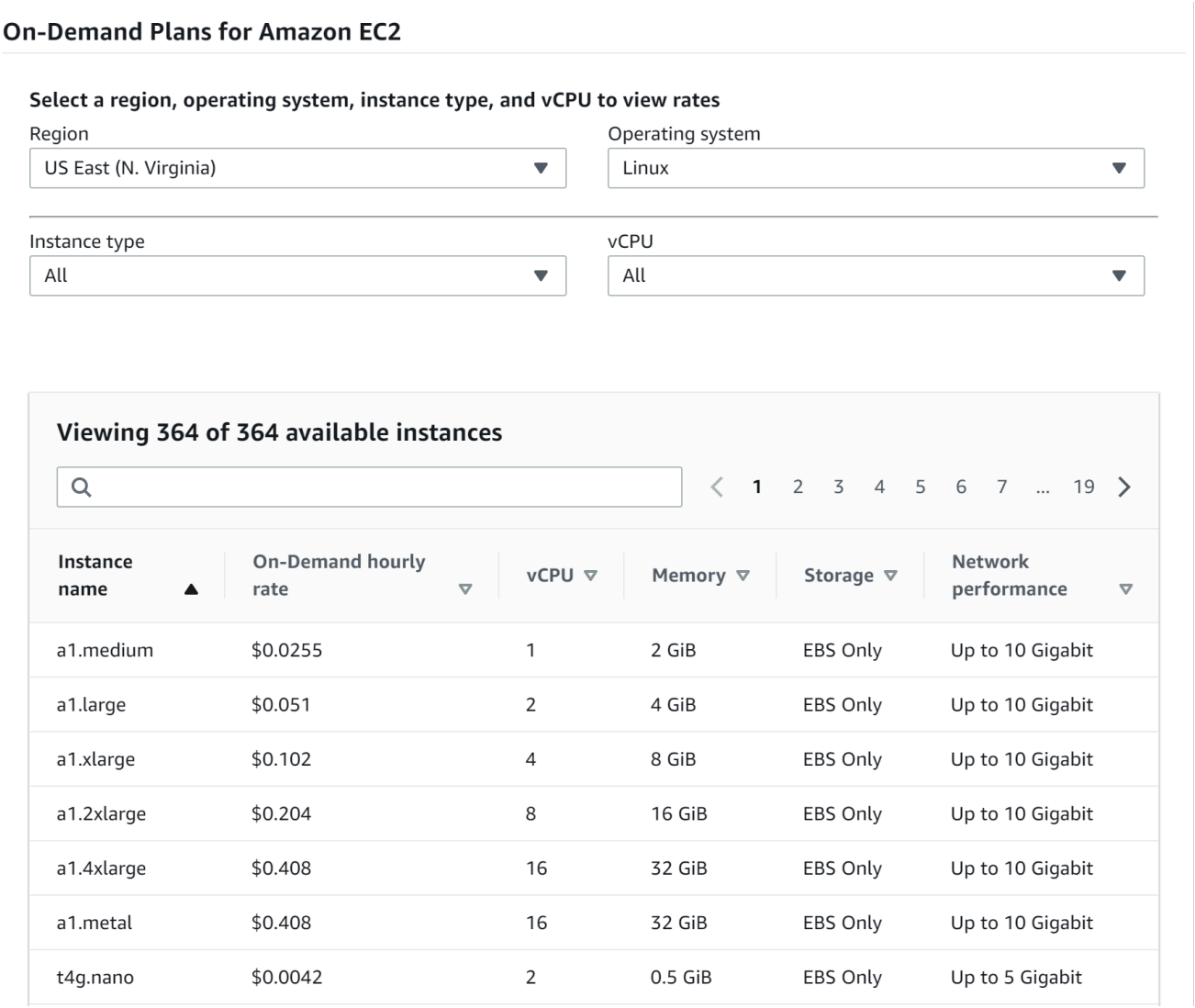
Pour effectuer les étapes suivantes, vous utiliserez l'un des exemples de modèle AWS CloudFormation comme point de départ et vous personnaliserez le modèle de façon à ce qu'il représente votre produit AWS Marketplace. Pour accéder aux exemples de modèle, consultez Exemples de modèle dans le Guide de l'utilisateur AWS CloudFormation.

1. Sur la page Exemples de modèles du guide de AWS CloudFormation l'utilisateur, choisissez une AWS région pour votre produit. La AWS région doit être prise en charge par votre AWS Marketplace produit. Vous pouvez afficher les régions prises en charge sur la page d'approvisionnement de produit dans AWS Marketplace.
2. Pour afficher une liste d'exemples de services adaptés à la région, cliquez sur le lien Services.
3. Vous pouvez utiliser tout modèle répondant à vos besoins comme point de départ. Les étapes de cette procédure utilisent le modèle Amazon EC2 instance in a security group. Pour afficher l'exemple de modèle, choisissez View, puis enregistrez une copie du modèle en local pour pouvoir le modifier. Votre fichier local doit avoir l'extension `.template`.
4. Ouvrez votre fichier de modèle dans un éditeur de texte.
5. Personnalisez la description en haut du modèle. Votre description peut ressembler à l'exemple suivant :

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

6. Personnalisez le paramètre `InstanceType` pour qu'il ne comprenne que les types d'instance EC2 qui sont pris en charge par votre produit. Si votre modèle inclut des types d'instances EC2 non pris en charge, le lancement du produit échouera pour vos utilisateurs finaux.

a. Sur la page d'expédition des produits enAWS Marketplace, consultez les types d'instances EC2 pris en charge dans la section Détails des prix.



On-Demand Plans for Amazon EC2

Select a region, operating system, instance type, and vCPU to view rates

Region: US East (N. Virginia)

Operating system: Linux

Instance type: All

vCPU: All

Viewing 364 of 364 available instances

1 2 3 4 5 6 7 ... 19

Instance name	On-Demand hourly rate	vCPU	Memory	Storage	Network performance
a1.medium	$0.0255	1	2 GiB	EBS Only	Up to 10 Gigabit
a1.large	$0.051	2	4 GiB	EBS Only	Up to 10 Gigabit
a1.xlarge	$0.102	4	8 GiB	EBS Only	Up to 10 Gigabit
a1.2xlarge	$0.204	8	16 GiB	EBS Only	Up to 10 Gigabit
a1.4xlarge	$0.408	16	32 GiB	EBS Only	Up to 10 Gigabit
a1.metal	$0.408	16	32 GiB	EBS Only	Up to 10 Gigabit
t4g.nano	$0.0042	2	0.5 GiB	EBS Only	Up to 5 Gigabit

b. Dans votre modèle, modifiez le type d'instance par défaut en un type d'instance EC2 pris en charge de votre choix.

c. Modifiez la liste `AllowedValues` pour qu'elle ne comprenne que les types d'instances EC2 qui sont pris en charge par votre produit.

d. Supprimez les types d'instances EC2 que vous ne souhaitez pas que vos utilisateurs finaux utilisent lorsqu'ils lancent le produit à partir de la liste `AllowedValues`.

Lorsque vous avez fini de modifier le paramètre `InstanceType`, celui-ci peut ressembler à l'exemple suivant :

```
    "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. Dans la section `Mappings` de votre modèle, modifiez les mappages `AWSInstanceType2Arch` de telle sorte que seuls les types d'instances EC2 et architectures pris en charge soient inclus.

   a. Modifiez la liste de mappages en supprimant tous les types d'instances EC2 qui ne sont pas inclus dans la liste `AllowedValues` pour le paramètre `InstanceType`.

   b. Modifiez la valeur `Arch` pour chaque type d'instance EC2 pour qu'elle corresponde au type d'architecture pris en charge par votre produit. Les valeurs valides sont `PV64`, `HVM64` et `HVMG2`. Pour savoir quelle architecture votre produit prend en charge, reportez-vous à la page des détails du produit dans AWS Marketplace. Pour savoir quelles architectures sont prises en charge par les familles d'instance EC2, consultez Tableau des versions de l'AMI Linux Amazon selon les types d'instances.

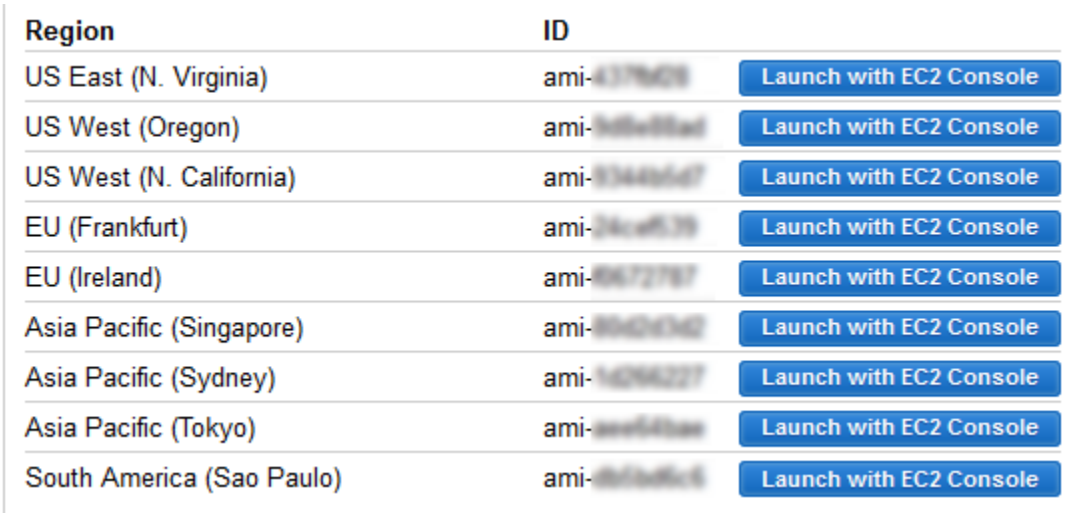
   Lorsque vous avez fini de modifier les mappages `AWSInstanceType2Arch`, cela peut ressembler à l'exemple suivant :

```
    "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. Dans la `Mappings` section de votre modèle, modifiez les `AWSRegionArch2AMI` mappages pour associer chaque AWS région à l'architecture et à l'ID AMI correspondants pour votre produit.

   a. Sur la page d'expédition du produit enAWS Marketplace, consultez l'ID AMI que votre produit utilise pour chaque AWS région, comme dans l'exemple suivant :



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. Dans votre modèle, supprimez les mappages pour toutes les AWS régions que vous ne prenez pas en charge.

   c. Modifiez le mappage pour chaque région afin de supprimer les architectures non prises en charge (`PV64`, `HVM64` ou `HVMG2`) et leurs ID d'AMI associés.

   d. Pour chaque mappage de AWS région et d'architecture restant, spécifiez l'ID d'AMI correspondant sur la page de détails du produit dansAWS Marketplace.

   Lorsque vous avez fini de modifier les mappages `AWSRegionArch2AMI`, votre code peut ressembler à l'exemple suivant :

```
    "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"}
  }
```

Vous pouvez désormais utiliser le modèle pour ajouter le produit à un AWS Service Catalog portefeuille. Si vous souhaitez apporter des modifications supplémentaires, consultez Utilisation des modèles AWS CloudFormation pour en savoir plus sur les modèles.

Pour ajouter votre AWS Marketplace produit à un AWS Service Catalog portefeuille

1. Connectez-vous à la console d'administration AWS Management Console et accédez à AWS Service Catalog celle-ci à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Sur la page Portefeuilles, choisissez le portefeuille auquel vous souhaitez ajouter votre AWS Marketplace produit.
3. Sur la page des détails du portefeuille, choisissez Importer un nouveau produit.
4. Tapez les détails du produit et les détails du support.
5. Sur la page Version details, choisissez Upload a template file, Browse, puis votre fichier de modèle.
6. Tapez un titre et une description pour la version.
7. Choisissez Suivant.
8. Sur la page Révision, vérifiez que le résumé est exact, puis choisissez Confirmer et chargez. Le produit est ajouté à votre portefeuille. Il est désormais disponible pour les utilisateurs finaux qui ont accès au portefeuille.

En utilisant AWS CloudFormation StackSets

> **Note**
>
> AutoTags ne sont actuellement pas pris en charge avec AWS CloudFormation StackSets.

Vous pouvez l'utiliser AWS CloudFormation StackSets pour lancer AWS Service Catalog des produits sur plusieurs Régions AWS comptes. Vous pouvez spécifier l'ordre dans lequel les produits seront déployés de manière séquentielle. Régions AWS Vers les comptes, les produits sont déployés en

parallèle. Lors du lancement, les utilisateurs peuvent spécifier la tolérance aux pannes et le nombre maximal de comptes concernés par le déploiement en parallèle. Pour plus d'informations, consultez Utilisation de AWS CloudFormation StackSets.

Comparaison des ensemble de piles et des instances de pile

Un ensemble de piles vous permet de créer des piles dans AWS des comptes de différentes AWS régions à l'aide d'un AWS CloudFormation modèle unique.

Une instance de pile fait référence à une pile dans un compte cible au sein d'une AWS région et n'est associée qu'à un seul ensemble de piles.

Pour plus d'informations, consultez Concepts StackSets.

Contraintes d'ensemble de piles

Dans AWS Service Catalog, vous pouvez utiliser des contraintes d'ensemble de piles pour configurer des options de déploiement de produit.

AWS Service Catalogprend en charge les contraintes liées au stack set sur les produits en deux AWS GovCloud (US) Regions catégories : AWS GovCloud (US-West) et AWS GovCloud (US-East).

Pour plus d'informations, consultez AWS Service CatalogStack Set Constraints.

Gestion des budgets

Vous pouvez utiliser AWS Budgets pour suivre vos coûts de service et votre utilisation dans AWS Service Catalog. Vous pouvez associer des budgets aux produits et portefeuilles AWS Service Catalog.

> **Note**
>
> AWS Service Catalogne prend pas en charge les budgets des produits Open Source Terraform.

AWS Budgets vous permet de définir des budgets personnalisés afin d'être alerté lorsque votre utilisation ou vos coûts dépassent (ou sont sur le point de dépasser) le montant prévu. Les informations sur AWS Budgets sont disponibles à l'adresse https://aws.amazon.com/aws-cost-management/aws-budgets.

Tâches

Prérequis

Avant d'utiliser AWS Budgets, vous devez activer les balises de répartition des coûts dans la console AWS Billing and Cost Management. Pour plus d’informations, consultez Activation des balises de répartition des coûts définies par l’utilisateur dans le Guide de l’utilisateur AWS Billing and Cost Management.

> **Note**
>
> L'activation des balises peut prendre jusqu'à 24 heures.

Vous devez également activer l'accès utilisateur à la console AWS Billing and Cost Management pour tous les utilisateurs ou groupes qui utiliseront la fonction Budgets. Pour ce faire, créez une nouvelle stratégie pour vos utilisateurs.

Pour permettre aux utilisateurs de créer des budgets, vous devez également autoriser les utilisateurs à afficher les informations de facturation. Si vous souhaitez utiliser les notifications Amazon SNS, vous pouvez donner aux utilisateurs la possibilité de créer des notifications Amazon SNS, comme indiqué dans l'exemple de politique ci-dessous.

Pour créer la stratégie des budgets

1. Ouvrez la console IAM à l’adresse https://console.aws.amazon.com/iam/.
2. Dans le panneau de navigation, choisissez Policies (Politiques).
3. Dans le panneau de contenu, sélectionnez Créer une politique.
4. Choisissez l'onglet JSON et copiez le texte du document de politique JSON suivant. Collez ce texte dans la zone de texte 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. Lorsque vous avez terminé, sélectionnez Examiner une politique. Le programme de validation de stratégie signale les éventuelles erreurs de syntaxe.
6. Sur la page Review (Vérification) attribuez un nom à votre stratégie. Passez en revue le Récapitulatif de la politique pour voir les autorisations accordées par votre politique, puis sélectionnez Créer une politique pour enregistrer votre travail.

   La nouvelle stratégie s'affiche dans la liste des stratégies gérées et est prête à être attachée à vos utilisateurs et groupes. Pour plus d'informations, consultez Créer et attacher une stratégie gérée par le client dans le Guide de l'utilisateur AWS Identity and Access Management.

Création d'un budget

Dans la console de l'AWS Service Catalogadministrateur, les pages Liste des produits et Portefeuilles contiennent des informations sur les produits et portefeuilles existants et vous permettent de prendre des mesures sur ceux-ci. Pour créer un budget, déterminez d'abord le produit ou le portefeuille auquel vous souhaitez associer le budget.

Pour créer un budget

1. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Choisissez Liste de produits ou Portefeuilles.
3. Sélectionnez le produit ou le portefeuille auquel vous souhaitez ajouter un budget.
4. Ouvrez le menu Actions, puis choisissez Créer un budget.
5. Sur la page Budget creation (Création du budget) associez un type de balise à votre budget.

   Il existe deux types de balises : AutoTags et TagOptions. AutoTags identifier le portefeuille, le produit et l'utilisateur qui a lancé un produit. AWS Service Catalogapplique ces balises automatiquement aux ressources provisionnées. A TagOption est une paire clé-valeur définie par l'administrateur qui est gérée dans. AWS Service Catalog

   Pour que les dépenses qui se produisent sur un portefeuille ou un produit soient reflétées sur le budget associé, elles doivent avoir la même balise. Notez que l'activation d'une clé de balise utilisée pour la première fois peut prendre 24 heures. Pour plus d'informations, consultez the section called “Prérequis”.
6. Choisissez Créer dans AWS Budgets. Vous êtes redirigé vers la page Définissez votre budget. Poursuivez la configuration de votre budget en suivant les étapes de la section Création d'un budget.

> **Note**
>
> Après avoir créé un budget, vous devez l'associer au produit ou au portefeuille.

Association d'un budget

Un budget peut être associé à chaque portefeuille ou produit. Chaque budget peut être associé à plusieurs portefeuilles et produits.

Lorsque vous associez un budget à un portefeuille ou à un produit, vous pouvez consulter les informations relatives au budget sur la page de détails de ce portefeuille ou de ce produit. Pour que les dépenses liées au portefeuille ou au produit soient reflétées dans le budget, vous devez associer les mêmes balises au budget et au portefeuille ou au produit.

> **Note**
>
> Si vous supprimez un budget deAWS Budgets, les associations existantes avec des AWS Service Catalog produits et des portefeuilles existent toujours. AWS Service Catalogne pourra afficher aucune information concernant le budget supprimé.

Pour associer un budget

1. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Choisissez Liste de produits ou Portefeuilles.
3. Sélectionnez le produit ou le portefeuille auquel vous souhaitez associer un budget.
4. Ouvrez le menu Actions, puis sélectionnez Associer un budget.
5. Sur la page Association de budget, sélectionnez un budget existant, puis choisissez Continuer.
6. Le tableau des produits ou des portefeuilles inclut désormais les données relatives au budget que vous venez d'ajouter.

Affichage d'un budget

Si un budget est associé à un produit, vous pouvez consulter les informations relatives au budget sur les pages Détails du produit et Liste des produits. Si un budget est associé à un portefeuille, vous pouvez consulter les informations relatives au budget sur les pages Portefeuilles et Détails du portefeuille.

Les pages Portefeuilles et Liste de produits affichent les informations budgétaires relatives aux ressources existantes. Vous pouvez voir les colonnes affichant Current vs. budget (Différences entre l'état actuel et le budget) et Forecast vs. budget (Différences entre les prévisions et l'état actuel).

Lorsque vous choisissez un produit ou un portefeuille, vous êtes dirigé vers une page de détails. Les pages Détails du portefeuille et Détails du produit comportent des sections contenant des informations détaillées sur les budgets associés. Vous pouvez consulter le montant budgété, les

dépenses réelles et les dépenses prévues. Vous avez également la possibilité d'afficher les détails du budget et de modifier le budget.

Dissociation d'un budget

Vous pouvez dissocier un budget d'un portefeuille ou d'un produit.

> **Note**
>
> Si vous supprimez un budget des AWS budgets, les associations existantes avec des AWS Service Catalog produits et des portefeuilles existent toujours. AWS Service Catalogne pourra afficher aucune information concernant le budget supprimé.

Pour dissocier un budget

1. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Choisissez Liste de produits ou Portefeuilles.
3. Sélectionnez le produit ou le portefeuille dont vous souhaitez dissocier un budget.
4. Choisissez Actions. Dans le menu déroulant, choisissez Dissocier le budget. Une alerte de confirmation apparaît.
5. Après avoir confirmé que vous souhaitez dissocier le budget du produit ou du portefeuille, choisissez Confirmer.

Gestion des produits provisionnés

AWS Service Catalog fournit une interface pour la gestion des produits provisionnés. Vous pouvez afficher, mettre à jour et mettre fin à tous les produits provisionnés pour votre catalogue selon le niveau d'accès. Vous trouverez dans les sections suivantes des exemples de procédures.

Rubriques

Gérer les produits provisionnés en tant qu'administrateur

Pour gérer tous les produits fournis pour un compte, vous devez disposer d'une autorisation IAM `AWSServiceCatalogAdminFullAccess` ou d'une autorisation IAM équivalente pour accéder aux opérations d'écriture des produits fournis. Pour plus d'informations, consultez Identity and Access Management dans AWS Service Catalog.

> **Tip**
>
> Pour le chaînage statique des produits approvisionnés, vous devez référencer les sorties des produits fournis dans un modèle d'artefact de produit avant que le produit fourni ne soit approvisionné. Pour plus d'informations, y compris un exemple, consultez ce qui suit :
>
> - AWS::ServiceCatalog::CloudFormationProvisionedProduct dans le guide de l'utilisateur AWS CloudFormation.
> - DescribeProvisioningParameters (ProvisioningArtifactOutputKeys) dans le Guide du AWS Service Catalog développeur.

Pour afficher et gérer tous les produits provisionnés

1. Ouvrez la AWS Service Catalog console à l'adresse https://console.aws.amazon.com/servicecatalog/.

   Si vous êtes déjà connecté à la AWS Service Catalog console, choisissez Service Catalog, puis Utilisateur final.
2. Si nécessaire, faites défiler la page vers le bas jusqu'à la section Produits approvisionnés.
3. Dans la section Produits fournis, choisissez la liste Afficher : et sélectionnez le niveau d'accès que vous souhaitez voir : utilisateur, rôle ou compte. Cette action affiche tous les produits approvisionnés dans le catalogue.
4. Choisissez un produit provisionné à afficher, mettre à jour ou résilier. Pour plus d'informations sur les détails fournis dans cette vue, consultez Affichage d'informations sur les produits provisionnés.

Modification du propriétaire du produit provisionné

Vous pouvez changer le propriétaire d'un produit provisionné à tout moment. Vous devez connaître l'ARN de l'utilisateur ou du rôle que vous souhaitez définir en tant que nouveau propriétaire.

Par défaut, cette fonctionnalité est disponible pour les administrateurs utilisant la politique `AWSServiceCatalogAdminFullAccess` gérée. Vous pouvez l'activer pour les utilisateurs finaux en leur accordant l'`servicecatalog:UpdateProvisionedProductProperties`autorisation dans AWS Identity and Access Management (IAM).

Modifier le propriétaire d'un produit provisionné

1. Dans la console AWS Service Catalog, choisissez Provisioned products list (Liste des produits provisionnés).
2. Localisez le produit approvisionné que vous souhaitez mettre à jour, puis choisissez les trois points situés à côté de celui-ci et choisissez Modifier le propriétaire du produit provisionné.Vous pouvez également accéder à l'option Change owner (Modifier le propriétaire) sur la page détaillée du produit provisionné, dans le menu Actions.
3. Dans la boîte de dialogue, saisissez l'ARN de l'utilisateur ou du rôle que vous souhaitez définir en tant que nouveau propriétaire. Un ARN commence par `arn:` et inclut d'autres informations séparées par des deux-points ou des barres obliques, par exemple `arn:aws:iam::123456789012:user/NewOwner`.

4. Sélectionnez Envoyer. Un message de succès de l’opération s'affiche lorsque le propriétaire a été mis à jour.

consultez aussi

- UpdateProvisionedProductProperties

Mise à jour des modèles pour les produits approvisionnés

Vous pouvez remplacer le modèle actuel d'un produit approvisionné par un autre modèle. Par exemple, si vous avez un produit EC2 dans Service Catalog, vous pouvez mettre à jour ce produit EC2 pour conserver le même identifiant de produit fourni, mais remplacer le modèle par un compartiment S3.

> **Note**
>
> La mise à jour des modèles n'est pas prise en charge pour les produits Terraform Open Source ou Terraform Cloud provisionnés. Si vous souhaitez utiliser un modèle différent pour un produit Terraform existant, vous devez supprimer le produit, puis créer un nouveau produit à l'aide du modèle souhaité.

Pour mettre à jour un modèle pour un produit approvisionné

1. Dans le menu de navigation de gauche, choisissez Provisioned products.
2. Dans Produits provisionnés, choisissez un produit provisionné et sélectionnez Actions, Mettre à jour.

   Notez que vous pouvez également sélectionner Actions, Mettre à jour sur la page de détails du produit provisionné.
3. (Facultatif) Dans Détails du produit, sélectionnez Modifier le produit.

   Dans Changer de produit, notez cet avertissement :

   La modification du produit mettra à jour ce produit approvisionné vers un autre modèle de produit. Cela peut mettre fin à des ressources et en créer de nouvelles.

Vous pouvez mettre à jour un produit approvisionné vers une version différente au sein du même produit.

4. (Facultatif) Dans Produits, choisissez le produit que vous souhaitez mettre à jour avec un autre modèle. Choisissez ensuite Modifier.

   Dans Détails du produit, notez cet avertissement :

   [Nom du produit] sera mis à jour de [nom du modèle actuel] à [nouveau nom du modèle]. Toutefois, le nom de votre produit approvisionné, [Nom du produit approvisionné], ne changera pas.

   Vous pouvez mettre à jour un produit approvisionné vers une version différente au sein du même produit.

5. Dans Versions du produit, choisissez la version du produit que vous souhaitez.
6. Dans Paramètres, sélectionnez les paramètres appropriés.
7. Choisissez Mettre à jour.

   Dans Détails du produit provisionné, vous pouvez consulter les détails de la mise à jour. Le nom du produit provisionné ne change pas, mais le produit provisionné possède désormais un modèle différent.

Didacticiel : Identification de l'utilisateur pour l'allocation des ressources

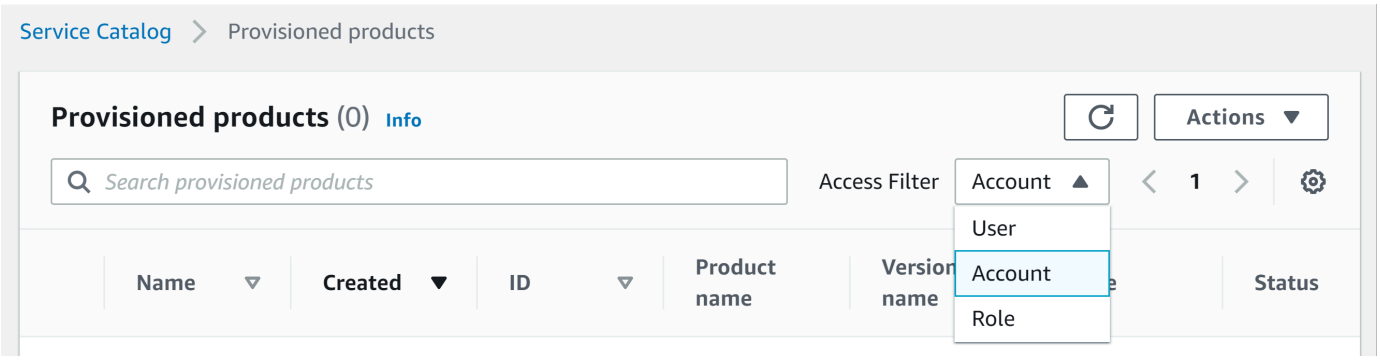
Vous pouvez identifier l'utilisateur qui a provisionné un produit et les ressources associées au produit à l'aide de la console AWS Service Catalog. Ce didacticiel vous aide à adapter cet exemple à vos propres produits provisionnés spécifiques.

Pour gérer tous les produits provisionnés pour le compte, vous avez besoin de l'accès `AWSServiceCatalogAdminFullAccess` ou d'un accès équivalent aux opérations d'écriture sur les produits provisionnés. Pour plus d'informations, consultez Identity and Access Management dans le guide de AWS Service Catalog l'administrateur.

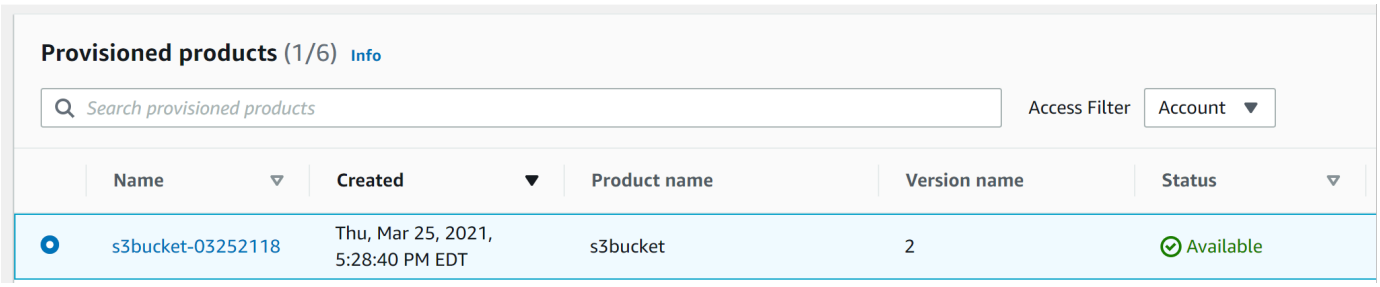
Pour identifier l'utilisateur qui a provisionné un produit et les ressources associées

1. Ouvrez https://console.aws.amazon.com/servicecatalog.

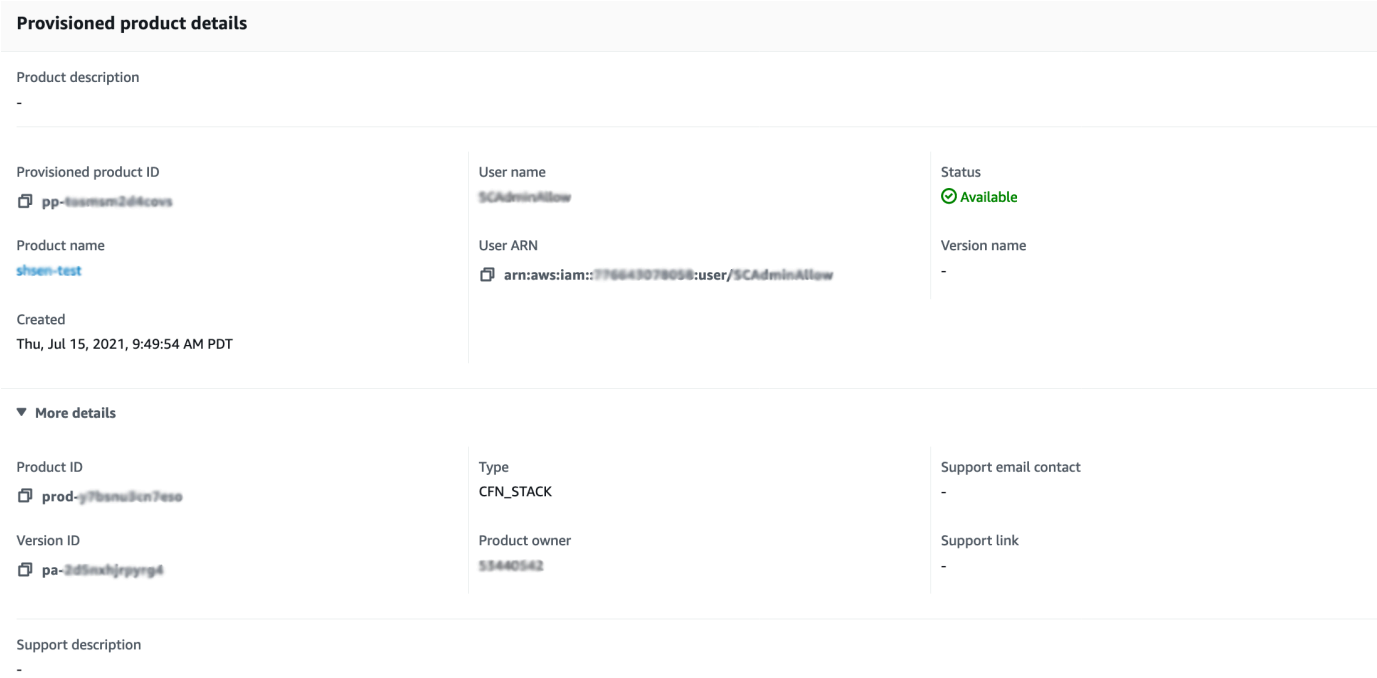
2. Dans le menu de navigation de gauche, choisissez Provisioned product.
3. Dans le menu déroulant du filtre d'accès, sélectionnez Compte.



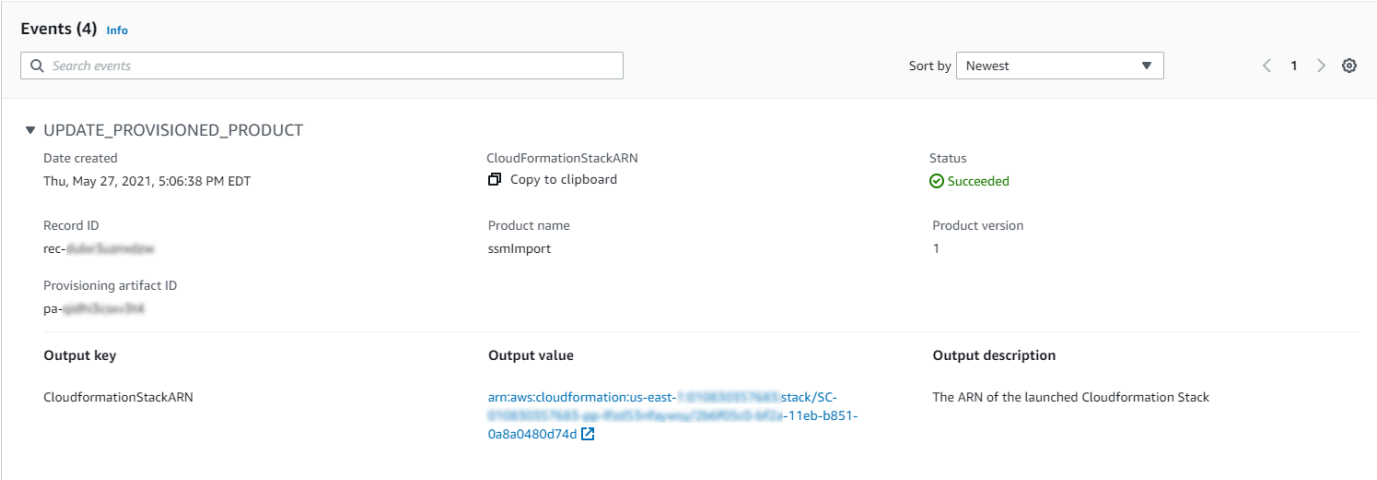
4. Dans la vue Compte, choisissez et ouvrez un produit approvisionné pour en afficher les détails.



Vous pouvez consulter les détails du produit approvisionné.



5. Faites défiler la page vers le bas pour développer la section Événements. Notez les `CloudformationStackARN` valeurs `Provisioned product ID` et.



6. Utilisez l'ID de produit fourni pour identifier l'AWS CloudTrailenregistrement correspondant à ce lancement et identifier l'utilisateur demandeur (généralement, vous entrez une adresse e-mail lors de la fédération). Dans cet exemple, il s'agit de « 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. Utilisez la `CloudformationStack`ARN valeur pour identifier les AWS CloudFormation événements afin de trouver des informations sur les ressources créées. Vous pouvez également

utiliser l'API AWS CloudFormation pour obtenir ces informations. Pour plus d'informations, veuillez consulter AWS CloudFormation Référence d'API .

Vous pouvez effectuer les étapes 1 à 4 à l'aide de l'AWS Service CatalogAPI ou duAWS CLI. Pour plus d'informations, consultez le guide AWS Service Catalog du développeur. et référence AWS Service Catalog de ligne de commande.

Gestion des erreurs d'état des produits Terraform Open Source

Les `ProvisionProduct` défaillances de Terraform Open Source sont renvoyées vers l'`TAINTED`État, ce qui permet à chaque produit provisionné de continuer. `UpdateProvisionedProduct` Lorsque cela se produit :

- `UpdateProvisionedProduct`ne tente pas de mettre à jour ou de corriger les balises, ni de créer ou de modifier un groupe de ressources.
- `UpdateProvisionedProduct`ne prend pas en compte les échecs liés aux opérations de provisionnement précédentes lorsqu'il décide si le produit provisionné doit être configuré sur ou. `AVAILABLE` `TAINTED`

AWS Service Catalogapplique uniquement les tags pendant`ProvisionProduct`. Tout échec de balisage résultant d'un échec de l'`ProvisionProduct`opération n'est pas automatiquement résolu.

Exemples d'erreurs de statut

Exemple 1 : AWS Service Catalog ne crée pas de groupe de ressources pendant `ProvisionProduct`

Dans le scénario ci-dessous, vous disposez d'un produit provisionné dans l'`AVAILABLE`état même s'il n'existe pas de groupe de ressources de support, et aucune balise n'est appliquée aux ressources.

1. Votre action démarre. `ProvisionProduct`
2. Le moteur de provisionnement Terraform répond à une défaillance du flux `ProvisionProduct` de travail et ne fournit pas de. `ResourceIdentifier`
3. Le `ProvisionProduct` flux de travail ne crée pas de groupe de ressources, puis définit l'état du produit provisionné sur`ERROR`.
4. Vous lancez ensuite l'`UpdateProvisionedproduct`opération.

5. Le moteur de provisionnement Terraform répond en indiquant « succès ».
6. Par conséquent, le `UpdateprovisionedProduct` flux de travail définit l'état du produit provisionné sur`AVAILABLE`, mais ne crée pas de groupe de ressources et ne tente pas d'appliquer de balises.

Exemple 2 : AWS Service Catalog crée de nouvelles ressources pendant `UpdateProvisionedProduct`

Dans le scénario ci-dessous, vous avez un produit provisionné dans l'`AVAILABLE`état même si aucune balise n'est appliquée aux nouvelles ressources.

1. Votre action démarre. `ProvisionProduct`
2. Le moteur de provisionnement Terraform répond en indiquant le « succès » et fournit un. `ResourceIdentifier`
3. Le `ProvisionProduct` flux de travail crée un groupe de ressources et applique des balises à toutes les ressources identifiées.
4. Vous lancez `UpdateProvisionedProduct` un nouvel artefact qui crée de nouvelles ressources.
5. Le moteur de provisionnement Terraform répond en indiquant « succès ».
6. Le `UpdateProvisionedProduct` flux de travail définit l'état du produit provisionné sur `AVAILABLE` mais ne tente pas d'appliquer de balises supplémentaires aux nouvelles ressources.

Solution d'erreur d'état

AWS Service Cataloggarantit qu'un groupe de ressources est créé pour tous les produits provisionnés définis à `TAINTED` partir de`ProvisionProduct`. Si le moteur de provisionnement Terraform ne renvoie pas de groupe de ressources`ResourceIdentifier`, ou s'il AWS Service Catalog ne parvient pas à créer de groupe de ressources, le produit provisionné est défini sur `ERROR` cet état, vous obligeant à le résilier.

Gestion du fichier d'état du produit Terraform Open Source

Chaque produit Terraform Open Source provisionné possède un fichier à état unique. Il existe une relation 1:1 entre le produit provisionné et son fichier d'état. Les fichiers sont stockés dans un compartiment Amazon S3 nommé`sc-terraform-engine-state-${AWS::AccountId}-`

`${AWS::Region}`. Le fichier d'état est enregistré sous la clé `ProvisionedProductID` d'objet `AccountID` ou.

L'accès aux fichiers d'état est limité aux modèles de lancement Amazon EC2 `GetStateFile` AWS Lambda et à ceux d'Amazon EC2. AWS Service Catalogles administrateurs n'ont pas d'accès direct aux fichiers d'état dans Amazon S3. Les administrateurs doivent accéder aux fichiers à l'aide d'Amazon EC2. Par défaut, AWS Service Catalog les administrateurs peuvent voir la liste des fichiers d'état, mais ne peuvent ni lire ni écrire le contenu des fichiers. Seul le moteur de provisionnement Terraform peut lire ou écrire le contenu du fichier.

Gestion des balises dans AWS Service Catalog

AWS Service Catalog fournit des balises afin que vous puissiez classer vos ressources par catégorie. Il existe deux types de balises : AutoTags et TagOptions.

AutoTags sont des balises qui identifient les informations relatives à l'origine d'une ressource provisionnée AWS Service Catalog et qui sont automatiquement appliquées par AWS Service Catalog celles-ci.

TagOptions sont des paires clé-valeur gérées AWS Service Catalog qui servent de modèles pour créer AWS des balises.

Rubriques

AWS Service Catalog AutoTags

> **Note**
>
> AWS Service Catalogne prend pas en charge AutoTags les produits Open Source Terraform.

AutoTags sont des balises qui identifient les informations relatives à l'origine d'une ressource provisionnée AWS Service Catalog et qui sont automatiquement appliquées par AWS Service Catalog celles-ci.

AutoTags incluez des balises pour les identifiants uniques du portefeuille, du produit, de l'utilisateur, de la version du produit et du produit approvisionné. Cela fournit un ensemble de balises qui reflètent la structure AWS Service Catalog que les clients ont configurée dans le catalogue. AutoTags ne comptez pas dans la limite de 50 étiquettes fixée par le client.

> **Note**
>
> AWS Service Catalogne prend pas en charge AutoTags les produits Open Source Terraform.

AWS Service Catalog AutoTags peut vous aider à étiqueter vos ressources de manière cohérente, ce qui est utile lors de la définition des budgets d'un portefeuille, d'un produit ou d'un utilisateur. Vous pouvez également utiliser le AutoTags pour identifier les ressources pour les opérations post-lancement, telles que la définition de AWS Config règles. AutoTags pour vos ressources provisionnées, vous pouvez consulter la section Tags des services en aval utilisés pour le provisionnementAWS CloudFormation, tels qu'Amazon EC2 et Amazon S3.

> **Note**
>
> AWS Service Catalogne se met pas à jour une AutoTags fois que vous avez soumis AutoTags une demande aux ressources provisionnées. Si vous mettez à jour le produit approvisionné vers un autre produit, un artefact provisionné ou un nouveau chemin de lancement, le produit existant affiche AutoTags toujours les valeurs d'origine.

AutoTag détails

- aws:servicecatalog:portfolioArn - ARN du portefeuille à partir duquel le produit provisionné a été lancé.
- aws:servicecatalog:productArn - ARN du produit à partir duquel le produit provisionné a été lancé.
- aws:servicecatalog : - provisioningPrincipalArn L'ARN du principal d'approvisionnement (utilisateur) qui a créé le produit approvisionné.
- aws:servicecatalog : - L'ARN provisionedProductArn du produit provisionné.
- aws:servicecatalog : provisioningArtifactIdentifier - L'ID de l'artefact d'approvisionnement d'origine (version du produit).

AWS Service Catalog TagOption Bibliothèque

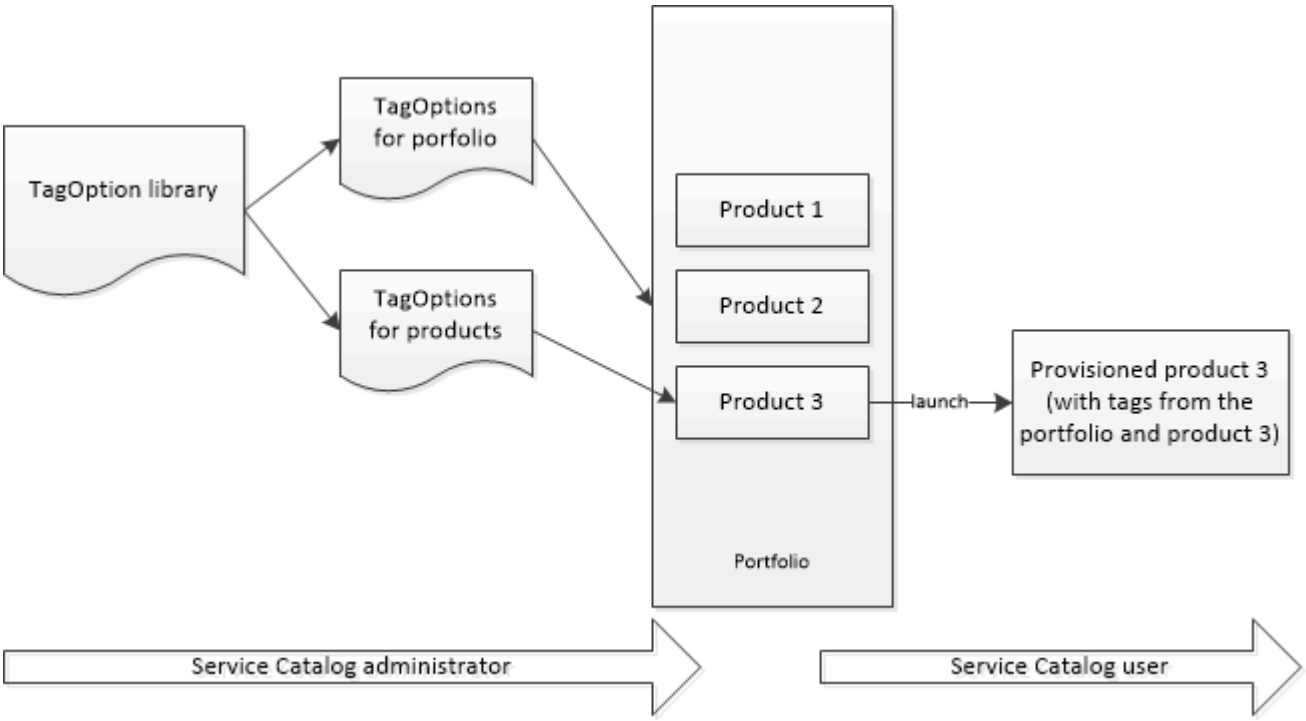
Pour permettre aux administrateurs de gérer facilement les balises sur les produits provisionnés, AWS Service Catalog fournit une TagOption bibliothèque. A TagOption est une paire clé-valeur gérée dans. AWS Service Catalog Il ne s'agit pas d'un AWS tag, mais sert de modèle pour créer un AWS tag basé sur le TagOption.

AWS Service Catalogne prend pas en charge TagOptions les produits Terraform Open Source ou Terraform Cloud.

La TagOption bibliothèque facilite l'application des éléments suivants :

- Une taxonomie cohérente
- Le balisage approprié des ressources AWS Service Catalog
- Des options définies et sélectionnables par l'utilisateur pour les balises autorisées

Les administrateurs peuvent s' TagOptions associer à des portefeuilles et à des produits. Lors du lancement d'un produit (provisionnement), AWS Service Catalog agrège le portefeuille et le produit TagOptions associés et les applique au produit approvisionné, comme indiqué dans le schéma suivant.



Avec la TagOption bibliothèque, vous pouvez désactiver TagOptions et conserver leurs associations avec des portefeuilles ou des produits, et les réactiver lorsque vous en avez besoin. Cette approche permet non seulement de préserver l'intégrité de la bibliothèque, mais également de gérer les bibliothèques TagOptions susceptibles d'être utilisées par intermittence ou uniquement dans des circonstances particulières.

Vous gérez à l' TagOptions aide de la AWS Service Catalog console ou de l'API de TagOption bibliothèque. Pour plus d'informations, consultez la section Service Catalog API Reference.

Table des matières

- Politiques TagOptions d'utilisation avec les AWS Organizations balises

Lancer un produit avec TagOptions

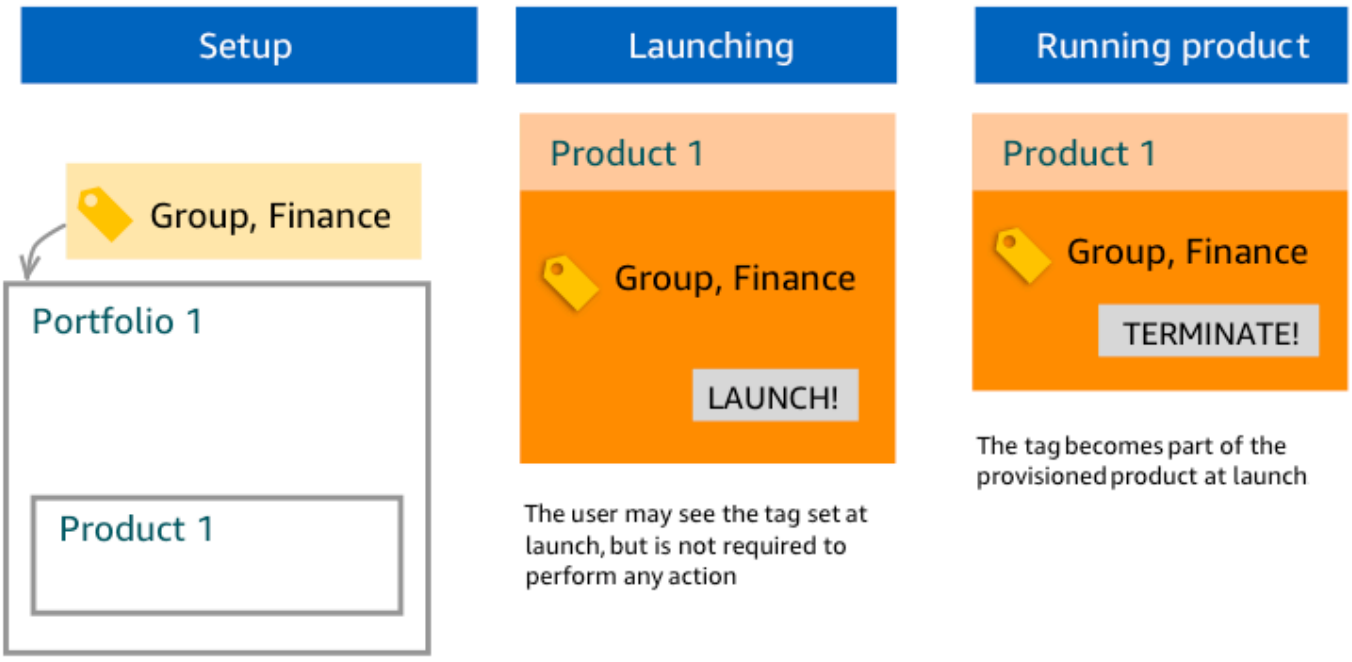
Lorsqu'un utilisateur lance un produit qui TagOptions a AWS Service Catalog effectué les actions suivantes en votre nom :

- Recueille tout TagOptions pour le produit et le portefeuille de lancement.
- Garantit que seules TagOptions des clés uniques sont utilisées dans une balise du produit provisionné. Les utilisateurs obtiennent des listes de valeurs à choix multiples pour une clé. Lorsque l'utilisateur choisit une valeur, elle devient une balise sur le produit provisionné.
- Permet aux utilisateurs d'ajouter des balises non conflictuelles au produit pendant la mise en service.

Les cas d'utilisation suivants illustrent le TagOptions fonctionnement lors du lancement.

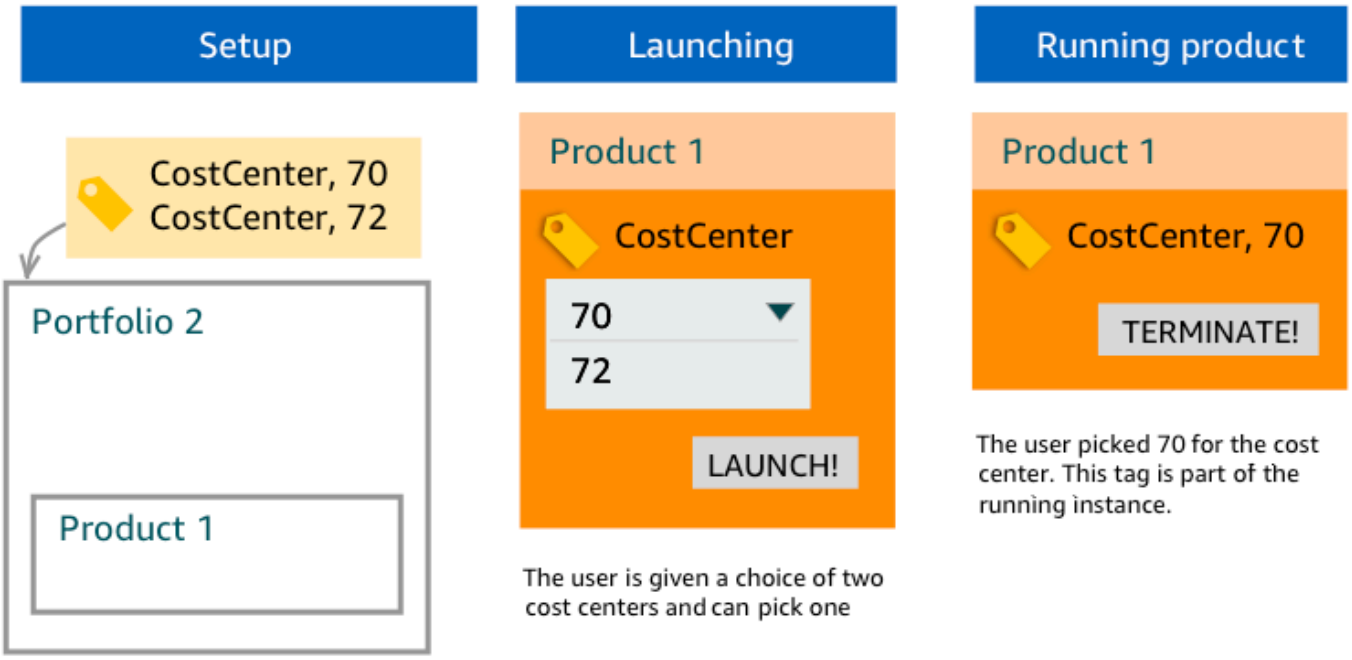
Exemple 1 : une TagOption clé unique

Un administrateur crée TagOption[Group=Finance] et l'associe à Portfolio1, qui possède Product1 sans numéro. TagOptions Lorsqu'un utilisateur lance le produit provisionné, le single TagOption devient Tag [Group=Finance], comme suit :



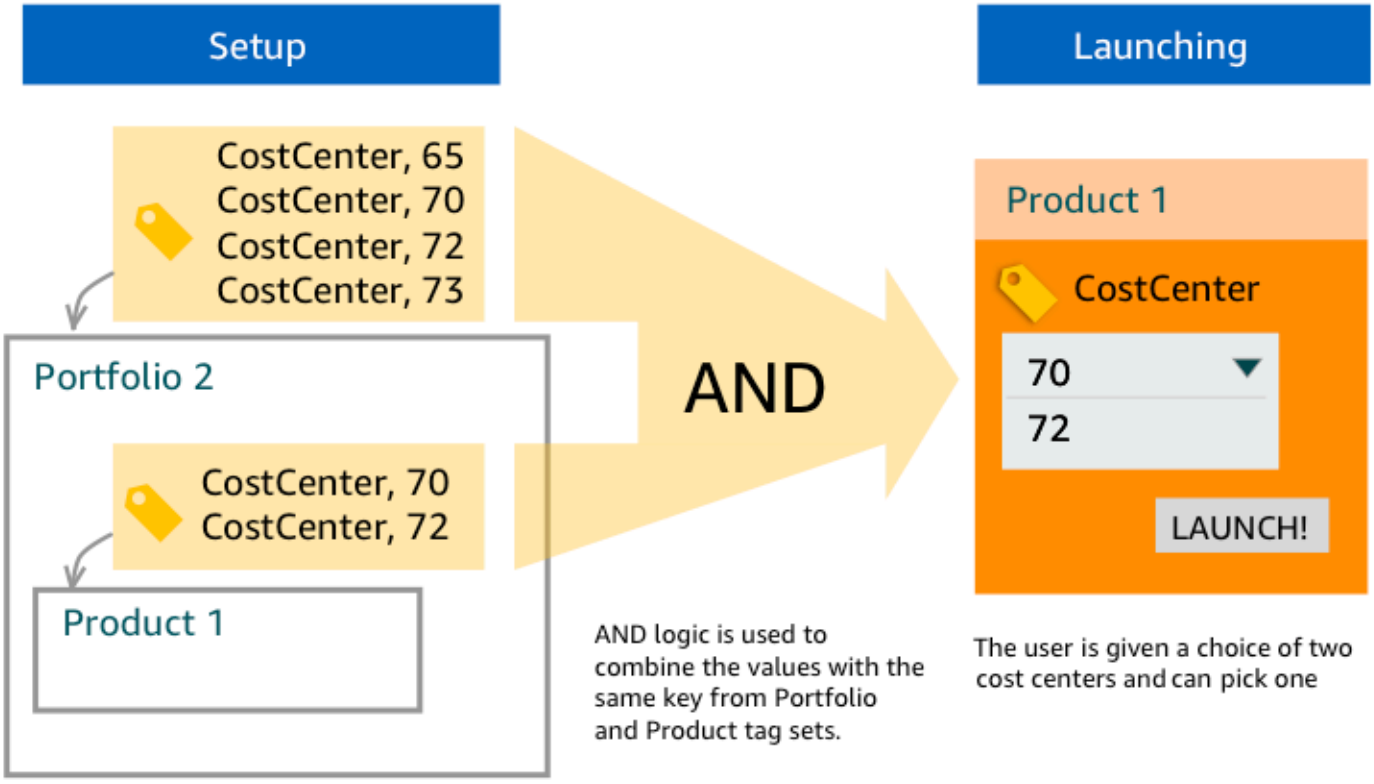
Exemple 2 : Un ensemble de fichiers TagOptions avec la même clé sur un portefeuille

Un administrateur en a placé deux TagOptions avec la même clé dans un portefeuille, et aucun TagOptions produit de ce portefeuille ne possède la même clé. Lors du lancement, l'utilisateur doit sélectionner l'une des deux valeurs associées à la clé. Le produit provisionné est alors balisé avec la clé et la valeur sélectionnée par l'utilisateur.



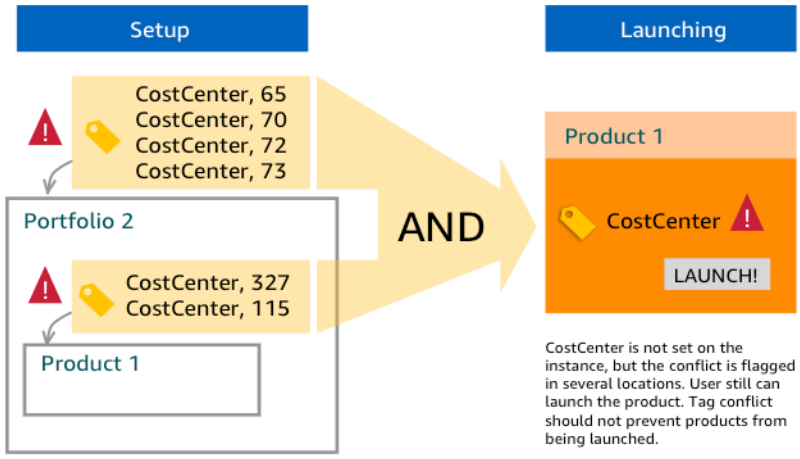
Exemple 3 : Un ensemble de TagOptions avec la même clé à la fois sur le portefeuille et sur un produit de ce portefeuille

Un administrateur en a placé plusieurs TagOptions avec la même clé dans un portefeuille, et il en existe également plusieurs TagOptions avec la même clé sur le produit au sein de ce portefeuille. AWS Service Catalogcrée un ensemble de valeurs à partir de l'agrégation (opération logique ET) du TagOptions. Lorsque l'utilisateur lance le produit, cet ensemble de valeurs s'affiche et il peut y faire son choix. Le produit provisionné est balisé avec la clé et la valeur sélectionnée par l'utilisateur.



Exemple 4 : Plusieurs TagOptions avec la même clé et des valeurs contradictoires

Un administrateur en a placé plusieurs TagOptions avec la même clé dans un portefeuille, et il en existe également plusieurs TagOptions avec la même clé sur le produit de ce portefeuille. AWS Service Catalogcrée un ensemble de valeurs à partir de l'agrégation (opération logique ET) du TagOptions. Si l'agrégation ne trouve pas de valeurs pour la clé, AWS Service Catalog crée une balise avec la même clé et la valeur `sc-tagconflict-`*`portfolioid`*`-`*`productid`*, où *`portfolioid`* et *`productid`* sont les ARN du portefeuille et du produit. Cela permet de s'assurer que le produit provisionné est balisé avec la clé appropriée et avec une valeur que l'administrateur peut trouver et corriger.



Gérer TagOptions

En tant qu'administrateur, vous pouvez effectuer les actions suivantes pour gérer TagOptions la TagOptions bibliothèque :

- Création et suppression
- Activer ou désactiver
- Associer ou dissocier
- Modifier

Pour créer TagOptions dans la console

1. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Dans le menu de navigation de gauche, choisissez TagOptionsbibliothèque.
3. Dans Créer nouveau TagOption, entrez une clé et une valeur, puis choisissez Ajouter.

   Une fois le nouveau TagOption fichier créé, il est regroupé par paire clé-valeur et trié par ordre alphabétique dans la liste. TagOptions

   Pour créer un à TagOption l'aide de l'AWS Service CatalogAPI, consultez CreateTagOption.

Pour supprimer TagOptions dans la console

1. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Dans le menu de navigation de gauche, choisissez TagOptions bibliothèque, puis Actions.

3. Sélectionnez Supprimer et confirmez la suppression.

Pour activer ou désactiver une ou plusieurs options TagOptions dans la console

1. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Dans le menu de navigation de gauche, choisissez TagOptions bibliothèque, puis Actions.
3. Pour l'activer, choisissez l'élément inactif TagOption que vous souhaitez. Choisissez ensuite Actions, puis sélectionnez Activer dans le menu déroulant, puis confirmez votre sélection.

   Pour le désactiver, choisissez l'actif TagOption que vous souhaitez. Choisissez ensuite Actions, puis sélectionnez Désactiver dans le menu déroulant, puis confirmez votre sélection.

Pour associer ou dissocier un ou plusieurs d'entre eux TagOptions à un portefeuille dans la console

1. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Dans le menu de navigation de gauche, choisissez Portefeuilles, puis ouvrez le portefeuille que vous souhaitez associer ou dissocier.
3. Choisissez l'TagOptionsonglet et sélectionnez-en un ou plusieurs TagOptions à associer ou à dissocier du portefeuille.
4. Choisissez Actions. Sélectionnez ensuite Associer ou Dissocier et confirmez votre sélection.

Pour associer ou dissocier un ou plusieurs TagOptions produits dans la console

1. Ouvrez la AWS Service Catalog console à l'adresse suivante : https://console.aws.amazon.com/servicecatalog/.
2. Dans le menu de navigation de gauche, sous Administration, sélectionnez Produits. Ouvrez ensuite le produit que vous souhaitez associer ou dissocier.
3. Choisissez l'TagOptionsonglet et sélectionnez-en un ou plusieurs TagOptions à associer ou à dissocier du portefeuille.
4. Choisissez Actions. Sélectionnez ensuite Associer ou Dissocier et confirmez votre sélection.

> **Note**
>
> Pour l' TagOptions associer à un portefeuille ou à un produit à l'aide de l'AWS Service CatalogAPI, consultez AssociateTagOptionWithResource.

Pour supprimer (dissocier) à TagOptions l'aide de l'AWS Service CatalogAPI, consultez DisassociateTagOptionFromResource.

Pour modifier les valeurs de TagOptions dans la console

1. Ouvrez la console Service Catalog à l'adresse https://console.aws.amazon.com/servicecatalog/.
2. Dans le menu de navigation de gauche, choisissez TagOptionsbibliothèque.
3. Choisissez un TagOption et ouvrez la valeur. (La valeur est un lien hypertexte.) Puis, choisissez Modifier.
4. Dans le champ Valeur, modifiez la valeur et choisissez Enregistrer les modifications.

Politiques TagOptions d'utilisation avec les AWS Organizations balises

Cette rubrique fournit un bref aperçu des politiques relatives aux balises pour AWS Organizations et TagOptions pourAWS Service Catalog. Il suggère également comment éviter les conflits de balisage lors de l'utilisation simultanée des deux fonctionnalités.

TagOptions pour AWS Service Catalog s'appliquer aux produits provisionnés (CloudFormationpiles), tandis que les politiques de balisage AWS Organizations s'appliquent aux AWS comptes et aux unités organisationnelles (UO) ou à une racine organisationnelle. Par exemple, si vous associez une politique de balises à une unité d'organisation, la même politique de balises s'applique à tous les comptes de cette unité d'organisation. Si vous utilisez les deux fonctionnalités de balisage simultanément, vous devez les configurer de manière à ce qu'elles n'entrent pas en conflit.

Politiques de balises

Les politiques relatives aux balises vous permettent de définir des règles relatives à l'utilisation des balises sur les AWS ressources de vos comptes dansAWS Organizations. Vous pouvez utiliser les politiques relatives aux balises pour créer et maintenir une approche cohérente en matière de balisage AWS des ressources au niveau du compte.

Les politiques relatives aux balises constituent un moyen simple de garantir que les utilisateurs appliquent des balises cohérentes, auditent les ressources balisées et assurent une catégorisation appropriée des ressources. Vous pouvez également définir la façon dont les clés de balise doivent être mises en majuscules, ainsi que les valeurs que vous souhaitez autoriser. Par exemple, vous

pouvez exiger que toutes les instances EC2 d'un compte aient une clé de balise définie comme **`CostCenter`** et que les valeurs de cette balise soient **`Data Insights`** ou**`Marketing`**.

Les politiques de balises vous permettent de sélectionner des options pour appliquer les règles de balisage, empêcher les opérations non conformes pour les balises et spécifier les types de ressources auxquels s'applique l'application de ces règles. Si vous ne choisissez aucune option d'application, les politiques de balises vous permettent de créer ou de muter les balises non conformes, mais les signalent comme non conformes dans la console. AWS Organizations

Pour plus d'informations sur la façon de configurer l'application du balisage au niveau du compte, consultez la section Politiques relatives aux balises dans AWS Organizations.

TagOptions

TagOptions sont une fonctionnalité de balisage qui AWS Service Catalog s'applique aux produits approvisionnés au niveau de la CloudFormation pile s'ils sont appliqués à un produit associé. AWS Service Catalogfournit une TagOptions bibliothèque dans laquelle vous pouvez définir les paires clé-valeur à associer à vos AWS Service Catalog produits. Lorsque vous lancez un AWS Service Catalog produit, vous devez choisir TagOption des valeurs pour les TagOption clés existantes associées à ce portefeuille ou à ce produit afin de lancer ce produit. Comme vous le définissez TagOptions au niveau du portefeuille ou du produit, vous pouvez appliquer une taxonomie cohérente pour le balisage des portefeuilles partagés entre les comptes et les régions.

Pour plus d'informations sur la configuration TagOptions dansAWS Service Catalog, consultez la section AWS Service Catalog TagOption Bibliothèque.

Éviter les conflits entre les politiques relatives aux AWS Organizations balises et AWS Service Catalog TagOptions

Si vous configurez des politiques de AWS Organizations balises pour les comptes de votre organisation, nous vous recommandons ce qui suit :

- Partagez les exigences relatives aux balises conformes avec les administrateurs qui gèrent également TagOptions les AWS Service Catalog portefeuilles et les produits.
- Partagez les exigences relatives aux balises conformes avec les utilisateurs finaux susceptibles de lancer des produits AWS Service Catalog et d'ajouter des balises d'utilisateur final facultatives à leurs lancements de produits.

Supposons que vous souhaitiez lancer un produit utilisant la TagOption clé `city` et AWS Service Catalog que vous ayez une politique en matière de balises qui exige que les clés `city` de balise contiennent les valeurs de balise des villes américaines**`Atlanta`**, telles que**`San Francisco`**, ou**`Austin`**. AWS Service Catalogne vous permet pas de lancer un produit sans avoir sélectionné TagOption les valeurs des TagOption clés requises pour un produit.

Dans ce cas, si vous avez des TagOption valeurs pour la TagOption clé `city` qui incluent des villes d'Amérique du Sud, telles que **`Rio de Janeiro`** ou**`Buenos Aires`**, le produit ne AWS Service Catalog sera pas lancé. Vous devez plutôt sélectionner une TagOption valeur qui inclut une ville américaine lors du lancement afin de respecter la politique en matière de balises.

Le tableau suivant propose des scénarios qui décrivent comment résoudre les problèmes de conflit de balisage que vous pouvez rencontrer en même temps lorsque vous utilisez des TagOptions politiques de balises.

Scénario	Raison	Solution
Le produit ne démarre pas en raison de balises non conformes si le respect des balises est vérifié dans la politique en matière de balises.	Spécifier TagOptions à l'aide de clés et de valeurs que vous n'avez pas ajoutées à la liste autorisée des balises conformes dans votre politique en matière de balises. Ajout de balises personnal isées facultatives qui ne sont pas conformes à votre politique en matière de balises.	Si vous configurez un schéma de capitalisation spécifique dans le cadre de l'application de votre politique de balises en majuscules, assurez-vous que vos clés de TagOption s balise et vos clés de balise personnalisées facultatives sont conformes à ce que vous avez spécifié dans votre politique de balise. Notez que lorsque la case d'application de la mise en majuscule des clés de balise est décochée dans votre politique de balises, toutes les clés de balise en minuscules sont conformes et vos clés de balise et les

Scénario	Raison	Solution
		clés de TagOptions balise personnalisées facultatives sont cohérentes (par exemple toutes en minuscules) avec ce que vous avez exigé dans votre politique de balise.
Le produit ne peut pas être lancé en raison d'une capitalisation non conforme des clés de balise.	Spécifier une capitalisation dans les TagOptions clés qui est incompatible avec les règles d'application de votre politique en matière de balises en matière de majuscules.	Configurez correctement vos politiques en matière de balises. Si vous ne spécifiez pas la conformité de la clé de balise en majuscules, la capitalisation de la clé de balise par défaut est entièrement en minuscules. En outre, si vous ne spécifiez pas la conformité à la capitalisation des clés de balise dans votre politique en matière de balises, assurez-vous que vos clés de TagOptions balise AWS Service Catalog sont toutes en minuscules afin de respecter les règles d'application. Si vous utilisez une politique de balise pour laquelle la conformité aux majuscules n'est pas activée, cette politique de balise considère uniquement que toutes les clés de balise en minuscules sont conformes.

Scénario	Raison	Solution
Le produit ne démarre pas en raison de valeurs de balises incompatibles.	Sélection d'une valeur de TagOptions balise pour le lancement d'un produit qui ne figure pas dans la liste autorisée de conformité aux valeurs de balise de votre politique en matière de balises.	Associez TagOptions à vos produits et à vos portefeuilles des valeurs conformes à ce que vous avez exigé dans la politique des balises de liste. Valeurs de balise autorisées.

Moteurs externes pour AWS Service Catalog

Dans AWS Service Catalog, les moteurs externes sont représentés par un type de `EXTERNAL` produit. Le type de `EXTERNAL` produit permet l'intégration de moteurs de provisionnement tiers, tels que Terraform. Vous pouvez utiliser des moteurs externes pour étendre les fonctionnalités de Service Catalog au-delà des AWS CloudFormation modèles natifs, ce qui permet d'utiliser d'autres outils d'instructure en tant que code (IaC).

Le type de `EXTERNAL` produit vous permet de gérer et de déployer des ressources à l'aide de l'interface familière de Service Catalog tout en tirant parti des fonctionnalités et de la syntaxe spécifiques de l'outil IaC que vous avez choisi.

Pour activer les types de `EXTERNAL` produits dans Service Catalog, vous devez définir un ensemble de ressources standard dans votre compte. Ces ressources sont connues sous le nom de moteur. Service Catalog délègue des tâches au moteur à des moments spécifiques des opérations d'analyse et de provisionnement des artefacts.

Un artefact de provisionnement représente la version spécifique d'un produit dans Service Catalog, ce qui vous permet de gérer et de déployer des ressources cohérentes.

Lorsque vous appelez DescribeProvisioningArtifactou AWS Service Catalog effectuez DescribeProvisioningParametersdes opérations pour un artefact d'approvisionnement pour un type de `EXTERNAL` produit, Service Catalog invoque une AWS Lambda fonction dans le moteur. Cela est nécessaire pour extraire la liste des paramètres de l'artefact de provisionnement fourni et les renvoyer à. AWS Service Catalog Ces paramètres seront utilisés ultérieurement dans le cadre du processus de provisionnement.

Lorsque vous approvisionnez un artefact de `EXTERNAL` provisionnement en appelant ProvisionProduct, Service Catalog exécute d'abord certaines actions en interne, puis envoie un message à une file d'attente Amazon SQS dans le moteur. Ensuite, le moteur assume le rôle de lancement fourni (le rôle IAM que vous attribuez à un produit en tant que contrainte de lancement), provisionne les ressources en fonction de l'artefact de provisionnement fourni et invoque l'NotifyProvisionProductEngineWorkflowResultAPI pour signaler le succès ou l'échec.

Les appels vers UpdateProvisionedProductet TerminateProvisionedProductsont traités de la même manière, chacun ayant une file d'attente et des API de notification distinctes :

- NotifyProvisionProductEngineWorkflowResult
- NotifyUpdateProvisionedProductEngineWorkflowResult

- NotifyTerminateProvisionedProductEngineWorkflowResult.

Rubriques

Considérations

Limite d'un moteur externe par compte hub

Vous ne pouvez utiliser qu'un seul moteur de `EXTERNAL` provisionnement par compte du hub Service Catalog. Le hub-and-spokemodèle Service Catalog permet au compte hub de créer des produits de base et de partager le portefeuille, tandis que les comptes satellites importent des portefeuilles et tirent parti des produits.

Cette limite est due au fait que le routage ne `EXTERNAL` peut être effectué que vers un seul moteur par compte. Si un administrateur souhaite disposer de plusieurs moteurs externes, il doit configurer les moteurs externes (ainsi que les portefeuilles et les produits) dans différents comptes du hub.

Les moteurs externes ne prennent en charge que les rôles de lancement soumis à des contraintes de lancement

`EXTERNAL`les artefacts de provisionnement prennent uniquement en charge le provisionnement avec des rôles de lancement spécifiés à l'aide de contraintes de lancement. Une contrainte de lancement spécifie le rôle IAM assumé par Service Catalog lorsqu'un utilisateur final lance, met à jour ou met fin à un produit. Pour plus d'informations sur les contraintes de lancement, consultez la section Contraintes de AWS Service Catalog lancement.

Analyse des paramètres

`EXTERNAL`les artefacts de provisionnement peuvent être de n'importe quel format. Cela signifie que lors de la création d'un type de `EXTERNAL` produit, le moteur doit extraire la liste des paramètres de l'artefact de provisionnement fourni et les renvoyer à Service Catalog. Cela se fait en créant une

fonction Lambda dans votre compte capable d'accepter le format de demande suivant, de traiter l'artefact de provisionnement et de renvoyer le format de réponse suivant.

> **Important**
>
> La fonction Lambda doit être nommée. `ServiceCatalogExternalParameterParser`

Syntaxe de la demande :

```
{
    "artifact": {
        "path": "string",
        "type": "string"
    },
    "launchRoleArn": "string"
}
```

Champ	Type	Obligatoire	Description
artefact	objet	Oui	Détails de l'artefact à analyser.
artéfact/chemin	chaîne	Oui	Emplacement à partir duquel l'analyseur télécharge l'artefact. Par exemple, pour`AWS_S3`, il s'agit de l'URI Amazon S3.
artéfact/type	chaîne	Oui	Type d'artefact. Valeur autorisée :`AWS_S3`.
Rôle de lancement	chaîne	Non	Nom de ressource Amazon (ARN) du rôle de lancement à assumer lors du téléchargement de

Champ	Type	Obligatoire	Description
			l'artefact. Si aucun rôle de lancement n'est fourni, le rôle d'exécution du Lambda est utilisé.

Syntaxe de la réponse :

```
{
    "parameters": [
        {
            "key": "string"
            "defaultValue": "string",
            "type": "string",
            "description": "string",
            "isNoEcho": boolean
        },
    ]
}
```

Champ	Type	Obligatoire	Description
parameters	liste	Oui	Liste des paramètres que Service Catalog demande à l'utilisa teur final de fournir lors du provision nement d'un produit ou de la mise à jour d'un produit provisionné. Si aucun paramètre n'est défini dans l'artefac t, une liste vide est renvoyée.

Champ	Type	Obligatoire	Description
key	chaîne	Oui	Clé de paramètre.
defaultValue	chaîne	Non	La valeur par défaut du paramètre si l'utilisateur final ne fournit aucune valeur.
type	chaîne	Oui	Type attendu de la valeur de paramètre pour le moteur. Par exemple, une chaîne, un booléen ou une carte. Les valeurs autorisées sont spécifiques à chaque moteur. Service Catalog transmet chaque valeur de paramètre au moteur sous forme de chaîne.
description	chaîne	Non	Description du paramètre. Il est recommandé que cela soit convivial.
isNoEcho	booléen	non	Détermine si la valeur du paramètre n'est pas répercutée dans les journaux. La valeur par défaut est false (les valeurs des paramètres sont répercutées).

Allouer

Pour le ProvisionProductfonctionnement, Service Catalog délègue le provisionnement réel des ressources au moteur. Le moteur est chargé de l'interfaçage avec la solution IaC de votre choix (telle que Terraform) pour fournir les ressources telles que définies dans l'artefact. Le moteur est également chargé de notifier le résultat à Service Catalog.

Service Catalog envoie toutes les demandes de fourniture à une file d'attente Amazon SQS dans votre compte nommé. `ServiceCatalogExternalProvisionOperationQueue`

Syntaxe de la demande :

```
{
    "token": "string",
    "operation": "string",
    "provisionedProductId": "string",
    "provisionedProductName": "string",
    "productId": "string",
    "provisioningArtifactId": "string",
    "recordId": "string",
    "launchRoleArn": "string",
    "artifact": {
        "path": "string",
        "type": "string"
    },
    "identity": {
        "principal": "string",
        "awsAccountId": "string",
        "organizationId": "string"
    },
    "parameters": [
        {
            "key": "string",
            "value": "string"
        }
    ],
    "tags": [
        {
            "key": "string",
            "value": "string"
        }
    ]
```

```
}
```

Champ	Type	Obligatoire	Description
jeton	chaîne	Oui	Le jeton qui identifie cette opération. Le jeton doit être renvoyé à Service Catalog pour notifier les résultats de l'exécuti on.
fonctionnement	chaîne	Oui	Ce champ doit être `PROVISION _PRODUCT` réservé à cette opération.
provisionedProductId	chaîne	Oui	ID du produit approvisionné.
provisionedProduct Name	chaîne	Oui	Nom du produit approvisionné.
ID du produit	chaîne	Oui	Identifiant du produit.
provisioningArtifactId	chaîne	Oui	ID de l'artefact d'approvisionnement.
recordId	chaîne	Oui	ID de l'enregistrement Service Catalog pour cette opération.
launchRoleArn	chaîne	Oui	Amazon Resource Name (ARN) pour le rôle IAM à utiliser pour le provision nement des ressource s.

Champ	Type	Obligatoire	Description
artefact	objet	Oui	Détails de l'artefact qui définit la manière dont les ressources sont provisionnées.
artéfact/chemin	chaîne	Oui	Emplacement à partir duquel le moteur télécharge l'artefac t. Par exemple, pour`AWS_S3`, il s'agit de l'URI Amazon S3.
artéfact/type	chaîne	Oui	Type d'artefac t. Valeur autorisée :`AWS_S3`.
une	chaîne	Non	Le champ n'est actuellement pas utilisé.
parameters	liste	Oui	Liste des paires clé-valeur de paramètre s que l'utilisateur a saisies dans Service Catalog en tant qu'entrées pour cette opération.
balises	liste	Oui	Liste key-value-pairs des utilisateurs entrés dans Service Catalog sous forme de balises à appliquer aux ressources mises en service.

Notification des résultats du flux de travail :

Appelez l'NotifyProvisionProductEngineWorkflowResult API avec l'objet de réponse spécifié sur la page de détails de l'API.

Mise à jour

Pour l'UpdateProvisionedProductopération, Service Catalog délègue la mise à jour effective des ressources au moteur. Le moteur est chargé de l'interfaçage avec la solution IaC de votre choix (telle que Terraform) pour mettre à jour les ressources telles que définies dans l'artefact. Le moteur est également chargé de notifier le résultat à Service Catalog.

Service Catalog envoie toutes les demandes de mise à jour à une file d'attente Amazon SQS dans votre compte nommé. `ServiceCatalogExternalUpdateOperationQueue`

Syntaxe de la demande :

```
{
    "token": "string",
    "operation": "string",
    "provisionedProductId": "string",
    "provisionedProductName": "string",
    "productId": "string",
    "provisioningArtifactId": "string",
    "recordId": "string",
    "launchRoleArn": "string",
    "artifact": {
        "path": "string",
        "type": "string"
    },
    "identity": {
        "principal": "string",
        "awsAccountId": "string",
        "organizationId": "string"
    },
    "parameters": [
        {
            "key": "string",
            "value": "string"
        }
    ],
```

```
    "tags": [
        {
            "key": "string",
            "value": "string"
        }
    ]
}
```

Champ	Type	Obligatoire	Description
jeton	chaîne	Oui	Le jeton qui identifie cette opération. Le jeton doit être renvoyé à Service Catalog pour notifier les résultats de l'exécuti on.
fonctionnement	chaîne	Oui	Ce champ doit être `UPDATE_PR OVISION_P RODUCT` réservé à cette opération.
provisionedProductId	chaîne	Oui	ID du produit approvisionné.
provisionedProduct Name	chaîne	Oui	Nom du produit approvisionné.
ID du produit	chaîne	Oui	Identifiant du produit.
provisioningArtifactId	chaîne	Oui	ID de l'artefact d'approvisionnement.
recordId	chaîne	Oui	ID de l'enregistrement Service Catalog pour cette opération.

Champ	Type	Obligatoire	Description
launchRoleArn	chaîne	Oui	Amazon Resource Name (ARN) pour le rôle IAM à utiliser pour le provision nement des ressource s.
artefact	objet	Oui	Détails de l'artefact qui définit la manière dont les ressources sont provisionnées.
artéfact/chemin	chaîne	Oui	Emplacement à partir duquel le moteur télécharge l'artefac t. Par exemple, pour`AWS_S3`, il s'agit de l'URI Amazon S3.
artéfact/type	chaîne	Oui	Type d'artefac t. Valeur autorisée :`AWS_S3`.
une	chaîne	Non	Le champ n'est actuellement pas utilisé.
parameters	liste	Oui	Liste des paires clé-valeur de paramètre s que l'utilisateur a saisies dans Service Catalog en tant qu'entrées pour cette opération.

Champ	Type	Obligatoire	Description
balises	liste	Oui	Liste key-value-pairs des utilisateurs entrés dans Service Catalog sous forme de balises à appliquer aux ressources mises en service.

Notification des résultats du flux de travail :

Appelez l'NotifyUpdateProvisionedProductEngineWorkflowResultAPI avec l'objet de réponse spécifié sur la page de détails de l'API.

Résiliation

Pour l'TerminateProvisionedProductopération, Service Catalog délègue la mise hors service effective des ressources au moteur. Le moteur est chargé de l'interfaçage avec la solution IaC de votre choix (telle que Terraform) pour mettre fin aux ressources telles que définies dans l'artefact. Le moteur est également chargé de notifier le résultat à Service Catalog.

Service Catalog envoie toutes les demandes de résiliation à une file d'attente Amazon SQS nommée dans votre compte. `ServiceCatalogExternalTerminateOperationQueue`

Syntaxe de la demande :

```
{
    "token": "string",
    "operation": "string",
    "provisionedProductId": "string",
    "provisionedProductName": "string",
    "recordId": "string",
    "launchRoleArn": "string",
    "identity": {
        "principal": "string",
        "awsAccountId": "string",
        "organizationId": "string"
    }
```

```
}
```

Champ	Type	Obligatoire	Description
jeton	chaîne	Oui	Le jeton qui identifie cette opération. Le jeton doit être renvoyé à Service Catalog pour notifier les résultats de l'exécuti on.
fonctionnement	chaîne	Oui	Ce champ doit être `TERMINATE _PROVISIO N_PRODUCT` réservé à cette opération.
provisionedProductId	chaîne	Oui	ID du produit approvisionné.
provisionedProduct Name	chaîne	Oui	Nom du produit approvisionné.
recordId	chaîne	Oui	ID de l'enregistrement Service Catalog pour cette opération.
launchRoleArn	chaîne	Oui	Amazon Resource Name (ARN) pour le rôle IAM à utiliser pour le provision nement des ressource s.

Champ	Type	Obligatoire	Description
une	chaîne	Non	Le champ n'est actuellement pas utilisé.

Notification des résultats du flux de travail :

Appelez l'NotifyTerminateProvisionedProductEngineWorkflowResultAPI avec l'objet de réponse spécifié sur la page de détails de l'API.

Identification

Pour gérer les tags via Resource Groups, votre rôle de lancement a besoin des déclarations d'autorisation supplémentaires suivantes :

```
{
    "Effect": "Allow",
    "Action": [
        "resource-groups:CreateGroup",
        "resource-groups:ListGroupResources"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "tag:GetResources",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:TagResources",
        "tag:UntagResources"
    ],
    "Resource": "*"
}
```

> **Note**
>
> Le rôle de lancement nécessite également des autorisations de balisage sur les ressources spécifiques de l'artefact, telles que. `ec2:CreateTags`

Surveillance dans AWS Service Catalog

Vous pouvez surveiller vos AWS Service Catalog ressources à l'aide d'Amazon CloudWatch, qui collecte et traite les données brutes sous forme AWS Service Catalog de métriques lisibles. Ces statistiques sont enregistrées pour une durée de deux semaines. Vous pouvez donc accéder aux informations historiques et mieux comprendre la façon dont votre service fonctionne. Les données de métrique AWS Service Catalog sont automatiquement envoyées à CloudWatch toutes les minutes. Pour plus d'informations CloudWatch, consultez le guide de CloudWatch l'utilisateur Amazon.

Pour obtenir une liste des métriques et des dimensions disponibles, consultez AWS Service Catalog CloudWatch Métriques.

La surveillance est un enjeu important pour assurer la fiabilité, la disponibilité et les performances d'AWS Service Catalog et de vos solutions AWS. Vous devez recueillir les données de surveillance de toutes les parties de votre solution AWS de telle sorte que vous puissiez déboguer plus facilement un éventuelle défaillance multipoint. Avant de commencer la surveillance de AWS Service Catalog, vous devez créer un plan de surveillance qui contient les réponses aux questions suivantes :

- Quels sont les objectifs de la surveillance ?
- Quelles sont les ressources à surveiller ?
- À quelle fréquence les ressources doivent-elles être surveillées ?
- Quels outils de surveillance utiliser ?
- Qui exécute les tâches de supervision ?
- Qui doit être informé en cas de problème ?

Outils de supervision

AWS fournit différents outils que vous pouvez utiliser pour surveiller AWS Service Catalog. Vous pouvez configurer certains outils pour qu'ils effectuent la supervision automatiquement, tandis que d'autres nécessitent une intervention manuelle. Nous vous recommandons d'automatiser le plus possible les tâches de supervision.

Outils de surveillance automatique

Vous pouvez utiliser les CloudWatch alarmes Amazon pour surveiller AWS Service Catalog et signaler les perturbations.

CloudWatch les alarmes surveillent une seule métrique sur une période que vous spécifiez et exécutent une ou plusieurs actions en fonction de la valeur de la métrique par rapport à un seuil donné sur un certain nombre de périodes. L'action est une notification envoyée à une rubrique Amazon Simple Notification Service (Amazon SNS) ou à une politique Amazon EC2 Auto Scaling. CloudWatch les alarmes n'appellent pas d'actions simplement parce qu'elles sont dans un état particulier ; l'état doit avoir changé et être maintenu pendant un certain nombre de périodes. Pour savoir comment créer une alarme, consultez Creating Amazon CloudWatch Alarms. Pour plus d'informations sur l'utilisation CloudWatch des métriques Amazon avecAWS Service Catalog, consultezAWS Service Catalog CloudWatch Métriques.

AWS Service Catalog CloudWatch Métriques

Vous pouvez surveiller vos AWS Service Catalog ressources à l'aide d'Amazon CloudWatch, qui collecte et traite les données brutes sous forme AWS Service Catalog de métriques lisibles. Ces statistiques sont enregistrées pour une durée de deux semaines. Vous pouvez donc accéder aux informations historiques et mieux comprendre la façon dont votre service fonctionne. Les données de métrique AWS Service Catalog sont automatiquement envoyées à CloudWatch toutes les minutes. Pour plus d'informations CloudWatch, consultez le guide de CloudWatch l'utilisateur Amazon.

Rubriques

- Activation CloudWatch des métriques
- Métriques et dimensions disponibles
- Affichage des métriques AWS Service Catalog

Activation CloudWatch des métriques

Les CloudWatch métriques Amazon sont activées par défaut.

Métriques et dimensions disponibles

Les statistiques et les dimensions AWS Service Catalog envoyées à Amazon CloudWatch sont répertoriées ci-dessous.

AWS Service Catalog Métriques

L'espace de noms `AWS/ServiceCatalog` inclut les métriques suivantes.

Métrique	Description
`ProvisionedProductLaunch`	Nombre de produits provisionnés lancés pour un produit donné et un artefact de provisionnement à un moment précis dans le temps. Unités : nombre Statistiques valides : minimum, maximum, somme, moyenne

Dimensions pour les métriques AWS Service Catalog

AWS Service Catalogenvoie les dimensions suivantes à Amazon CloudWatch.

Dimension	Description
`State`	Cette dimension filtre les données que vous demandez pour tous les produits provisionnés lancés avec l'état spécifié. Cela vous permet de classer vos données en fonction de l'état du lancement. États valides : SUCCEEDED (succès), FAILED (échec)
`ProductId`	Cette dimension filtre les données que vous demandez uniquement pour l'ID de produit identifié. Cela vous permet de sélectionner plus facilement le produit exact à partir duquel effectuer le lancement.
`ProvisioningArtifactId`	Cette dimension filtre les données que vous demandez uniquement pour l'ID d'artefact de provisionnement identifié. Cela vous permet de sélectionner plus facilement la version exacte des produits à partir desquels effectuer le lancement.

Affichage des métriques AWS Service Catalog

Vous pouvez consulter CloudWatch les statistiques Amazon dans la CloudWatch console Amazon, qui fournit un affichage détaillé et personnalisable de vos ressources, ainsi que du nombre de tâches en cours dans un service.

Rubriques

Afficher AWS Service Catalog les métriques dans la CloudWatch console Amazon

Vous pouvez consulter AWS Service Catalog les statistiques dans la CloudWatch console Amazon. La CloudWatch console Amazon fournit une vue détaillée des AWS Service Catalog statistiques, que vous pouvez personnaliser en fonction de vos besoins. Pour plus d'informations sur Amazon CloudWatch, consultez le guide de CloudWatch l'utilisateur Amazon.

Pour consulter les statistiques dans la CloudWatch console Amazon

1. Ouvrez la CloudWatch console Amazon à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans la section Métriques du volet de navigation de gauche, choisissez Catalogue des services.
3. Choisissez les métriques à afficher.

Journalisation des appels d'API AWS Service Catalog avec AWS CloudTrail

AWS Service Catalogest intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dansAWS Service Catalog. CloudTrail capture tous les appels d'API AWS Service Catalog sous forme d'événements. Les appels capturés incluent des appels de la console AWS Service Catalog et les appels de code vers les opérations d'API AWS Service Catalog. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris les événements pourAWS Service Catalog. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faiteAWS

Service Catalog, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour en savoir plus CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

AWS Service Cataloginformations dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité se produit dansAWS Service Catalog, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez afficher, rechercher et télécharger les événements récents dans votre compte AWS. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour enregistrer en continu les événements dans votre compte AWS, y compris les événements d'AWS Service Catalog, créez un journal d'activité. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal d'activité dans la console, il s'applique à toutes les régions Régions AWS. Le journal de suivi consigne les événements de toutes les régions dans la partition AWS et livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour en savoir plus, consultez les ressources suivantes :

- Présentation de la création d'un journal de suivi
- Intégrations et services pris en charge par AWS CloudTrail
- Configuration des notifications Amazon SNS pour AWS CloudTrail
- Réception de fichiers journaux AWS CloudTrail de plusieurs régions et Réception de fichiers journaux AWS CloudTrail de plusieurs comptes

CloudTrail enregistre toutes les AWS Service Catalog actions. Par exemple, les appels au `CreatePortfolio` `CreateProduct` et les `UpdateProvisionedProduct` actions génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou AWS Identity and Access Management (IAM).

- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été effectuée par un autre service AWS.

Pour de plus amples informations, veuillez consulter l'élément userIdentity CloudTrail .

Présentation des entrées des fichiers journaux AWS Service Catalog

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique. L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`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"
}
```

Préférences de marque de la console

AWS Service Catalogpermet aux administrateurs de définir les préférences de personnalisation de la console pour les comptes. Les administrateurs peuvent utiliser l'image de marque de la console pour spécifier le nom de l'entreprise, l'image du logo et une couleur principale et secondaire (accent) pour divers composants du site. Ces préférences de marque sont visibles à la fois par les administrateurs et les utilisateurs finaux lorsqu'ils utilisent la console.

Les préférences relatives à l'image de marque de la console améliorent l'apparence d'un compte et permettent d'accomplir les tâches suivantes :

- Crée une transition visuelle fluide entre la console et les applications internes
- Distingue les comptes utilisés par les différentes équipes internes d'une même entreprise
- Permet de différencier les comptes dans plusieurs environnements, tels que le développement, la mise en scène ou la production

> **Note**
>
> Les administrateurs définissent les préférences relatives à l'image de marque de la console au niveau du compte.

Pour définir les préférences de marque de la console

1. Dans le menu de navigation de gauche, sélectionnez Préférences.
2. Choisissez Modifier pour les préférences de marque en mode clair ou en mode sombre.
3. Téléchargez un logo, entrez un nom de marque, puis sélectionnez la couleur principale et la couleur secondaire.
4. Choisissez Enregistrer.

Pour obtenir la liste des régions où l'image de marque des consoles est prise AWS Service Catalog en charge, consultez la section Région AWSAssistance relative à l'image de marque des consoles.

Région AWSprise en charge des préférences de marque de la console

AWS Service Catalogprend en charge les préférences de personnalisation de la console Régions AWS répertoriées dans le tableau ci-dessous.

Nom de l'Région AWS	Identité Région AWS
US East (Virginie du Nord)	us-east-1
USA Est (Ohio)	us-east-2
USA Ouest (Californie du Nord)	us-west-1
US West (Oregon)	us-west-2
Afrique (Le Cap)	af-south-1
Asie-Pacifique (Hong Kong)	ap-east-1
Asie-Pacifique (Jakarta)	ap-southeast-3
Asie-Pacifique (Mumbai)	ap-south-1
Asie-Pacifique (Osaka)	ap-northeast-3
Asie-Pacifique (Séoul)	ap-northeast-2
Asie-Pacifique (Singapour)	ap-southeast-1
Asie-Pacifique (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Canada (Central)	ca-central-1
Europe (Francfort)	eu-central-1
Europe (Irlande)	eu-west-1
Europe (Londres)	eu-west-2

Nom de l'Région AWS	Identité Région AWS
Europe (Milan)	eu-south-1
Europe (Paris)	eu-west-3
Europe (Stockholm)	eu-north-1
Moyen-Orient (Bahreïn)	me-south-1
Amérique du Sud (São Paulo)	sa-east-1
AWS GovCloud (USA Est)	us-gov-east-1
AWS GovCloud (US-Ouest)	us-gov-west-1

Historique du document

Le tableau suivant décrit les modifications importantes apportées à la documentation de AWS Service Catalog. Pour recevoir les notifications de mise à jour de cette documentation, abonnez-vous à un flux RSS.

- Version de l'API : 2014-11-12
- Dernière mise à jour de la documentation : 16 mai 2024

Modification	Description	Date
Moteurs externes pour AWS Service Catalog	AWS Service Catalog ajoute une nouvelle documentation pour les moteurs externes. Les moteurs externes sont représentés par un type de `EXTERNAL` produit. Le type de `EXTERNAL` produit permet l'intégration de moteurs de provisionnement tiers, tels que Terraform. Vous pouvez utiliser des moteurs externes pour étendre les fonctionn alités de Service Catalog au-delà des AWS CloudForm ation modèles natifs, ce qui permet d'utiliser d'autres outils d'instructure en tant que code (IaC). Pour plus d'informations, consultez la section Moteurs externes pour AWS Service Catalog.	16 mai 2024
Mise à jour de sécurité IAM	AWS Service Catalog met à jour la `AWSServic eCatalogSyncServic`	7 mai 2024

	`eRolePolicy` politique pour la `codestar-connections` remplacer par`codeconnections` . Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Service Catalog AppRegistry.	

Mises à jour antérieures

Le tableau suivant décrit l'historique des publications de documentation AWS Service Catalog antérieures au 25 avril 2024.

Fonctionnalité	Description	Date de publication
AWS Service Catalog	Pour en savoir plus sur les modifications apportées par Hashicorp aux licences Terraform et la mise à jour du type de produit externe, consultez. Mise à jour des produits Open Source Terraform existants et des produits fournis vers le type de produit externe	20 octobre 2023
AWS Service Catalog	Pour en savoir plus sur le partage d'un portefeuille AWS Organizations et sur l'autorisation AWS Service Catalog de synchronisation avec celui-ci AWS Organizations, consultez la AWSServiceCatalogOrgsDataSyncServiceRolePolicypolitique	14 avril 2023

Fonctionnalité	Description	Date de publication
	et le rôle AWSServiceRoleForServiceCatalogOrgsDataSynclié au service.	
AWS Service Catalog	Pour en savoir plus sur la gestion des produits connectés AWS Service Catalog à Git et sur l'autorisation de synchroniser les modèles d'un référentiel externe avec vos AWS Service Catalog produits, consultez la AWSServiceCatalogSyncServiceRolePolicypolitique et le rôle lié au AWSServiceRoleForServiceCatalogSyncservice.	18 novembre 2022
AWS Service Catalog AppRegistry	Pour en savoir plus sur la AppRegistry manière dont vous pouvez stocker vos AWS applications, leurs collections de ressources associées et les groupes d'attributs d'applications, consultez AWS Service Catalog AppRegistry.	15 juin 2022
Connecteur AWS Service Management	Pour en savoir plus sur les connecteurs pour Jira Service Management et ServiceNow consultez la section Connecteur AWS de gestion des services.	9 juin 2022

Fonctionnalité	Description	Date de publication
Connecteur pour Jira Service Management	Pour en savoir plus sur les mises à jour apportées au connecteur pour Jira Service Management, voir Connecteur de gestion des AWS services pour Jira Service Management.	25 mai 2021
Connecteur pour ServiceNow	Pour en savoir plus sur les mises à jour apportées au connecteur pour ServiceNow, consultez la section Connecteur de gestion des AWS services pour ServiceNow.	7 avril 2021
Connecteur pour ServiceNow	Pour en savoir plus sur les mises à jour apportées au connecteur pour ServiceNow, consultez la section Connecteur de gestion des AWS services pour ServiceNow.	24 septembre 2020
AWS Quotas de service	Pour en savoir plus sur le AWS Service Catalog fonctionnement des quotas de AWS service, consultez la section Quotas de service AWS Service Catalog par défaut.	24 mars 2020

Fonctionnalité	Description	Date de publication
Bibliothèque de mise en route	Pour en savoir plus sur la bibliothèque de modèles de produits bien architecturés proposée par AWS Service Catalog, voir Bibliothèque de mise en route	10 mars 2020
Guide de version	Pour en savoir plus sur les directives relatives aux versions des produits, consultez les instructions relatives aux versions.	17 décembre 2019
Connecteur pour Jira Service Desk	Pour commencer à utiliser le connecteur pour Jira Service Desk, voir Connecteur de gestion des AWS services pour Jira Service Desk.	21 novembre 2019
Connecteur pour ServiceNow	Pour en savoir plus sur les mises à jour apportées au connecteur pour ServiceNow, consultez la section Connecteur de gestion des AWS services pour ServiceNow.	18 novembre 2019
Nouveau chapitre sur la sécurité	Pour en savoir plus sur la sécurité dans AWS Service Catalog, voir Sécurité dans AWS Service Catalog.	31 octobre 2019

Fonctionnalité	Description	Date de publication
Changer le propriétaire du produit provisionné	Pour savoir comment modifier le propriétaire des produits approvisionnés, voir Changer le propriétaire du produit provisionné.	31 octobre 2019
Nouvelle contrainte de mise à jour des ressources	Pour savoir comment utiliser la contrainte RESOURCE_UPDATE pour mettre à jour les balises dans les produits provisionnés, consultez AWS Service Catalog la section Contraintes de mise à jour des balises.	17 avril 2019
Connecteur pour ServiceNow	Pour commencer à utiliser le connecteur pour ServiceNow, voir Connecteur AWS de gestion des services pour ServiceNow.	19 mars 2019
Support pour AWS CloudFormation StackSets	Pour commencer à utiliser AWS CloudFormation StackSets, voir Utilisation AWS CloudFormation StackSets.	14 novembre 2018
Actions en libre-service	Pour commencer à utiliser les actions en libre-service, consultez la section Actions AWS CloudFormation de service.	17 octobre 2018

Fonctionnalité	Description	Date de publication
CloudWatch Métriques Amazon	Pour en savoir plus sur CloudWatch les statistiques Amazon, consultez AWS Service CatalogAmazon CloudWatch.	26 septembre 2018
Support pour TagOptions	Pour gérer les balises, consultez la section AWS Service Catalog TagOption Bibliothèque.	28 juin 2017
Importation d'un portefeuille	Pour importer un portefeuille partagé depuis un autre AWS compte, consultez la section Importation d'un portefeuille.	16 février 2016
Informations sur les autorisations mises à jour	Pour accorder l'accès à la vue de la console à l'utilisateur final, consultez la section Accès à la console pour les utilisateurs finaux.	16 février 2016
Première version	Il s'agit de la version initiale du guide de AWS Service Catalog l'administrateur.	9 juillet 2015

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.