POST EDIT. ADDED PROOFREAD. ADDED PP1

AWS Service Catalog

AWS Service Catalog: POST EDIT. ADDED PROOFREAD. ADDED PP1

Table of Contents

Was ist Service Catalog? 1
Video: Einführung in AWS Service Catalog 2
Übersicht 2
Benutzer 2
Produkte 3
HashiCorp Unterstützung für Terraform Open Source und Terraform Cloud 3
Bereitgestellte Produkte 3
Portfolios 4
Versionsverwaltung 4
Berechtigungen 4
Beschränkungen 5
Anfänglicher Administrator-Workflow 5
Anfänglicher Endbenutzer-Workflow 6
Kontingente 6
AWS Organizations 7
Kontingente für Einschränkungen 7
Portfoliokontingente 7
Produktkontingente 7
Kontingente für bereitgestellte Produkte 7
Regionale Kontingente 7
Kontingente für Service-Aktionen 8
TagOptions -Kontingente 8
Einrichten 9
..... 9
Melden Sie sich an für eine AWS-Konto 9
Erstellen Sie einen Benutzer mit Administratorzugriff 9
Erteilen von Berechtigungen für Administratoren 11
Endbenutzern Berechtigungen erteilen 14
Installieren und Konfigurieren der Terraform-Bereitstellungs-Engine 15
Bestimmung der Warteschlange 15
Hinzufügen von Confused Deputy zu Ihrer Terraform-Bereitstellungs-Engine 16
Erste Schritte 20
Bibliothek „Erste Schritte“ 20
Voraussetzungen 21

Weitere Informationen 21
Erste Schritte mit einem -AWS CloudFormationProdukt 21
Schritt 1: Herunterladen der Vorlage 22
Schritt 2: Erstellen eines Schlüsselpaares 27
Schritt 3: Erstellen eines Portfolios 28
Schritt 4: Erstellen eines neuen Produkts im Portfolio 28
Schritt 5: Fügen Sie eine Vorlagenbeschränkung hinzu 29
Schritt 6: Hinzufügen einer Starteinschränkung 30
Schritt 7: Endbenutzern Zugriff auf das Portfolio gewähren 33
Schritt 8: Testen der Endbenutzererfahrung 34
Erste Schritte mit einem Terraform-Produkt 35
Aktualisieren auf den externen Produkttyp 37
Voraussetzung: Konfigurieren Ihrer Terraform-Bereitstellungs-Engine 38
Schritt 1: Herunterladen der Terraform-Konfigurationsdatei 39
Schritt 2: Erstellen eines Terraform-Produkts 40
Schritt 3: Erstellen eines Portfolios 42
Schritt 4: Hinzufügen eines Produkts zum Portfolio 42
Schritt 5: Erstellen von Startrollen 43
Schritt 6: Hinzufügen einer Starteinschränkung 47
Schritt 7: Endbenutzerzugriff gewähren 48
Schritt 8: Freigeben des Portfolios für Endbenutzer 49
Schritt 9: Testen der Endbenutzererfahrung 50
Schritt 10: Überwachen von Terraform-Bereitstellungsvorgängen 50
Sicherheit 52
Datenschutz 53
Datenschutz durch Verschlüsselung 54
Identitäts- und Zugriffsverwaltung 54
Zielgruppe 55
Beispiele für identitätsbasierte Richtlinien für AWS Service Catalog 55
AWS verwaltete Richtlinien 61
Verwenden von serviceverknüpften Rollen 72
Problembehandlung bei AWS Service Catalog Identität und Zugriff 77
Zugriffssteuerung 79
Protokollieren und Überwachen 80
Compliance-Validierung 80
Ausfallsicherheit 81

Sicherheit der Infrastruktur 82
Bewährte Methoden für die Sicherheit 83
Verwalten von Katalogen 84
Verwalten von Portfolios 84
Erstellen, Anzeigen und Löschen von Portfolios 85
Anzeigen von Portfoliodetails 85
Erstellen und Löschen von Portfolios 85
Hinzufügen von Produkten 86
Hinzufügen von Einschränkungen 89
Gewähren des Zugriffs für Benutzer 90
Freigeben eines Portfolios 91
Freigeben und Importieren von Portfolios 99
Verwalten von Produkten 104
Anzeigen der Produktseite 104
Erstellen von Produkten 105
Hinzufügen von Produkten zu Portfolios 108
Aktualisieren von Produkten 109
Produkte mit Vorlagendateien aus externen Repositorys synchronisieren 110
Löschen von Produkten 119
Verwalten von Versionen 127
Verwenden von Einschränkungen 129
Starteinschränkungen 129
Benachrichtigungseinschränkungen 135
Einschränkungen für die Tag-Aktualisierung 136
Stack-Set-Einschränkungen 137
Vorlageneinschränkungen 138
Verwenden von Service-Aktionen 143
Voraussetzungen 143
Schritt 1: Konfigurieren von Berechtigungen für Endbenutzer 144
Schritt 2: Erstellen einer Service-Aktion 145
Schritt 3: Verknüpfen der Service-Aktion mit einer Produktversion 146
Schritt 4: Testen der Endbenutzerumgebung 147
Schritt 5: Verwalten von Service-Aktionen mit AWS CloudFormation 147
Schritt 6: Fehlerbehebung 148
Hinzufügen von AWS Marketplace-Produkten zu Ihrem Portfolio 150
Verwalten von AWS Marketplace-Produkten mithilfe von AWS Service Catalog 151

Verwalten und manuelles Hinzufügen von AWS Marketplace-Produkten 151
Verwenden von AWS CloudFormation StackSets 156
Stack-Sets und Stack-Instances 157
Stack-Set-Einschränkungen 157
Verwalten von Budgets 157
Voraussetzungen 158
Erstellen eines Budgets 159
Ein Budget zuordnen 160
Ein Budget anzeigen 161
Die Zuordnung eines Budgets aufheben 162
Verwalten von bereitgestellten Produkten 163
Verwalten von bereitgestellten Produkten als Administrator 163
Ändern des Besitzers des bereitgestellten Produkts 164
Weitere Informationen finden Sie unter: 165
Aktualisieren von Vorlagen für bereitgestellte Produkte 165
Tutorial: Identifizieren der Benutzerressourcenzuordnung 166
Verwalten von Terraform-Open-Source-Produktstatusfehlern 170
Beispiele für Statusfehler 170
Verwalten der Terraform-Open-Source-Produktstatusdatei 171
Verwalten von Tags 173
AutoTags 173
TagOption Bibliothek 174
Starten eines Produkts mit TagOptions 176
Verwalten von TagOptions 180
Verwenden von TagOptions mit AWS Organizations Tag-Richtlinien 182
Externe Motoren 187
Überlegungen 188
Parsen von Parametern 188
Bereitstellung 192
Aktualisieren 195
Wird beendet 199
Tagging 201
Überwachen 202
Überwachungstools 202
Automatisierte Tools 203
CloudWatch Metriken 203

Aktivieren von CloudWatch Metriken 203
Verfügbare Metriken und Dimensionen 204
Anzeigen von AWS Service Catalog-Metriken 205
CloudTrail -Protokolle 205
AWS Service Catalog -Informationen in CloudTrail 206
Grundlagen zu AWS Service Catalog-Protokolldateieinträgen 207
Konsolen-Branding 209
AWS-Region -Unterstützung für Konsolen-Branding 210
Dokumentverlauf 212
Frühere Aktualisierungen 213
..... ccxix

Was ist Service Catalog?

Service Catalog ermöglicht es Organisationen, Kataloge von IT-Services zu erstellen und zu verwalten, die für genehmigt sindAWS. Diese IT-Services können alles umfassen, von Images virtueller Maschinen, Servern, Software, Datenbanken und mehr bis hin zu mehrstufigen Anwendungsarchitekturen.

Service Catalog ermöglicht es Organisationen, häufig bereitgestellte IT-Services zentral zu verwalten, und hilft Unternehmen, eine konsistente Governance zu erreichen und die Compliance-Anforderungen zu erfüllen. Endbenutzer können schnell nur die jeweils benötigten genehmigten IT-Services bereitstellen, wobei die Einschränkungen Ihrer Organisation berücksichtigt werden.

Service Catalog bietet die folgenden Vorteile:

- Standardisierung

  Verwalten Sie genehmigte Komponenten, indem Sie einschränken, wo das Produkt gestartet werden kann und welcher Instance-Typ verwendet werden kann. Außerdem stehen viele weitere Konfigurationsoptionen zur Verfügung. Das Ergebnis ist eine standardisierte Umgebung für die Produktbereitstellung für Ihre gesamte Organisation.
- Self-Service-Erkennung und Start

  Benutzer durchsuchen Produktangebote (Services oder Anwendungen), auf die sie Zugriff haben, um das gewünschte Produkt zu finden und es eigenständig als bereitgestelltes Produkt zu starten.
- Differenzierte Zugriffskontrolle

  Administratoren stellen Portfolios von Produkten aus ihrem Katalog zusammen, fügen Einschränkungen und Ressourcen-Tags hinzu, die bei der Bereitstellung verwendet werden sollen, und gewähren dann über AWS Identity and Access Management (IAM)-Benutzer und -Gruppen Zugriff auf das Portfolio.
- Erweiterbarkeit und Versionskontrolle

  Administratoren können ein Produkt einer beliebigen Anzahl von Portfolios hinzufügen und es einschränken, ohne eine weitere Kopie zu erstellen. Durch ein Update auf eine neue Produktversion werden alle Produkte in jedem Portfolio, auf das es verweist, aktualisiert.

Weitere Informationen finden Sie auf der Detailseite zum Service Catalog .

Die Service-Catalog-API bietet als Alternative zur Verwendung der programmgesteuerte Kontrolle über alle EndbenutzeraktionenAWS Management Console. Weitere Informationen finden Sie im Service-Catalog-Entwicklerhandbuch.

Video: Einführung in AWS Service Catalog

In diesem Video (7:27) wird beschrieben, wie Sie einen kuratierten AWS Produktkatalog erstellen, organisieren und verwalten und Produkte mit Berechtigungsstufe teilen. Dadurch können Endbenutzer schnell genehmigte IT-Ressourcen bereitstellen, ohne direkten Zugriff auf die zugrunde liegenden AWS Services zu haben.

Einführung in AWS Service Catalog

Übersicht über Service Catalog

Bei den ersten Schritten mit Service Catalog profitieren Sie davon, die Komponenten und die ersten Workflows für Administratoren und Endbenutzer zu verstehen.

Benutzer

Service Catalog unterstützt die folgenden Arten von Benutzern:

- Katalogadministratoren (Administratoren) – Verwalten Sie einen Katalog von Produkten (Anwendungen und Services), organisieren Sie sie in Portfolios und gewähren Sie Endbenutzern Zugriff. Katalogadministratoren bereiten AWS CloudFormation Vorlagen vor, konfigurieren Einschränkungen und verwalten IAM-Rollen für -Produkte, um ein erweitertes Ressourcenmanagement bereitzustellen.
- Endbenutzer – Erhalten Sie AWS Anmeldeinformationen von ihrer IT-Abteilung oder ihrem Manager und verwenden Sie die , AWS Management Console um Produkte zu starten, auf die sie Zugriff erhalten haben. Endbenutzer, die manchmal einfach als Benutzer bezeichnet werden, können je nach betrieblichen Anforderungen verschiedene Berechtigungen erhalten. Ein Benutzer kann z. B. über die maximale Berechtigungsebene (zum Starten und Verwalten aller Ressourcen, die für die von ihnen verwendeten Ressourcen erforderlich sind) verfügen oder nur berechtigt sein, bestimmte Service-Funktionen zu verwenden.

Produkte

Ein -Produkt ist ein IT-Service, den Sie für die Bereitstellung in zur Verfügung stellen möchtenAWS. Ein Produkt besteht aus einer oder mehreren AWS Ressourcen, wie EC2-Instances, Speicher-Volumes, Datenbanken, Überwachungskonfigurationen und Netzwerkkomponenten oder verpackten AWS Marketplace Produkten. Ein Produkt kann eine einzelne Rechen-Instance sein, auf der AWS Linux ausgeführt wird, eine vollständig konfigurierte mehrstufige Webanwendung, die in einer eigenen Umgebung ausgeführt wird, oder alles dazwischen.

Sie erstellen ein Produkt, indem Sie eine -AWS CloudFormationVorlage importieren. -AWS CloudFormationVorlagen definieren die für das Produkt erforderlichen AWS Ressourcen, die Beziehungen zwischen Ressourcen und die Parameter, die Endbenutzer beim Starten des Produkts verwenden können, um Sicherheitsgruppen zu konfigurieren, Schlüsselpaare zu erstellen und andere Anpassungen durchzuführen.

HashiCorp Unterstützung für Terraform Open Source und Terraform Cloud

AWS Service Catalog ermöglicht eine schnelle Self-Service-Bereitstellung mit Governance für Ihre HashiCorp Terraform-Open-Source- und Terraform-Cloud-Konfigurationen in AWS. Sie können Service Catalog als ein einziges Tool verwenden, um Ihre Terraform-Konfigurationen in großem Umfang innerhalb von zu organisieren, zu verwalten und zu verteilenAWS. Sie können auf die wichtigsten Funktionen von Service Catalog zugreifen, einschließlich der Katalogisierung standardisierter und vorab genehmigter Terraform-Vorlagen, der Zugriffskontrolle, der Bereitstellung mit den geringsten Berechtigungen, der Versionsverwaltung, der Markierung und der Freigabe für Tausende von AWS Konten. Ihre Endbenutzer sehen eine einfache Liste der Produkte und Versionen, auf die sie Zugriff haben, und können diese Produkte dann in einer einzigen Aktion bereitstellen.

Weitere Informationen und ein Terraform-Produkt-Tutorial finden Sie unter Erste Schritte mit einem Terraform-Produkt.

Bereitgestellte Produkte

AWS CloudFormation -Stacks erleichtern die Verwaltung des Lebenszyklus Ihres Produkts, da Sie Ihre Produkt-Instance als eine Einheit bereitstellen, markieren, aktualisieren und beenden können. Ein AWS CloudFormation-Stack umfasst eine AWS CloudFormation-Vorlage entweder im JSON- oder YAML-Format sowie die zugehörige Sammlung von Ressourcen. Ein bereitgestelltes Produkt ist ein Stack. Wenn ein Endbenutzer ein Produkt startet, ist die Instance des Produkts, die von

Service Catalog bereitgestellt wird, ein Stack mit den Ressourcen, die zum Ausführen des Produkts erforderlich sind. Weitere Informationen finden Sie im AWS CloudFormation-Benutzerhandbuch.

Portfolios

Ein Portfolio ist eine Sammlung von Produkten, die Konfigurationsinformationen enthalten. Portfolios erleichtern das Verwalten der zulässigen Benutzer und Nutzungsarten bestimmter Produkte. Mit Service Catalog können Sie ein angepasstes Portfolio für jeden Benutzertyp in Ihrer Organisation erstellen und selektiv Zugriff auf das entsprechende Portfolio gewähren. Wenn Sie eine neue Version eines Produkts oder Portfolios hinzufügen, so ist diese automatisch für alle aktuellen Benutzer verfügbar.

Sie können Ihre Portfolios auch für andere AWS Konten freigeben und dem Administrator dieser Konten erlauben, Ihre Portfolios mit zusätzlichen Einschränkungen zu verteilen, z. B. um einzuschränken, welche EC2-Instances ein Benutzer erstellen kann. Durch die Nutzung von Portfolios, Berechtigungen, Freigaben und Einschränkungen können Sie sicherstellen, dass Benutzer nur Produkte starten, die ordnungsgemäß für die Anforderungen und Standards der Organisation konfiguriert sind.

Versionsverwaltung

Mit Service Catalog können Sie mehrere Versionen der Produkte in Ihrem Katalog verwalten. Mit diesem Ansatz können Sie neue Versionen von Vorlagen und zugehörige Ressourcen basierend auf Softwareupdates oder Konfigurationsänderungen hinzufügen.

Wenn Sie eine neue Version eines Produkts erstellen, wird das Update automatisch an alle Benutzer verteilt, die Zugriff auf das Produkt haben. Die Benutzer können auswählen, welche Version des Produkts sie verwenden möchten. Das Update laufender Produktinstanzen auf die neue Version ist für Benutzer schnell und einfach.

Berechtigungen

Ein Benutzer, dem Zugriff auf ein Portfolio gewährt wird, kann das Portfolio durchsuchen und die darin enthaltenen Produkte starten. Sie wenden AWS Identity and Access Management (IAM)-Berechtigungen an, um zu steuern, wer Ihren Katalog anzeigen und ändern kann. IAM-Berechtigungen können IAM-Benutzern, -Gruppen und -Rollen zugewiesen werden.

Wenn ein Benutzer ein Produkt startet, dem eine IAM-Rolle zugewiesen ist, verwendet Service Catalog die Rolle , um die Cloud-Ressourcen des Produkts mit zu startenAWS CloudFormation.

Indem Sie jedem Produkt eine IAM-Rolle zuweisen, können Sie vermeiden, Benutzern Berechtigungen zum Ausführen nicht genehmigter Vorgänge zu erteilen und ihnen ermöglichen, Ressourcen mithilfe des Katalogs bereitzustellen.

Beschränkungen

Einschränkungen steuern, wie Sie bestimmte AWS Ressourcen für ein Produkt bereitstellen können. Sie können sie verwenden, um zu Governance- oder Kostenkontrollzwecken Beschränkungen für Produkte einzurichten. Es gibt verschiedene Arten von AWS Service Catalog-Einschränkungen: Starteinschränkungen, Benachrichtigungseinschränkungen und Vorlageneinschränkungen.

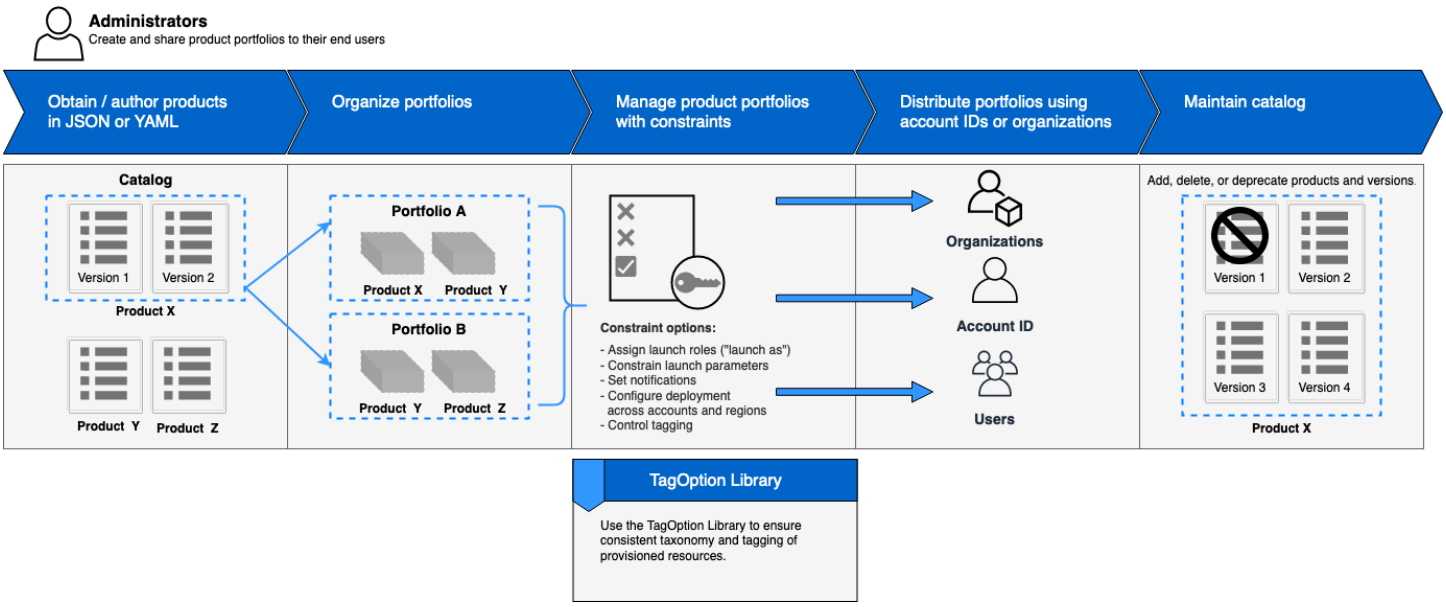
Mit Starteinschränkungen können Sie eine Rolle für ein Produkt im Portfolio festlegen. Verwenden Sie diese Rolle, um die Ressourcen beim Start bereitzustellen, sodass Sie Benutzerberechtigungen einschränken können, ohne die Fähigkeit der Benutzer zu beeinträchtigen, Produkte aus dem Katalog bereitzustellen.

Benachrichtigungseinschränkungen ermöglichen es Ihnen, Benachrichtigungen über Stack-Ereignisse mithilfe eines Amazon SNS-Themas zu erhalten.

Vorlageneinschränkungen grenzen die Konfigurationsparameter ein, über die der Benutzer beim Start des Produkts verfügt (beispielsweise EC2 Instance-Typen oder IP-Adressbereiche). Mit Vorlageneinschränkungen können Sie generische AWS CloudFormation-Vorlagen für Produkte wiederverwenden und jeweils für ein Produkt oder Portfolio Einschränkungen auf die Vorlagen anwenden.

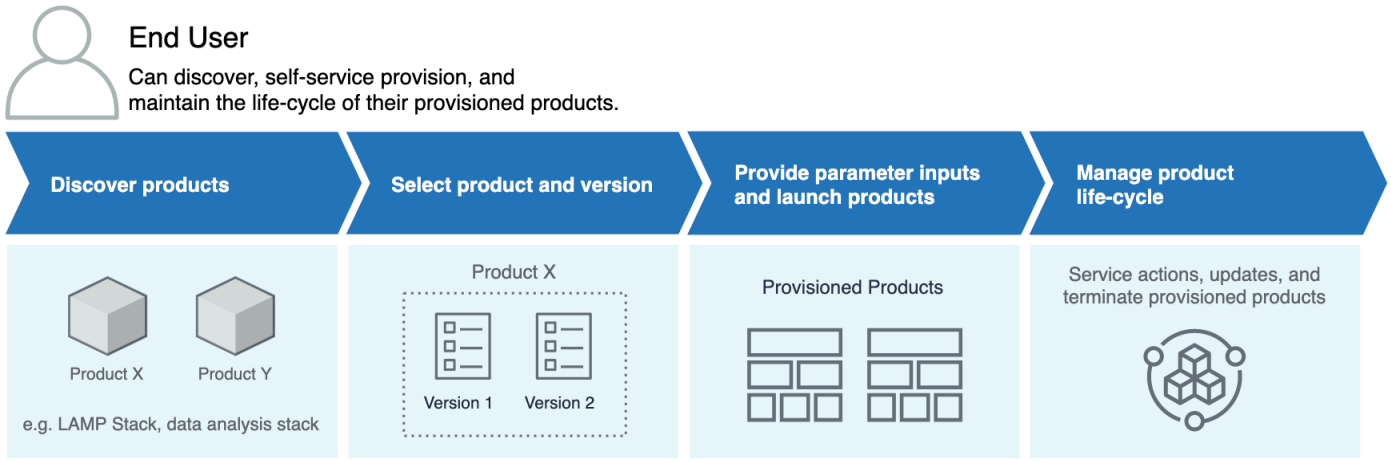
Anfänglicher Administrator-Workflow

Dieses Diagramm zeigt den anfänglichen Workflow für einen Administrator zum Erstellen eines Katalogs.



Anfänglicher Endbenutzer-Workflow

Dieses Diagramm zeigt den anfänglichen Workflow für einen Endbenutzer.



AWS Service Catalog-Standard-Servicekontingente

Ihr AWS Konto verfügt über die folgenden Standardkontingente für AWS Organizations, Einschränkung, Portfolio, Produkt, bereitgestelltes Produkt, regional, Service-Aktion und TagOptions.

Sie können verwendenService Quotas, um Ihre Kontingente zu verwalten oder eine Kontingenterhöhung anzufordern. Weitere Informationen zu Service Quotasfinden Sie unter Was sind Service Quotas? im Service Quotas -Benutzerhandbuch. Informationen zum Beantragen einer Kontingenterhöhung finden Sie unter Beantragen einer Kontingenterhöhung.

AWS Organizations

- AWS Service Catalog delegierte Administratoren pro Organisation: 50

Kontingente für Einschränkungen

- Einschränkungen pro Produkt und Portfolio: 100

Portfoliokontingente

- Benutzer, Gruppen und Rollen pro Portfolio: 100
- Produkte pro Portfolio: 150
- Tags pro Portfolio: 20
- Gemeinsame Konten pro Portfolio: 5.000
- Tag-Werte pro Tag-Schlüssel: 25

Produktkontingente

- Benutzer, Gruppen und Rollen pro Produkt: 200
- Produktversionen pro Produkt: 100
- Tags pro Produkt: 20
- Tag-Werte pro Tag-Schlüssel: 25

Kontingente für bereitgestellte Produkte

- Tags pro bereitgestelltem Produkt: 50

Regionale Kontingente

- Portfolios: 100
- Produkte: 350

Kontingente für Service-Aktionen

- Service-Aktionen pro Region: 200
- Service-Aktionszuordnungen pro Produktversion: 25

TagOptions -Kontingente

- TagOptions pro Ressource: 25
- Werte pro TagOption: 25

Einrichten AWS Service Catalog

Bevor Sie beginnen AWS Service Catalog, führen Sie die folgenden Aufgaben aus.

Themen

- Melden Sie sich an für eine AWS-Konto
- Erstellen Sie einen Benutzer mit Administratorzugriff

Melden Sie sich an für eine AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS -Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

Anweisungen finden Sie im Benutzerhandbuch unter Einen Berechtigungssatz erstellen.AWS IAM Identity Center

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.

- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erteilen von Berechtigungen für AWS Service Catalog Administratoren

Als Katalogadministrator benötigen Sie Zugriff auf die Ansicht der AWS Service Catalog Administratorkonsole und IAM-Berechtigungen, mit denen Sie Aufgaben wie die folgenden ausführen können:

- Erstellen und Verwalten von Portfolios
- Erstellen und Verwalten von Produkten

- Hinzufügen von Vorlageneinschränkungen, um die Optionen für Endbenutzer zu beschränken, wenn sie ein Produkt starten
- Hinzufügen von Starteinschränkungen zur Definition der IAM-Rollen, die AWS Service Catalog annimmt, wenn Endbenutzer Produkte starten
- Gewähren von Zugriff auf Ihre Produkte für Endbenutzer

Sie oder ein Administrator, der Ihre IAM-Berechtigungen verwaltet, müssen Ihrem IAM-Benutzer, Ihrer IAM-Gruppe oder -Rolle Richtlinien anfügen, die für dieses Tutorial erforderlich sind.

So weisen Sie einem Katalogadministrator Berechtigungen zu

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Zugriffsverwaltung und dann Benutzer aus. Wenn Sie bereits einen IAM-Benutzer erstellt haben, den Sie als Katalogadministrator verwenden möchten, wählen Sie den Benutzernamen und dann Berechtigungen hinzufügen aus. Andernfalls erstellen Sie einen Benutzer wie folgt:
   a. Wählen Sie Benutzer hinzufügen.
   b. Geben Sie für User name **`ServiceCatalogAdmin`** ein.
   c. Wählen Sie Programmatischer Zugriff und AWS Management Console Zugriff aus.
   d. Wählen Sie Weiter: Berechtigungen aus.
3. Wählen Sie Vorhandene Richtlinien direkt zuordnen.
4. Wählen Sie Richtlinie erstellen und gehen Sie dann wie folgt vor:
   a. Wählen Sie den Tab JSON.
   b. Kopieren Sie die folgende Beispielrichtlinie und fügen Sie sie in das Richtliniendokument ein:

```
{
    "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. Wählen Sie Weiter: Markierungen.

d. (Optional) Wählen Sie Tag hinzufügen, um der Ressource ein Schlüssel-Wert-Paar zuzuordnen. Sie können maximal 50 Tags hinzufügen.

> **Note**
>
> Tags sind Schlüssel-Wert-Paare, die Sie Ressourcen hinzufügen können. Dies hilft, Ressourcen zu identifizieren, zu organisieren und nach ihnen zu suchen. Weitere Informationen finden Sie unter Markieren von -AWSRessourcen im Allgemeine AWS-Referenz -Referenzhandbuch.

e. Wählen Sie Weiter: Prüfen aus.

f. Geben Sie für Policy Name **`ServiceCatalogAdmin-AdditionalPermissions`** ein.

> **Important**
>
> Sie müssen Administratoren Amazon S3 Berechtigungen für den Zugriff auf Vorlagen erteilen, die in Amazon S3 AWS Service Catalog speichert. Weitere Informationen finden Sie unter Beispiele für Benutzerrichtlinien im Benutzerhandbuch für Amazon Simple Storage Service .

g. Wählen Sie Richtlinie erstellen aus.

5. Wechseln Sie wieder zum Browserfenster mit der Seite mit den Berechtigungen und klicken Sie auf Refresh.
6. Geben Sie im Suchfeld **`ServiceCatalog`** ein, um die Richtlinienliste zu filtern.
7. Aktivieren Sie die Kontrollkästchen für die **`ServiceCatalogAdmin-AdditionalPermissions`** Richtlinien **`AWSServiceCatalogAdminFullAccess`** und und wählen Sie dann Weiter: Überprüfen aus.
8. Wenn Sie einen Benutzer aktualisieren wählen Sie Add permissions aus.

   Wenn Sie einen Benutzer erstellen, klicken Sie auf Create user. Sie können die Anmeldeinformationen herunterladen und kopieren. Klicken Sie dann auf Close.
9. Um sich als Katalogadministrator anzumelden, verwenden Sie die kontospezifische URL. Diese URL können Sie abrufen, indem Sie Dashboard im Navigationsbereich auswählen und auf Copy Link klicken. Fügen Sie den Link in Ihren Browser ein und verwenden Sie den Namen und das Passwort des IAM-Benutzers, den Sie in diesem Prozess erstellt oder aktualisiert haben.

AWS Service Catalog Endbenutzern Berechtigungen erteilen

Bevor der Endbenutzer AWS Service Catalog verwenden kann, müssen Sie der Konsolenansicht des AWS Service Catalog-Endbenutzers Zugriff gewähren. Zum Gewähren des Zugriffs fügen Sie dem IAM-Benutzer, der Gruppe oder der Rolle, die vom Endbenutzer verwendet wird, Richtlinien an. Im folgenden Verfahren fügen wir die **`AWSServiceCatalogEndUserFullAccess`** Richtlinie an eine IAM-Gruppe an.

So erteilen Sie einer Endbenutzer-Gruppe Berechtigungen

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Klicken Sie im Navigationsbereich auf Benutzergruppen.
3. Wählen Sie Gruppe erstellen und gehen Sie wie folgt vor:

   a. Geben Sie für Benutzergruppenname ein**`Endusers`**.

   b. Geben Sie im Suchfeld **`AWSServiceCatalog`** ein, um die Richtlinienliste zu filtern.

   c. Aktivieren Sie das Kontrollkästchen für die **`AWSServiceCatalogEndUserFullAccess`** Richtlinie. Sie haben auch die Möglichkeit, stattdessen **`AWSServiceCatalogEndUserReadOnlyAccess`** auszuwählen.

   d. Wählen Sie Create Group.

4. Klicken Sie im Navigationsbereich auf Users (Benutzer).
5. Wählen Sie Benutzer hinzufügen und gehen Sie wie folgt vor:

    a. Geben Sie für Benutzername einen Namen für den Benutzer ein.

    b. Wählen Sie Passwort – Zugriff auf die AWS Managementkonsole aus.

    c. Wählen Sie Weiter: Berechtigungen aus.

    d. Wählen Sie Add user to group.

    e. Aktivieren Sie das Kontrollkästchen für die Gruppe Endusers (Endbenutzer), wählen Sie Next: Tags (Weiter: Tags) und anschließend Next: Review (Weiter: Prüfen).

    f. Wählen Sie auf der Seite Review die Option Create user aus. Laden Sie die Anmeldeinformationen herunter oder kopieren Sie sie, und wählen Sie dann Schließen.

Installieren und Konfigurieren der Terraform-Bereitstellungs-Engine

Um Terraform-Produkte erfolgreich mit verwenden zu könnenAWS Service Catalog, müssen Sie eine Terraform-Bereitstellungs-Engine in demselben Konto installieren und konfigurieren, in dem Sie Terraform-Produkte verwalten werden. Zu Beginn können Sie die von bereitgestellte Terraform-Bereitstellungs-Engine verwendenAWS, die den Code und die Infrastruktur installiert und konfiguriert, die für die Arbeit der Terraform-Bereitstellungs-Engine mit erforderlich sindAWS Service Catalog. Diese einmalige Einrichtung dauert etwa 30 Minuten. AWS Service Catalog stellt ein GitHub Repository mit Anweisungen zur Installation und Konfiguration der Terraform-Bereitstellungs-Engine bereit.

Bestimmung der Warteschlange

Wenn Sie einen Bereitstellungsvorgang aufrufen, AWS Service Catalog bereitet eine Nutzlastnachricht vor, die an die entsprechende Warteschlange in der Bereitstellungs-Engine gesendet wird. Um den ARN für die Warteschlange zu erstellen, AWS Service Catalog geht von folgenden Annahmen aus:

- Die Bereitstellungs-Engine befindet sich im Konto des Produkteigentümers
- Die Bereitstellungs-Engine befindet sich in derselben Region, in der der Aufruf an getätigt AWS Service Catalog wurde.
- Die Warteschlangen der Bereitstellungs-Engine folgen dem unten beschriebenen dokumentierten Benennungsschema

Wenn beispielsweise `us-east-1` von Konto 1111111111 aus mit einem Produkt aufgerufen ProvisionProduct wird, das von Konto 0000000000000 erstellt wurde, geht AWS Service Catalog davon aus, dass der richtige SQS-ARN ist`arn:aws:sqs:us-east-1:0000000000000:ServiceCatalogTerraformOSProvisionOperationQueue`.

Die gleiche Logik gilt für die von aufgerufene Lambda-Funktion`DescribeProvisioningParameters`.

Hinzufügen von Confused Deputy zu Ihrer Terraform-Bereitstellungs-Engine

Verwirrte Stellvertreter-Kontextschlüssel auf den Endpunkten, um den Zugriff auf -**`lambda:Invoke`**Operationen einzuschränken

Die von von bereitgestellte Engines erstellte LambdaAWS Service Catalog-Funktion für Parameterparser verfügt über eine Zugriffsrichtlinie, die dem AWS Service Catalog Service-Prinzipal nur kontoübergreifende `lambda:Invoke` Berechtigungen gewährt:

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

Dies sollte die einzige Berechtigung sein, die erforderlich istAWS Service Catalog, damit die Integration mit ordnungsgemäß funktioniert. Sie können dies jedoch mit dem `aws:SourceAccount` Confused-Deputy-Kontextschlüssel weiter einschränken. Wenn Nachrichten an diese Warteschlangen AWS Service Catalog sendet, AWS Service Catalog füllt den Schlüssel mit der ID des Bereitstellungskontos aus. Dies ist hilfreich, wenn Sie beabsichtigen, Produkte über die Portfoliofreigabe zu verteilen und sicherstellen möchten, dass nur bestimmte Konten Ihre Engine verwenden.

Sie können Ihre Engine beispielsweise so einschränken, dass nur Anforderungen zugelassen werden, die von 000000000000 und 111111111111 stammen, indem Sie die unten gezeigte Bedingung verwenden:

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

Verwirrte Stellvertreter-Kontextschlüssel auf den Endpunkten, um den Zugriff auf -**`sqs:SendMessage`**Operationen einzuschränken

Der Bereitstellungsvorgang nimmt Amazon SQSAWS Service Catalog-Warteschlangen auf, die von bereitgestellten Engines erstellt wurden, verfügt über eine Zugriffsrichtlinie, die dem AWS Service Catalog Service-Prinzipal nur kontoübergreifende `sqs:SendMessage` (und zugehörige KMS) Berechtigungen gewährt:

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

Dies sollte die einzige Berechtigung sein, die erforderlich istAWS Service Catalog, damit die Integration mit ordnungsgemäß funktioniert. Sie können dies jedoch mit dem `aws:SourceAccount` Confused-Deputy-Kontextschlüssel weiter einschränken. Wenn Nachrichten an diese Warteschlangen AWS Service Catalog sendet, AWS Service Catalog füllt die Schlüssel mit der ID des Bereitstellungskontos aus. Dies ist hilfreich, wenn Sie beabsichtigen, Produkte über die Portfoliofreigabe zu verteilen und sicherstellen möchten, dass nur bestimmte Konten Ihre Engine verwenden.

Sie können Ihre Engine beispielsweise so einschränken, dass nur Anforderungen zugelassen werden, die von 000000000000 und 111111111111 stammen, indem Sie die unten gezeigte Bedingung verwenden:

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

Erste Schritte

Sie können mit beginnen, AWS Service Catalog indem Sie eine der gut strukturierten Produktvorlagen in der Bibliothek Erste Schritte verwenden oder die Schritte in einem der Tutorials für die ersten Schritte befolgen.

Im Tutorial führen Sie Aufgaben als Katalogadministrator und Endbenutzer aus. Als Katalogadministrator erstellen Sie ein Portfolio und dann ein Produkt. Als Endbenutzer überprüfen Sie, ob Sie auf die Endbenutzerkonsole zugreifen und das Produkt starten können. Das Produkt ist eines der folgenden:

- Eine Cloud-Entwicklungsumgebung, die auf Amazon Linux ausgeführt wird und auf einer -AWS CloudFormationVorlage basiert, die die AWS Ressourcen definiert, die das Produkt verwenden kann.
- Eine Open-Source-Umgebung, die auf einer Terraform-Bereitstellungs-Engine ausgeführt wird und auf einer tar.gz-Konfigurationsdatei basiert, die die AWS Ressourcen definiert, die das Produkt verwenden kann.

> **Note**
>
> Bevor Sie beginnen, stellen Sie sicher, dass Sie die Aktionselemente in abschließenEinrichten AWS Service Catalog.

Themen

- Bibliothek „Erste Schritte“
- Erste Schritte mit einem -AWS CloudFormationProdukt
- Erste Schritte mit einem Terraform-Produkt

Bibliothek „Erste Schritte“

AWS Service Catalog stellt eine Bibliothek „Erste Schritte“ mit gut strukturierten Produktvorlagen zur Verfügung, damit Sie schnell loslegen können. Sie können jedes der Produkte in unseren Erste Schritte-Bibliotheksportfolios in Ihr eigenes Konto kopieren und sie dann an Ihre Anforderungen anpassen.

Themen

- Voraussetzungen
- Weitere Informationen

Voraussetzungen

Bevor Sie die Vorlagen in unserer Bibliothek „Erste Schritte“ verwenden, stellen Sie sicher, dass Sie Folgendes besitzen:

- die erforderlichen Berechtigungen zum Verwenden von AWS CloudFormation-Vorlagen. Weitere Informationen finden Sie unter Zugriffskontrolle mit AWS Identity and Access Management.
- Die erforderlichen Administratorberechtigungen zum Verwalten von AWS Service Catalog. Weitere Informationen finden Sie unter the section called “Identitäts- und Zugriffsverwaltung”.

Weitere Informationen

Weitere Informationen zum gut strukturierten Framework finden Sie unter AWS Well-Architected.

Erste Schritte mit einem -AWS CloudFormationProdukt

Sie können mit beginnen, AWS Service Catalog indem Sie eine der gut strukturierten Produktvorlagen in der Bibliothek Erste Schritte verwenden oder die Schritte im Tutorial Erste Schritte befolgen.

Im Tutorial führen Sie Aufgaben als Katalogadministrator und Endbenutzer aus. Als Katalogadministrator erstellen Sie ein Porfolio und dann ein Produkt. Als Endbenutzer überprüfen Sie, ob Sie auf die Endbenutzerkonsole zugreifen und das Produkt starten können. Das Produkt ist eine Cloud-Entwicklungsumgebung, die auf Amazon Linux ausgeführt wird und auf einer -AWS CloudFormationVorlage basiert, die die AWS Ressourcen definiert, die das Produkt verwenden kann.

> **Note**
>
> Bevor Sie beginnen, stellen Sie sicher, dass Sie die Aktionselemente in abschließenEinrichten AWS Service Catalog.

Themen

- Schritt 1: Herunterladen der AWS CloudFormation Vorlage
- Schritt 2: Erstellen eines Schlüsselpaares
- Schritt 3: Erstellen eines Portfolios
- Schritt 4: Erstellen eines neuen Produkts im Portfolio
- Schritt 5: Fügen Sie eine Vorlagenbeschränkung hinzu, um die Instanzgröße zu begrenzen
- Schritt 6: Hinzufügen einer Starteinschränkung zum Zuweisen einer IAM-Rolle
- Schritt 7: Endbenutzern Zugriff auf das Portfolio gewähren
- Schritt 8: Testen der Endbenutzererfahrung

Schritt 1: Herunterladen der AWS CloudFormation Vorlage

Sie können -AWS CloudFormationVorlagen verwenden, um Portfolios und Produkte zu konfigurieren und bereitzustellen. Bei diesen Vorlagen handelt es sich um Textdateien, die in JSON oder YAML formatiert werden können und die Ressourcen beschreiben, die Sie bereitstellen möchten. Weitere Informationen finden Sie unter Vorlagenformate im AWS CloudFormation-Benutzerhandbuch. Sie können den AWS CloudFormation Editor oder einen Texteditor Ihrer Wahl verwenden, um Vorlagen zu erstellen und zu speichern. In diesem Tutorial stellen wir eine einfache Vorlage bereit, damit Sie loslegen können. Die Vorlage startet eine einzelne Linux-Instance, die für den SSH-Zugriff konfiguriert ist.

> **Note**
>
> Die Verwendung von -AWS CloudFormationVorlagen erfordert spezielle Berechtigungen. Bevor Sie beginnen, stellen Sie sicher, dass Sie über die richtigen Berechtigungen verfügen. Weitere Informationen finden Sie unter Voraussetzungen in Bibliothek „Erste Schritte“.

Herunterladen der Vorlage

Die für dieses Tutorial bereitgestellte Beispielvorlage, `development-environment.template`, ist unter https://awsdocs.s3.amazonaws.com/servicecatalog/development-environment.template verfügbar.

Vorlagen – Übersicht

Der Text der Beispielvorlage lautet wie folgt:

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

Vorlagenressourcen

Die Vorlage deklariert Ressourcen, die erstellt werden, wenn das Produkt gestartet wird. Sie besteht aus folgenden Abschnitten:

- AWSTemplateFormatVersion (optional) – Die Version des AWS Vorlagenformats, das zum Erstellen dieser Vorlage verwendet wurde. Die neueste Version des Vorlagenformats ist 2010-09-09 und derzeit der einzige gültige Wert.
- Beschreibung (optional) – Eine Beschreibung der Vorlage.
- Parameter (optional) – Die Parameter, die Ihr Benutzer angeben muss, um das Produkt zu starten. Für jeden Parameter enthält die Vorlage eine Beschreibung und Einschränkungen, die der eingegebene Wert erfüllen muss. Weitere Informationen zu den Einschränkungen finden Sie unter Verwenden von AWS Service Catalog-Einschränkungen.

  Mit dem `KeyName` Parameter können Sie einen Amazon Elastic Compute Cloud (Amazon EC2)-Schlüsselpaarnamen angeben, den Endbenutzer angeben müssen, wenn sie AWS Service Catalog zum Starten Ihres Produkts verwenden. Das Schlüsselpaar erstellen Sie im nächsten Schritt.

- Metadaten (optional) – Objekte, die zusätzliche Informationen über die Vorlage bereitstellen. Der Schlüssel AWS::CloudFormation::Interface definiert, wie die Ansicht der Endbenutzerkonsole Parameter anzeigt. Die Eigenschaft `ParameterGroups` legt fest, wie Parameter gruppiert werden und welche Überschriften die Gruppen erhalten. Die Eigenschaft `ParameterLabels` definiert benutzerfreundliche Parameternamen. Wenn ein Benutzer Parameter zum Starten eines Produkts auf Basis dieser Vorlage angibt, zeigt die Endbenutzer-Konsolenansicht den Parameter mit der Bezeichnung `Server size:` unter der Überschrift `Instance configuration` und die Parameter mit der Bezeichnung `Key pair:` und `CIDR range:` unter der Überschrift `Security configuration` an.
- Zuordnungen (optional) – Eine Zuordnung von Schlüsseln und zugehörigen Werten, mit der Sie bedingte Parameterwerte angeben können, ähnlich wie bei einer Nachschlagetabelle. Sie können einen Schlüssel einem entsprechenden Wert zuordnen, indem Sie die intrinsische Funktion Fn::FindInMap in den Abschnitten Ressourcen und Ausgaben verwenden. Die obige Vorlage enthält eine Liste von AWS Regionen und das Amazon Machine Image (AMI), das jeder Region entspricht. AWS Service Catalog verwendet diese Zuordnung, um anhand der AWS Region, die der Benutzer in der auswählt, zu bestimmen, welches AMI verwendet werden sollAWS Management Console.
- Ressourcen (erforderlich) – Stack-Ressourcen und ihre Eigenschaften. Sie können auf Ressourcen in den Abschnitten Ressourcen und Ausgaben der Vorlage verweisen. In der obigen Vorlage geben wir eine EC2-Instance an, auf der Amazon Linux ausgeführt wird, und eine Sicherheitsgruppe, die SSH-Zugriff auf die Instance ermöglicht. Der Abschnitt Eigenschaften der EC2-Instance-Ressource verwendet die Informationen, die der Benutzer zum Konfigurieren des Instance-Typs und eines Schlüsselnamens für den SSH-Zugriff verwendet.

  AWS CloudFormation verwendet die aktuelle AWS Region, um die AMI-ID aus den zuvor definierten Zuordnungen auszuwählen, und weist ihr eine Sicherheitsgruppe zu. Die Sicherheitsgruppe wird so konfiguriert, dass der eingehende Zugriff auf Port 22 aus dem CIDR-IP-Adressbereich, den der Benutzer angibt, zugelassen wird.
- Ausgaben (optional) – Text, der dem Benutzer mitteilt, wann der Produktstart abgeschlossen ist. Die angegebene Vorlage ruft den öffentlichen DNS-Namen der gestarteten Instance ab und zeigt sie dem Benutzer an. Der Benutzer benötigt den DNS-Namen zum Herstellen einer Verbindung mit der Instance per SSH.

  Weitere Informationen zur Seite Vorlagenanatomie finden Sie unter Vorlagenreferenz im AWS CloudFormation -Benutzerhandbuch.

Schritt 2: Erstellen eines Schlüsselpaares

Damit Ihre Endbenutzer das Produkt starten können, das auf der Beispielvorlage für dieses Tutorial basiert, müssen Sie ein Amazon EC2 EC2-Schlüsselpaar erstellen. Ein Schlüsselpaar ist eine Kombination aus einem öffentlichen Schlüssel für die Verschlüsselung von Daten und einem privaten Schlüssel, der verwendet wird, um Daten zu entschlüsseln. Für weitere Informationen über Schlüsselpaare stellen Sie sicher, dass Sie bei der AWS Konsole angemeldet sind, und lesen Sie dann Amazon EC2 EC2-Schlüsselpaare im Amazon EC2 EC2-Benutzerhandbuch.

Die AWS CloudFormation Vorlage für dieses Tutorial enthält den `development-environment.template` `KeyName` folgenden Parameter:

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

Endbenutzer müssen den Namen eines key pair angeben, wenn sie das auf der Vorlage basierende Produkt starten. AWS Service Catalog

Wenn Sie bereits über ein Schlüsselpaar in Ihrem Konto verfügen und dieses Paar verwenden möchten, können Sie diesen Schritt überspringen und mit Schritt 3: Erstellen eines Portfolios fortfahren. Führen Sie andernfalls die folgenden Schritte aus.

So erstellen Sie ein Schlüsselpaar

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Network & Security die Option Key Pairs aus.
3. Wählen Sie auf der Seite Key Pairs die Option Create Key Pair aus.
4. Geben Sie im Feld Key pair nameeinen Namen ein, den Sie sich leicht merken können, und klicken Sie dann auf Create.
5. Wenn Sie von der Konsole dazu aufgefordert werden, die Datei mit dem privaten Schlüssel zu speichern, legen Sie diese an einem sicheren Ort ab.

> **Important**
>
> Dies ist die einzige Möglichkeit, die private Schlüsseldatei zu speichern.

Schritt 3: Erstellen eines Portfolios

Um Benutzern Produkte zur Verfügung zu stellen, erstellen Sie zunächst ein Portfolio für diese Produkte.

So erstellen Sie ein Portfolio

1. Öffnen Sie die Service-Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie im linken Navigationsbereich Portfolios und dann Portfolio erstellen aus.
3. Geben Sie die folgenden Werte ein:
   - Portfolio-Name – **`Engineering Tools`**
   - Portfoliobeschreibung – **`Sample portfolio that contains a single product.`**
   - Besitzer – **`IT (it@example.com)`**
4. Wählen Sie Create (Erstellen) aus.

Schritt 4: Erstellen eines neuen Produkts im Portfolio

Nachdem Sie ein Portfolio erstellt haben, können Sie ein Produkt innerhalb des Portfolios erstellen. Für dieses Tutorial erstellen Sie ein Produkt namens Linux Desktop, eine Cloud-Entwicklungsumgebung, die auf Amazon Linux ausgeführt wird, innerhalb des Engineering-Tool-Portfolios.

So erstellen Sie ein Produkt innerhalb eines Portfolios

1. Wenn Sie den vorherigen Schritt ausgeführt haben, ist die Seite Portfolios bereits geöffnet. Andernfalls öffnen Sie https://console.aws.amazon.com/servicecatalog/.
2. Wählen und öffnen Sie das Engineering-Tool-Portfolio, das Sie in Schritt 2 erstellt haben.
3. Wählen Sie Neues Produkt hochladen.
4. Geben Sie auf der Seite Produkt erstellen im Abschnitt Produktdetails Folgendes ein:

- Product name – **Linux Desktop**
- Produktbeschreibung – **Cloud development environment configured for engineering staff. Runs AWS Linux.**
- Besitzer – **IT**
- Distributor – (leer)

5. Wählen Sie auf der Seite Versionsdetails die Option CloudFormation Vorlage verwenden aus. Wählen Sie dann Amazon S3-Vorlagen-URL angeben und geben Sie Folgendes ein:
   - Select template – **https://awsdocs.s3.amazonaws.com/servicecatalog/development-environment.template**
   - Versionstitel – **v1.0**
   - Description (Beschreibung) – **Base Version**
6. Geben Sie im Abschnitt Support-Details Folgendes ein:
   - E-Mail-Kontakt – **ITSupport@example.com**
   - Support-Link – **https://wiki.example.com/IT/support**
   - Support-Beschreibung – **Contact the IT department for issues deploying or connecting to this product.**
7. Wählen Sie Produkt erstellen aus.

Schritt 5: Fügen Sie eine Vorlagenbeschränkung hinzu, um die Instanzgröße zu begrenzen

Durch Einschränkungen wird die Kontrolle über Produkte auf Portfolioebene weiter erhöht. Einschränkungen können die Startumgebung eines Produkts (Starteinschränkungen) kontrollieren oder der AWS CloudFormation -Vorlage Regeln hinzufügen (Vorlageneinschränkungen). Weitere Informationen finden Sie unter Verwenden von AWS Service Catalog-Einschränkungen.

Fügen Sie dem Linux Desktop-Produkt eine Vorlageneinschränkung hinzu, die verhindert, dass Benutzer beim Start große Instance-Typen auswählen. Die Entwicklungsumgebungsvorlage ermöglicht die Auswahl aus sechs Instance-Typen. Diese Einschränkung beschränkt die gültigen Instance-Typen auf die beiden kleinsten Typen `t2.micro` und `t2.small`. Weitere Informationen finden Sie unter T2-Instances im Amazon EC2 EC2-Benutzerhandbuch.

So fügen Sie dem Linux Desktop-Produkt eine Vorlageneinschränkung hinzu

1. Wählen Sie auf der Seite mit den Portfoliodetails die Option Einschränkungen und anschließend Einschränkung erstellen aus.
2. Wählen Sie auf der Seite „Einschränkung erstellen“ für Produkt die Option Linux Desktop aus. Wählen Sie dann für Einschränkungstyp die Option Vorlage aus.
3. Wählen Sie im Abschnitt Vorlageneinschränkung die Option Texteditor aus.
4. Fügen Sie Folgendes in den Texteditor ein:

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

5. Geben Sie als Beschreibung der Einschränkung ein**`Small instance sizes`**.
6. Wählen Sie Create (Erstellen) aus.

Schritt 6: Hinzufügen einer Starteinschränkung zum Zuweisen einer IAM-Rolle

Eine Starteinschränkung bezeichnet eine IAM-Rolle, die AWS Service Catalog annimmt, wenn ein Endbenutzer ein Produkt startet.

Für diesen Schritt fügen Sie dem Linux-Desktop-Produkt eine Starteinschränkung hinzu, sodass die IAM-Ressourcen verwenden AWS Service Catalog kann, aus denen die AWS CloudFormation Produktvorlage besteht.

Die IAM-Rolle, die Sie einem Produkt als Starteinschränkung zuweisen, muss über die folgenden Berechtigungen verfügen.

1. AWS CloudFormation
2. Services in der AWS CloudFormation Vorlage für das Produkt
3. Lesezugriff auf die AWS CloudFormation Vorlage in einem serviceeigenen Amazon S3-Bucket.

Diese Starteinschränkung ermöglicht es dem Endbenutzer, das Produkt zu starten und es nach dem Start als bereitgestelltes Produkt zu verwalten. Weitere Informationen finden Sie unter AWS Service Catalog-Starteinschränkungen.

Ohne Starteinschränkung müssen Sie Ihren Endbenutzern zusätzliche IAM-Berechtigungen erteilen, bevor sie das Linux-Desktop-Produkt verwenden können. Beispielsweise gewährt die `ServiceCatalogEndUserAccess` Richtlinie die minimalen IAM-Berechtigungen, die für den Zugriff auf die AWS Service Catalog Endbenutzerkonsolenansicht erforderlich sind.

Durch die Verwendung einer Starteinschränkung können Sie die bewährte Methode von IAM befolgen, um die IAM-Berechtigungen von Endbenutzern auf ein Minimum zu beschränken. Weitere Informationen finden Sie unter Gewähren von geringsten Rechten im IAM-Benutzerhandbuch.

So fügen Sie eine Starteinschränkung hinzu

1. Folgen Sie den Anweisungen zum Erstellen neuer Richtlinien auf der Registerkarte JSON im IAM-Benutzerhandbuch.
2. Fügen Sie das folgende JSON-Richtliniendokument ein:

   - `cloudformation`– Ermöglicht AWS Service Catalog vollständige Berechtigungen zum Erstellen, Lesen, Aktualisieren, Löschen, Auflisten und Markieren von AWS CloudFormationStacks.
   - `ec2`– Ermöglicht AWS Service Catalog vollständige Berechtigungen zum Auflisten, Lesen, Schreiben, Bereitstellen und Markieren von Amazon Elastic Compute Cloud (Amazon EC2)-Ressourcen, die Teil des AWS Service Catalog Produkts sind. Abhängig von der AWS Ressource, die Sie bereitstellen möchten, kann sich diese Berechtigung ändern.
   - `ec2`– Erstellt eine neue verwaltete Richtlinie für Ihr AWS Konto und fügt die angegebene verwaltete Richtlinie an die angegebene IAM-Rolle an.
   - `s3`– Ermöglicht den Zugriff auf Amazon S3-Buckets, die gehörenAWS Service Catalog. Um das Produkt bereitzustellen, AWS Service Catalog benötigt Zugriff auf Bereitstellungsartefakte.
   - `servicecatalog`– Ermöglicht AWS Service Catalog Berechtigungen zum Auflisten, Lesen, Schreiben, Markieren und Starten von Ressourcen im Namen des Endbenutzers.

- `sns`– Ermöglicht AWS Service Catalog Berechtigungen zum Auflisten, Lesen, Schreiben und Markieren von Amazon SNS-Themen für die Starteinschränkung.

> **Note**
>
> Abhängig von den zugrunde liegenden Ressourcen, die Sie bereitstellen möchten, müssen Sie möglicherweise die Beispiel-JSON-Richtlinie ändern.

```
{
    "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. Wählen Sie Weiter, Tags aus.
4. Wählen Sie Weiter, Überprüfen aus.
5. Geben Sie auf der Seite Richtlinie überprüfen für den Namen ein**`linuxDesktopPolicy`**.
6. Wählen Sie Richtlinie erstellen aus.
7. Wählen Sie im Navigationsbereich Rollen aus. Wählen Sie dann Rolle erstellen und gehen Sie wie folgt vor:

   a. Wählen Sie für Vertrauenswürdige Entität auswählen die Option -AWSService und dann unter Anwendungsfall für andere AWS Services die Option Service Catalog aus. Wählen Sie den Anwendungsfall für Service Catalog und dann Weiter aus.

   b. Suchen Sie nach der linuxDesktopPolicy Richtlinie und aktivieren Sie dann das Kontrollkästchen.

   c. Wählen Sie Weiter aus.

   d. Geben Sie für Role name (Rollenname) **`linuxDesktopLaunchRole`** ein.

   e. Wählen Sie Rolle erstellen aus.
8. Öffnen Sie die -AWS Service CatalogKonsole unter https://console.aws.amazon.com/servicecatalog.
9. Wählen Sie das Portfolio Engineering Tools aus.
10. Wählen Sie auf der Seite mit den Portfolio-Details die Registerkarte Einschränkungen und dann Einschränkung erstellen aus.
11. Wählen Sie für Produkt Linux Desktop und für Einschränkungstyp die Option Starten aus.
12. Wählen Sie IAM-Rolle auswählen aus. Wählen Sie als Nächstes linuxDesktopLaunchRolle und dann Erstellen aus.

Schritt 7: Endbenutzern Zugriff auf das Portfolio gewähren

Nachdem Sie ein Portfolio erstellt und ein Produkt hinzugefügt haben, können Sie Endbenutzern Zugriff erteilen.

Voraussetzungen

Wenn Sie noch keine IAM-Gruppe für die Endbenutzer erstellt haben, finden Sie weitere Informationen unter AWS Service Catalog Endbenutzern Berechtigungen erteilen.

So erteilen Sie Zugriff auf das Portfolio

1. Wählen Sie auf der Seite mit den Portfoliodetails die Registerkarte Zugriff aus.
2. Wählen Sie Grant access (Zugriff gewähren).
3. Aktivieren Sie auf der Registerkarte Gruppen das Kontrollkästchen für die IAM-Gruppe für die Endbenutzer.
4. Wählen Sie Zugriff hinzufügen aus.

Schritt 8: Testen der Endbenutzererfahrung

Um zu überprüfen, ob der Endbenutzer erfolgreich auf die Ansicht der Endbenutzerkonsole zugreifen und Ihr Produkt starten kann, melden Sie sich bei AWS als Endbenutzer an und führen Sie diese Aufgaben aus.

So überprüfen Sie, ob der Endbenutzer auf die Endbenutzerkonsole zugreifen kann

1. Folgen Sie den Anweisungen zur Anmeldung als IAM-Benutzer im IAM-Benutzerhandbuch.
2. Wählen Sie in der Menüleiste die AWS Region aus, in der Sie das `Engineering Tools` Portfolio erstellt haben. Wählen Sie für dieses Tutorial die Region us-east-1 aus.
3. Öffnen Sie die -AWS Service CatalogKonsole unter https://console.aws.amazon.com/servicecatalog/, um Folgendes zu sehen:
   - Products – Die Produkte, die der Benutzer verwenden kann.
   - Provisioned products – Die bereitgestellten Produkte, die der Benutzer gestartet hat.

So überprüfen Sie, ob der Endbenutzer das Linux-Desktop-Produkt starten kann

Beachten Sie, dass Sie für dieses Tutorial die Region us-east-1 auswählen.

1. Wählen Sie im Abschnitt Produkte der -Konsole Linux Desktop aus.
2. Wählen Sie Produkt starten, um den Assistenten zu starten, der Ihr Produkt konfiguriert.
3. Geben Sie auf der Seite Launch: Linux Desktop **`Linux-Desktop`** als Namen des bereitgestellten Produkts ein.
4. Geben Sie auf der Seite Parameter Folgendes ein und wählen Sie Weiter aus:
   - Servergröße – Wählen Sie **`t2.micro`**.

- Key pair – Wählen Sie das Schlüsselpaar aus, das Sie in Schritt 2: Erstellen eines Schlüsselpaares erstellt haben.
- CIDR-Bereich – Geben Sie einen gültigen CIDR-Bereich für die IP-Adresse ein, um eine Verbindung mit der Instance herzustellen. Sie können den Standardwert (0.0.0.0/0) verwenden, um den Zugriff von einer beliebigen IP-Adresse aus zu erlauben, dann Ihre IP-Adresse, gefolgt von , **/32** um den Zugriff nur auf Ihre IP-Adresse einzuschränken, oder etwas dazwischen.

5. Wählen Sie Produkt starten, um den Stack zu starten. Die Konsole zeigt die Stack-Detailseite für den Linux-Desktop-Stack an. Der Anfangsstatus des Produkts lautet Änderung . Es dauert einige Minuten, bis AWS Service Catalog das Produkt startet. Aktualisieren Sie den Browser, um den aktuellen Status anzuzeigen. Nach dem Start des Produkts lautet der Status Verfügbar .

Erste Schritte mit einem Terraform-Produkt

AWS Service Catalog ermöglicht eine schnelle Self-Service-Bereitstellung mit Governance für Ihre HashiCorp Terraform-Konfigurationen in AWS. Sie können AWS Service Catalog als einzelnes Tool verwenden, um Ihre Terraform-Konfigurationen in in großem Umfang zu organisieren, zu verwalten und zu verteilenAWS. AWS Service Catalog unterstützt Terraform über mehrere wichtige Funktionen hinweg, darunter die Katalogisierung standardisierter und vorab genehmigter Terraform-Vorlagen, die Zugriffskontrolle, Versionierung, Tagging und die Freigabe an andere AWS Konten. In sehen Ihre Endbenutzer eine einfache Liste der Produkte und VersionenAWS Service Catalog, auf die sie Zugriff haben, und können diese Produkte dann in einer einzigen Aktion bereitstellen.

> **Note**
>
> Um die Unterstützung von HashiCorp Technologien fortzusetzen, hat aufgrund der letzten Lizenzänderungen an Terraform alle vorherigen Verweise auf Terraform Open Source auf Extern AWS Service Catalog geändert. Der externe Produkttyp unterstützt die Terraform Community Edition, die zuvor als Terraform Open Source bezeichnet wurde. Weitere Informationen und Anweisungen zur Migration Ihrer bestehenden Open-Source-Produkte von Terraform und bereitgestellten Produkte zum Produkttyp Externe finden Sie unter Aktualisieren vorhandener Open-Source-Produkte von Terraform und bereitgestellter Produkte auf den externen Produkttyp.

Die Schritte im folgenden Tutorial helfen Ihnen beim Einstieg in ein Terraform-Produkt in AWS Service Catalog.

Als Katalogadministrator arbeiten Sie in einem zentralen Administratorkonto (Hub-Konto). Sowohl Terrafrm Community Edition als auch Terraform Cloud-Produkte erfordern eine Terraform-Bereitstellungs-Engine, über die Sie in Bereitstellungs-Engine für Terraform Community Edition (Externer Produkttyp) und mehr erfahren könnenBereitstellungs-Engine für Terraform Cloud .

Während des Tutorials führen Sie die folgenden Aufgaben im Administratorkonto aus:

- Erstellen Sie ein Terraform-Produkt entweder mit der Terraform Cloud oder dem Produkttyp Extern. Service Catalog verwendet den Produkttyp Extern, um Produkte der Terraform Community Edition zu unterstützen.
- Zuordnen des Produkts zu einem Portfolio
- Erstellen Sie eine Starteinschränkung, damit Ihre Endbenutzer das Produkt bereitstellen können
- Markieren des Produkts
- Teilen Sie das Portfolio und das Terraform-Produkt mit dem Endbenutzerkonto (Spoke-Konto)

In dem Tutorial geben Sie ein Portfolio mithilfe der Option Organisationsfreigabe aus dem Admin-Hub-Konto frei, das auch das Verwaltungskonto der Organisation ist. Weitere Informationen zur Freigabe von Organisationen finden Sie unter Freigeben eines Portfolios.

Die im Terraform-Produkt enthaltene AWS Ressource, die Sie im Tutorial erstellen, ist ein einfacher Amazon S3-Bucket.

> **Note**
>
> Bevor Sie beginnen, stellen Sie sicher, dass Sie die Aktionselemente in abschließenEinrichten AWS Service Catalog.

Themen

- Aktualisieren vorhandener Open-Source-Produkte von Terraform und bereitgestellter Produkte auf den externen Produkttyp
- Voraussetzung: Konfigurieren Ihrer Terraform-Bereitstellungs-Engine
- Schritt 1: Herunterladen der Terraform-Konfigurationsdatei
- Schritt 2: Erstellen eines Terraform-Produkts

- Schritt 3: Erstellen eines AWS Service Catalog Portfolios
- Schritt 4: Hinzufügen eines Produkts zum Portfolio
- Schritt 5: Erstellen von Startrollen
- Schritt 6: Hinzufügen einer Starteinschränkung zu Ihrem Terraform-Produkt
- Schritt 7: Endbenutzerzugriff gewähren
- Schritt 8: Freigeben des Portfolios für Endbenutzer
- Schritt 9: Testen der Endbenutzererfahrung
- Schritt 10: Überwachen von Terraform-Bereitstellungsvorgängen

Aktualisieren vorhandener Open-Source-Produkte von Terraform und bereitgestellter Produkte auf den externen Produkttyp

Um die Unterstützung von HashiCorp Technologien fortzusetzen, hat aufgrund der letzten Lizenzänderungen an Terraform alle vorherigen Verweise auf Terraform Open Source auf Extern AWS Service Catalog geändert. Der externe Produkttyp bietet Unterstützung für Terraform Community Edition, früher bekannt als Terraform Open Source. unterstützt Terraform Open Source AWS Service Catalog nicht mehr als gültigen Produkttyp für neue Produkte oder bereitgestellte Produkte. Sie können nur vorhandene Terraform-Open-Source-Ressourcen aktualisieren oder beenden, einschließlich Produktversionen und bereitgestellter Produkte.

Wenn Sie dies noch nicht getan haben, müssen Sie alle vorhandenen Terraform-Open-Source-Produkte und bereitgestellten Produkte auf externe Produkte umstellen, indem Sie den Anweisungen in diesem Abschnitt folgen.

1. Aktualisieren Sie Ihre vorhandene Terraform-Referenz-Engine für AWS Service Catalog , um Unterstützung sowohl für externe als auch für Terraform-Open-Source-Produkttypen einzuschließen. Anweisungen zum Aktualisieren Ihrer Terraform Reference Engine finden Sie in unserem GitHub Repository .
2. Erstellen Sie alle vorhandenen Open-Source-Produkte von Terraform mit dem neuen externen Produkttyp neu.
3. Löschen Sie alle vorhandenen Produkte, die den Produkttyp Terraform Open Source verwenden.
4. Stellen Sie die verbleibenden Ressourcen erneut bereit, um den neuen externen Produkttyp zu verwenden.
5. Beenden Sie alle vorhandenen bereitgestellten Produkte, die den Terraform-Open-Source-Produkttyp verwenden.

Verwenden Sie nach der Umstellung Ihrer vorhandenen Produkte den Produkttyp Extern für alle neuen Produkte, die eine tar.gz-Konfigurationsdatei verwenden.

AWS Service Catalog unterstützt Kunden bei dieser Änderung nach Bedarf. Wenn diese Änderungen einen umfangreichen Aufwand für Ihr Konto erfordern oder sich auf kritische Produktworkloads auswirken, wenden Sie sich an Ihr Konto, um Unterstützung anzufordern.

Voraussetzung: Konfigurieren Ihrer Terraform-Bereitstellungs-Engine

Als Voraussetzung für die Erstellung von Terraform-Produkten in müssen AWS Service CatalogSie eine Bereitstellungs-Engine in Ihrem Service-Catalog-Administratorkonto (Hub-Konto) installieren und konfigurieren. Die Bereitstellungs-Engine ist sowohl für Produkte der Terraform Community Edition (mit dem externen Produkttyp) als auch für Produkte der Terraform Cloud (mit dem Produkttyp Terraform Cloud) erforderlich.

> **Note**
>
> Die Engine-Konfiguration ist eine einmalige Einrichtung, die etwa 30 Minuten dauert.

Bereitstellungs-Engine für Terraform Community Edition (Externer Produkttyp)

AWS Service Catalog verwendet den Produkttyp Extern, um Produkte der Terraform Community Edition zu unterstützen. Der externe Produkttyp unterstützt auch andere Bereitstellungstools, einschließlich Pulumi, Ansible, Chef und mehr, basierend auf der Konfiguration der Bereitstellungs-Engine.

Für AWS Service Catalog Produkte, die den externen Produkttyp mit der Terraform Community Edition von verwenden, müssen Sie eine Terraform- HashiCorpBereitstellungs-Engine in Ihrem AWS Service Catalog Administratorkonto (Hub-Konto) installieren und konfigurieren. AWS verwaltet diese Engine und ihre Ressourcen.

AWS Service Catalog stellt ein GitHub Repository mit Anweisungen zur Installation und Konfiguration der von bereitgestellten TerraformAWS-Bereitstellungs-Engine bereit. Das Repo enthält die folgenden Informationen:

- Erforderliche Installationstools
- Erstellen des Codes
- Bereitstellen auf einem AWS Konto

- Zusätzliche Informationen zu Bereitstellungsworkflows, Qualitätssicherung und Einschränkungen

Bereitstellungs-Engine für Terraform Cloud

Für AWS Service Catalog Produkte, die den Terraform Cloud-Produkttyp mit HashiCorpder Terraform Cloud von verwenden, müssen Sie eine Terraform-Bereitstellungs-Engine in Ihrem AWS Service Catalog Administratorkonto (Hub-Konto) installieren und konfigurieren. HashiCorp verwaltet diese Engine in einer Remote-Umgebung.

HashiCorp stellt ein GitHub Repository mit Anweisungen zur Konfiguration der Terraform Cloud-Engine für AWS Service Catalogbereit. Das Repo enthält die folgenden Informationen:

- Erforderliche Installationstools
- Erstellen des Codes
- Bereitstellen auf einem AWS Konto
- Zusätzliche Informationen zu Bereitstellungsworkflows, Qualitätssicherung und Einschränkungen

Schritt 1: Herunterladen der Terraform-Konfigurationsdatei

Sie können eine Terraform-Konfigurationsdatei verwenden, um HashiCorp Terraform-Produkte zu erstellen und bereitzustellen. Diese Konfigurationen sind Klartextdateien und beschreiben die Ressourcen, die Sie bereitstellen möchten. Sie können den Texteditor Ihrer Wahl verwenden, um Konfigurationen zu erstellen, zu aktualisieren und zu speichern. Für die Produkterstellung müssen Sie Terraform-Konfigurationen als tar.gz-Datei hochladen. In diesem Tutorial AWS Service Catalog stellt eine einfache Konfigurationsdatei bereit, damit Sie beginnen können. Die Konfiguration erstellt einen Amazon S3-Bucket.

Herunterladen der Konfigurationsdatei

AWS Service Catalog bietet eine `simple-s3-bucket.tar.gz` Beispielkonfigurationsdatei, die Sie in diesem Tutorial verwenden können.

Übersicht über die Konfigurationsdatei

Der Text der Beispielkonfigurationsdatei folgt:

```
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
}
```

Konfigurationsressourcen

Die Konfigurationsdatei deklariert die Ressourcen, die erstellt werden sollen, wenn das Produkt AWS Service Catalog bereitstellt. Sie besteht aus folgenden Abschnitten:

- Variable (optional) – Die Wertdefinitionen, die ein Administratorbenutzer (Hub-Kontoadministrator) zuweisen kann, um die Konfiguration anzupassen. Variablen bieten eine konsistente Schnittstelle, um das Verhalten einer bestimmten Konfiguration zu ändern. Die Bezeichnung nach dem Variablenschlüsselwort ist ein Name für die Variable, der unter allen Variablen im selben Modul eindeutig sein muss. Dieser Name wird verwendet, um der Variablen einen externen Wert zuzuweisen und innerhalb des Moduls auf den Wert der Variablen zu verweisen.
- Anbieter (optional) – Der Cloud-Service-Anbieter für die Ressourcenbereitstellung, der ist`AWS`. unterstützt AWS Service Catalog nur `AWS` als Anbieter. Daher überschreibt die Terraform-Bereitstellungs-Engine jeden anderen aufgeführten Anbieter für `AWS`.
- Ressource (erforderlich) – Die AWS Infrastrukturressource für die Bereitstellung. Für dieses Tutorial gibt die Terraform-Konfigurationsdatei Amazon S3 an.
- Ausgabe (optional) – Die zurückgegebenen Informationen oder Werte, ähnlich den zurückgegebenen Werten in einer Programmiersprache. Sie können Ausgabedaten verwenden, um den Infrastruktur-Workflow mit Automatisierungstools zu konfigurieren.

Schritt 2: Erstellen eines Terraform-Produkts

Nach der Installation der Terraform-Bereitstellungs-Engine können Sie ein HashiCorp Terraform-Produkt in erstellenAWS Service Catalog. In diesem Tutorial erstellen Sie ein Terraform-Produkt mit einem einfachen Amazon S3-Bucket.

So erstellen Sie ein Terraform-Produkt

1. Öffnen Sie die -AWS Service CatalogKonsole unter https://console.aws.amazon.com/servicecatalog/ und melden Sie sich als Administratorbenutzer an.
2. Navigieren Sie zum Abschnitt Administration und wählen Sie dann Produktliste aus.
3. Wählen Sie Produkt erstellen aus.
4. Wählen Sie auf der Seite Produkt erstellen im Abschnitt Produktdetails den Produkttyp Externe oder Terraform Cloud aus. Service Catalog verwendet den Produkttyp Extern, um Produkte der Terraform Community Edition zu unterstützen.
5. Geben Sie die folgenden Produktdetails ein:
   - Product name – **`Simple S3 bucket`**
   - Produktbeschreibung – Terraform-Produkt, das einen Amazon S3-Bucket enthält.
   - Besitzer – **`IT`**
   - Distributor – (leer)
6. Wählen Sie im Bereich Versionsdetails die Option Vorlagendatei hochladen und dann Datei auswählen aus. Wählen Sie die Datei aus, die Sie in heruntergeladen habenSchritt 1: Herunterladen der Terraform-Konfigurationsdatei.
7. Geben Sie Folgendes ein:
   - Versionsname – **`v1.0`**
   - Versionsbeschreibung – **`Base Version`**
8. Geben Sie im Abschnitt Support-Details Folgendes ein und wählen Sie dann Produkt erstellen aus.
   - E-Mail-Kontakt – **`ITSupport@example.com`**
   - Support-Link – **`https://wiki.example.com/IT/support`**
   - Support-Beschreibung – **`Contact the IT department for issues deploying or connecting to this product.`**
9. Wählen Sie Produkt erstellen aus.

Nachdem das Produkt erfolgreich erstellt wurde, AWS Service Catalog zeigt ein Bestätigungsbanner auf der Produktseite an.

Schritt 3: Erstellen eines AWS Service Catalog Portfolios

Sie können in Ihrem AWS Service Catalog Administratorkonto (Hub-Konto) ein Portfolio für eine einfache Produktorganisation und Verteilung an Endbenutzerkonten (Spoke-Konten) erstellen.

So erstellen Sie ein Portfolio

1. Öffnen Sie die -AWS Service CatalogKonsole unter https://console.aws.amazon.com/servicecatalog/ und melden Sie sich als Administrator an.
2. Wählen Sie im linken Navigationsbereich Portfolios und dann Portfolio erstellen aus.
3. Geben Sie die folgenden Werte ein:
   - Portfolio-Name – **`S3 bucket`**
   - Portfoliobeschreibung – **`Sample portfolio for Terraform configurations.`**
   - Besitzer – **`IT (it@example.com)`**
4. Wählen Sie Create (Erstellen) aus.

Schritt 4: Hinzufügen eines Produkts zum Portfolio

Nachdem Sie ein Portfolio erstellt haben, können Sie das HashiCorp Terraform-Produkt hinzufügen, das Sie in Schritt 2 erstellt haben.

So fügen Sie einem Portfolio ein Produkt hinzu

1. Navigieren Sie zur Seite Produktliste.
2. Wählen Sie das Terraform-Produkt für den einfachen S3-Bucket aus, das Sie in Schritt 2 erstellt haben, und wählen Sie dann Aktionen aus. Wählen Sie im Dropdown-Menü Produkt zum Portfolio hinzufügen aus. AWS Service Catalog zeigt den Bereich Einfachen S3-Bucket zum Portfolio hinzufügen an.
3. Wählen Sie das S3-Bucket-Portfolio aus und deaktivieren Sie dann Starteinschränkung erstellen. Sie erstellen die Starteinschränkung später im Tutorial.
4. Wählen Sie Produkt zum Portfolio hinzufügen aus.

Nachdem das Produkt erfolgreich zum Portfolio hinzugefügt wurde, AWS Service Catalog zeigt auf der Seite Produktliste ein Bestätigungsbanner an.

Schritt 5: Erstellen von Startrollen

In diesem Schritt erstellen Sie eine IAM-Rolle (Startrolle), die die Berechtigungen angibt, die die Terraform-Bereitstellungs-Engine übernehmen AWS Service Catalog kann, wenn ein Endbenutzer ein HashiCorp Terraform-Produkt startet.

Die IAM-Rolle (Startrolle), die Sie später Ihrem einfachen Amazon S3-Bucket-Terraform-Produkt als Starteinschränkung zuweisen, muss über die folgenden Berechtigungen verfügen:

- Zugriff auf die zugrunde liegenden AWS Ressourcen für Ihr Terraform-Produkt. In diesem `s3:CreateBucket*`Tutorial umfasst dies den Zugriff auf die `s3:PutBucketTagging` Amazon-SAmazon S3-Operationen `s3:DeleteBucket*`, `s3:Get*`, `s3:List*`, und .
- Lesezugriff auf die Amazon S3-Vorlage in einem AWS Service Catalog-eigenen Amazon S3-Bucket
- Zugriff auf die `Tag` Ressourcengruppenoperationen `CreateGroup`, `ListGroupResourcesDeleteGroup`, und . Diese Operationen ermöglichen AWS Service Catalog die Verwaltung von Ressourcengruppen und Tags

So erstellen Sie eine Startrolle im AWS Service Catalog Administratorkonto

1. Folgen Sie während der Anmeldung beim AWS Service Catalog Administratorkonto den Anweisungen unter Erstellen neuer Richtlinien auf der Registerkarte JSON im IAM-Benutzerhandbuch.
2. Erstellen Sie eine Richtlinie für Ihr Amazon S3-Bucket-Terraform-Produkt. Diese Richtlinie muss erstellt werden, bevor Sie die Startrolle erstellen, und besteht aus den folgenden Berechtigungen:
   - `s3`– Ermöglicht AWS Service Catalog vollständige Berechtigungen zum Auflisten, Lesen, Schreiben, Bereitstellen und Markieren des Amazon S3-Produkts.
   - `s3`– Ermöglicht den Zugriff auf Amazon S3-Buckets, die gehörenAWS Service Catalog. Um das Produkt bereitzustellen, AWS Service Catalog benötigt Zugriff auf Bereitstellungsartefakte.
   - `resourcegroups`– Ermöglicht AWS Service Catalog das Erstellen, Auflisten, Löschen und Markieren von AWS Resource Groups.
   - `tag`– Ermöglicht AWS Service Catalog Tagging-Berechtigungen.

> **Note**
>
> Abhängig von den zugrunde liegenden Ressourcen, die Sie bereitstellen möchten, müssen Sie möglicherweise die Beispiel-JSON-Richtlinie ändern.

Fügen Sie das folgende JSON-Richtliniendokument ein:

```
{
    "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. Wählen Sie Weiter, Tags aus.
   b. Wählen Sie Weiter, Überprüfen aus.
   c. Geben Sie auf der Seite Richtlinie überprüfen für den Namen ein**`S3ResourceCreationAndArtifactAccessPolicy`**.
   d. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie im Navigationsbereich Roles (Rollen) und dann Create role (Rolle erstellen).
5. Wählen Sie für Vertrauenswürdige Entität auswählen die Option Benutzerdefinierte Vertrauensrichtlinie aus und geben Sie dann die folgende JSON-Richtlinie ein:

```
{
    "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. Wählen Sie Weiter aus.
7. Wählen Sie in der Liste Richtlinien die aus, die `S3ResourceCreationAndArtifactAccessPolicy` Sie gerade erstellt haben.
8. Wählen Sie Weiter aus.
9. Geben Sie für Rollenname den Namen **`SCLaunch-S3product`** ein.

> **Important**
>
> Die Namen der Startrolle müssen mit „SCLaunch“ beginnen, gefolgt vom gewünschten Rollennamen.

10. Wählen Sie Rolle erstellen aus.

> **Important**
>
> Nachdem Sie die Startrolle in Ihrem AWS Service Catalog Administratorkonto erstellt haben, müssen Sie auch eine identische Startrolle im AWS Service Catalog Endbenutzerkonto erstellen. Die Rolle im Endbenutzerkonto muss denselben Namen haben und dieselbe Richtlinie wie die Rolle im Administratorkonto enthalten.

So erstellen Sie eine Startrolle im AWS Service Catalog Endbenutzerkonto

1. Melden Sie sich als Administrator beim Endbenutzerkonto an und folgen Sie dann den Anweisungen unter Erstellen neuer Richtlinien auf der Registerkarte JSON im IAM-Benutzerhandbuch.
2. Wiederholen Sie die Schritte 2-10 unter So erstellen Sie eine Startrolle im oben genannten AWS Service Catalog Administratorkonto.

> **Note**
>
> Stellen Sie beim Erstellen einer Startrolle im AWS Service Catalog Endbenutzerkonto sicher, dass Sie denselben Administrator **`AccountId`** in der benutzerdefinierten Vertrauensrichtlinie verwenden.

Nachdem Sie nun eine Startrolle sowohl im Administrator- als auch im Endbenutzerkonto erstellt haben, können Sie dem Produkt eine Starteinschränkung hinzufügen.

Schritt 6: Hinzufügen einer Starteinschränkung zu Ihrem Terraform-Produkt

> **Important**
>
> Sie müssen eine Starteinschränkung für HashiCorp Terraform-Produkte erstellen. Ohne eine Starteinschränkung können Endbenutzer das Produkt nicht bereitstellen.

Nachdem Sie eine Startrolle in Ihrem Administratorkonto erstellt haben, können Sie die Startrolle einer Starteinschränkung für Ihr externes oder Terraform-Cloud-Produkt zuordnen.

Diese Starteinschränkung ermöglicht es dem Endbenutzer, das Produkt zu starten und es nach dem Start als bereitgestelltes Produkt zu verwalten. Weitere Informationen finden Sie unter AWS Service Catalog-Starteinschränkungen.

Durch die Verwendung einer Starteinschränkung können Sie die bewährte Methode von IAM befolgen, um die IAM-Berechtigungen von Endbenutzern auf ein Minimum zu beschränken. Weitere Informationen finden Sie unter Gewähren von geringsten Rechten im IAM-Benutzerhandbuch.

So weisen Sie dem Produkt eine Starteinschränkung zu

1. Öffnen Sie die -AWS Service CatalogKonsole unter https://console.aws.amazon.com/servicecatalog.
2. Wählen Sie in der linken Navigationskonsole Portfolio aus.
3. Wählen Sie das S3-Bucket-Portfolio aus.
4. Wählen Sie auf der Seite mit den Portfolio-Details die Registerkarte Einschränkungen und dann Einschränkung erstellen aus.
5. Wählen Sie für Produkt die Option Einfacher S3-Bucket aus. wählt AWS Service Catalog automatisch den Typ Einschränkung starten aus.
6. Wählen Sie Rollenname eingeben und dann SCLaunch-S3product aus.
7. Wählen Sie Erstellen aus.

> **Note**
>
> Der angegebene Rollenname muss in dem Konto vorhanden sein, das die Starteinschränkung erstellt hat, und im Konto des Benutzers, der ein Produkt mit dieser Starteinschränkung startet.

Schritt 7: Endbenutzerzugriff gewähren

Nachdem Sie die Starteinschränkung auf Ihr HashiCorp Terraform-Produkt angewendet haben, können Sie Endbenutzern im Spoke-Konto Zugriff gewähren.

In diesem Tutorial gewähren Sie Endbenutzern mithilfe der Freigabe von Prinzipalnamen Zugriff. Prinzipalnamen sind Namen für Gruppen, Rollen und Benutzer, die Administratoren in einem Portfolio angeben und dann mit dem Portfolio teilen können. Wenn Sie das Portfolio freigeben, AWS Service Catalog überprüft , ob diese Prinzipalnamen bereits vorhanden sind. Wenn sie vorhanden sind, ordnet die übereinstimmenden IAM-Prinzipale AWS Service Catalog automatisch dem gemeinsamen Portfolio zu, um Endbenutzern Zugriff zu gewähren. Weitere Informationen finden Sie unter Freigeben eines Portfolios.

Voraussetzungen

Wenn Sie noch keine IAM-Gruppe für die Endbenutzer erstellt haben, finden Sie weitere Informationen unter AWS Service Catalog Endbenutzern Berechtigungen erteilen.

So erteilen Sie Zugriff auf das Portfolio

1. Navigieren Sie zur Seite Portfolio und wählen Sie das S3-Bucket-Portfolio aus.
2. Wählen Sie die Registerkarte Zugriff und dann Zugriff gewähren aus.
3. Wählen Sie im Bereich Zugriffstyp die Option Prinzipalname aus.
4. Wählen Sie im Bereich Prinzipalname den Typ Prinzipalname aus und geben Sie dann den Prinzipalnamen des gewünschten Endbenutzers im Spoke-Konto ein.
5. Wählen Sie Grant access (Zugriff gewähren).

Schritt 8: Freigeben des Portfolios für Endbenutzer

Der AWS Service Catalog Administrator kann Portfolios mithilfe von Freigabe oder AWS Organizations Freigabe mit account-to-account Endbenutzerkonten verteilen. In diesem Tutorial teilen Sie Ihr Portfolio mit der Organisation über das Administratorkonto (Hub-Konto), das auch das Verwaltungskonto der Organisation ist.

So geben Sie das Portfolio über das Admin-Hub-Konto frei

1. Öffnen Sie die -AWS Service CatalogKonsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie auf der Seite Portfolios das S3-Bucket-Portfolio aus. Wählen Sie im Menü Aktionen die Option Teilen aus.
3. Wählen Sie und filtern Sie AWS Organizationsdann in Ihre Organisationsstruktur.
4. Wählen Sie im Bereich AWS Organization das Endbenutzerkonto (Spoke-Konto) aus.

   Sie können auch einen Root-Knoten auswählen, um das Portfolio basierend auf Ihrer Organisationsstruktur für die gesamte Organisation, eine übergeordnete Organisationseinheit (OU) oder eine untergeordnete Organisationseinheit innerhalb Ihrer Organisation freizugeben. Weitere Informationen finden Sie unter Freigeben eines Portfolios.
5. Wählen Sie im Bereich Einstellungen freigeben die Option Prinzipalfreigabe aus.
6. Wählen Sie Freigeben.

Nachdem das Portfolio erfolgreich mit Endbenutzern geteilt wurde, besteht der nächste Schritt darin, die Endbenutzererfahrung zu überprüfen und das Terraform-Produkt bereitzustellen.

Schritt 9: Testen der Endbenutzererfahrung

Um zu überprüfen, ob Endbenutzer erfolgreich auf die Ansicht der Endbenutzerkonsole zugreifen und Ihr **`Simple S3 bucket`** Produkt starten können, melden Sie sich bei AWS als Endbenutzer an und führen Sie die folgenden Aufgaben aus.

So überprüfen Sie, ob der Endbenutzer auf die Endbenutzerkonsole zugreifen kann

- Öffnen Sie die -AWS Service CatalogKonsole unter https://console.aws.amazon.com/servicecatalog/, um Folgendes zu sehen:
  - Products – Die Produkte, die der Benutzer verwenden kann.
  - Provisioned products – Die bereitgestellten Produkte, die der Benutzer gestartet hat.

So überprüfen Sie, ob der Endbenutzer das Terraform-Produkt starten kann

1. Wählen Sie im Abschnitt Produkte der -Konsole Einfaches S3-Bucket aus.
2. Wählen Sie Produkt starten, um den Assistenten zu starten, der Ihr Produkt konfiguriert.
3. Geben Sie auf der Seite Einfachen S3-Bucket starten **`Amazon S3 product`** für den bereitgestellten Produktnamen ein.
4. Geben Sie auf der Seite Parameter Folgendes ein und wählen Sie Weiter aus:
   - bucket_name – Geben Sie einen eindeutigen Namen für den Amazon S3-Bucket an. Beispiel: **`terraform-s3-product`**
5. Wählen Sie Produkt starten aus. Die Konsole zeigt die Seite mit den Stack-Details für den Amazon S3-Produktstart an. Der Anfangsstatus des Produkts lautet Änderung . Es dauert einige Minuten, bis AWS Service Catalog das Produkt startet. Aktualisieren Sie den Browser, um den aktuellen Status anzuzeigen. Nach einem erfolgreichen Produktstart lautet der Status Verfügbar.

   AWS Service Catalog erstellt einen neuen Amazon S3-Bucket mit dem Namen **`terraform-s3-product`**.

Schritt 10: Überwachen von Terraform-Bereitstellungsvorgängen

Wenn Sie Bereitstellungsvorgänge überwachen möchten, können Sie Amazon- CloudWatch Protokolle und AWS Step Functions für jeden Bereitstellungsworkflow überprüfen.

Es gibt zwei Zustandsautomaten für den Bereitstellungs-Workflow:

- `ManageProvisionedProductStateMachine` – AWS Service Catalog ruft diesen Zustandsautomaten auf, wenn ein neues Terraform-Produkt bereitgestellt wird und wenn ein vorhandenes bereitgestelltes Terraform-Produkt aktualisiert wird.
- `TerminateProvisionedProductStateMachine` – AWS Service Catalog ruft diesen Zustandsautomaten auf, wenn ein vorhandenes von Terraform bereitgestelltes Produkt beendet wird.

So führen Sie den Überwachungs-Zustandsautomaten aus

1. Öffnen Sie die -AWSManagementkonsole und melden Sie sich als Administrator im Admin-Hub-Konto an, in dem die Terraform-Bereitstellungs-Engine installiert ist.
2. Öffnen Sie AWS Step Functions.
3. Wählen Sie im linken Navigationsbereich Zustandsautomaten aus.
4. Wählen Sie ManageProvisionedProductStateMachine.
5. Geben Sie in der Liste Ausführungen die bereitgestellte Produkt-ID ein, um Ihre Ausführung zu finden.

   > **Note**
   >
   > AWS Service Catalog erstellt die bereitgestellte Produkt-ID, wenn Sie das Produkt bereitstellen. Die bereitgestellte Produkt-ID ist wie folgt formatiert: **`pp-1111pwtn[ID number]`**.

6. Wählen Sie die Ausführungs-ID aus.

Auf der resultierenden Seite Ausführungsdetails können Sie alle Schritte im Bereitstellungsworkflow anzeigen. Sie können auch alle fehlgeschlagenen Schritte überprüfen, um die Ursache des Fehlers zu ermitteln.

Sicherheit in AWS Service Catalog

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS -Compliance-Programme regelmäßig.

  Weitere Informationen zu den Compliance-Programmen, die für gelten AWS Service Catalog, finden Sie unter AWS Services in Umfang nach Compliance-Programmen
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Nutzung anwenden können AWS Service Catalog. In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen AWS Service Catalog , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie werden auch mit anderen AWS Diensten vertraut gemacht, die Sie bei der Überwachung und Sicherung Ihrer AWS Service Catalog Ressourcen unterstützen.

Themen

- Datenschutz in AWS Service Catalog
- Identity and Access Management in AWS Service Catalog
- Einloggen und Überwachen AWS Service Catalog
- Konformitätsüberprüfung für AWS Service Catalog
- Resilienz in AWS Service Catalog
- Sicherheit der Infrastruktur in AWS Service Catalog
- Bewährte Sicherheitsmethoden für AWS Service Catalog

Datenschutz in AWS Service Catalog

Das Modell der AWS gemeinsamen Verantwortung und geteilter Verantwortung gilt für den Datenschutz in AWS Service Catalog. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen AWS Cloud. Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS -Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter Häufig gestellte Fragen zum Datenschutz. Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag AWS -Modell der geteilten Verantwortung und in der DSGVO im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS -Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit der Konsole, der API AWS Service Catalog oder den SDKs arbeiten oder diese anderweitig AWS -Services verwenden. AWS CLI AWS Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine

Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Datenschutz durch Verschlüsselung

Verschlüsselung im Ruhezustand

AWS Service Catalog verwendet Amazon S3 S3-Buckets und Amazon DynamoDB DynamoDB-Datenbanken, die im Ruhezustand mit von Amazon verwalteten Schlüsseln verschlüsselt sind. Weitere Informationen finden Sie in den Informationen zur Verschlüsselung im Ruhezustand von Amazon S3 und Amazon DynamoDB.

Verschlüsselung während der Übertragung

AWS Service Catalog verwendet Transport Layer Security (TLS) und die clientseitige Verschlüsselung von Informationen, die zwischen dem Anrufer und übertragen werden. AWS

Sie können privat auf AWS Service Catalog APIs von Ihrer Amazon Virtual Private Cloud (Amazon VPC) zugreifen, indem Sie VPC-Endpunkte erstellen. Bei VPC-Endpunkten AWS Service Catalog wird das Routing zwischen der VPC und dem AWS Netzwerk abgewickelt, ohne dass ein Internet-Gateway, ein NAT-Gateway oder eine VPN-Verbindung erforderlich ist.

Die neueste Generation von VPC-Endpunkten, die von verwendet werden, AWS Service Catalog basiert auf einer AWS Technologie AWS PrivateLink, die die private Konnektivität zwischen AWS Diensten mithilfe von Elastic Network Interfaces mit privaten IP-Adressen in Ihren VPCs ermöglicht.

Identity and Access Management in AWS Service Catalog

Für den Zugriff auf sind Anmeldeinformationen erforderlich AWS Service Catalog . Mit diesen Zugangsdaten müssen Sie berechtigt sein, auf AWS Ressourcen zuzugreifen, z. B. auf ein AWS Service Catalog Portfolio oder ein Produkt. AWS Service Catalog ist in AWS Identity and Access Management (IAM) integriert, sodass Sie AWS Service Catalog Administratoren die Berechtigungen gewähren können, die sie zum Erstellen und Verwalten von Produkten benötigen, und AWS Service Catalog Endbenutzern die Berechtigungen gewähren können, die sie benötigen, um Produkte zu starten und bereitgestellte Produkte zu verwalten. Diese Richtlinien werden entweder von Administratoren und Endbenutzern AWS oder individuell von diesen erstellt und verwaltet. Um den Zugriff zu kontrollieren, fügen Sie diese Richtlinien Benutzern, Gruppen und Rollen hinzu, die Sie zusammen verwenden AWS Service Catalog.

Zielgruppe

Welche Berechtigungen Sie für AWS Identity and Access Management (IAM) haben, können von der Rolle abhängen, in AWS Service Catalog der Sie spielen.

Welche Berechtigungen Sie über AWS Identity and Access Management (IAM) haben, können auch von der Rolle abhängen, in der Sie spielen. AWS Service Catalog

Administrator — Als AWS Service Catalog Administrator benötigen Sie vollen Zugriff auf die Administratorkonsole und IAM-Berechtigungen, mit denen Sie Aufgaben wie das Erstellen und Verwalten von Portfolios und Produkten, das Verwalten von Einschränkungen und das Gewähren von Zugriff für Endbenutzer ausführen können.

Endbenutzer — Bevor Ihre Endbenutzer Ihre Produkte verwenden können, müssen Sie ihnen Berechtigungen erteilen, die ihnen Zugriff auf die AWS Service Catalog Endbenutzerkonsole gewähren. Sie können auch über Berechtigungen zum Starten von Produkten und zum Verwalten von bereitgestellten Produkten verfügen.

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff darauf zu verwalten. AWS Service Catalog Beispiele für AWS Service Catalog identitätsbasierte Richtlinien, die Sie in IAM verwenden können, finden Sie unter. the section called “AWS verwaltete Richtlinien”

Beispiele für identitätsbasierte Richtlinien für AWS Service Catalog

Themen

- Konsolenzugriff für Endbenutzer
- Produktzugriff für Endbenutzer
- Beispielrichtlinien für die Verwaltung bereitgestellter Produkte

Konsolenzugriff für Endbenutzer

Die Richtlinien **`AWSServiceCatalogEndUserFullAccess`** und **`AWSServiceCatalogEndUserReadOnlyAccess`** gewähren den Zugriff auf die AWS Service Catalog -Endbenutzerkonsolenansicht. Wenn ein Benutzer, der über eine dieser Richtlinien verfügt AWS Management Console, AWS Service Catalog in der Ansicht der Endbenutzer-Konsole die Produkte auswählt, zu deren Start er berechtigt ist.

Bevor Endbenutzer ein Produkt, auf das Sie Zugriff gewähren, erfolgreich starten können, müssen Sie ihnen zusätzliche IAM-Berechtigungen gewähren, damit sie jede der zugrunde liegenden AWS Ressourcen in der AWS CloudFormation Produktvorlage verwenden können. AWS Service Catalog Wenn eine Produktvorlage beispielsweise Amazon Relational Database Service (Amazon RDS) enthält, müssen Sie den Benutzern Amazon RDS-Berechtigungen zum Starten des Produkts gewähren.

Weitere Informationen darüber, wie Sie Endbenutzern ermöglichen, Produkte auf den Markt zu bringen und gleichzeitig die geringsten Zugriffsberechtigungen für Ressourcen durchzusetzen, finden Sie unter. AWS the section called “Verwenden von Einschränkungen”

Wenn Sie die Richtlinie **`AWSServiceCatalogEndUserReadOnlyAccess`** anwenden, verfügen Ihre Benutzer zwar über Zugriff auf die Endbenutzerkonsolenansicht, nicht jedoch über die Berechtigungen, die zum Starten von Produkten und zum Verwalten von bereitgestellten Produkten erforderlich sind. Sie können diese Berechtigungen mithilfe von IAM direkt einem Endbenutzer gewähren. Wenn Sie jedoch den Zugriff von Endbenutzern auf AWS Ressourcen einschränken möchten, sollten Sie die Richtlinie einer Startrolle zuordnen. Anschließend wenden Sie die Startrolle auf eine Startbeschränkung für das Produkt an. AWS Service Catalog Weitere Informationen zum Anwenden einer Startrolle und zu Startrolleneinschränkungen sowie ein Startrollenbeispiel finden Sie unter AWS Service Catalog-Starteinschränkungen.

> **Note**
>
> Wenn Sie Benutzern IAM-Berechtigungen für AWS Service Catalog Administratoren gewähren, wird stattdessen die Ansicht der Administratorkonsole angezeigt. Gewähren Sie diese Berechtigungen Endbenutzern nur, wenn sie Zugriff auf die Administratorkonsolenansicht haben sollen.

Produktzugriff für Endbenutzer

Bevor Endbenutzer ein Produkt verwenden können, auf das Sie Zugriff gewähren, müssen Sie ihnen zusätzliche IAM-Berechtigungen gewähren, damit sie jede der zugrunde liegenden AWS Ressourcen in der AWS CloudFormation Vorlage eines Produkts verwenden können. Wenn eine Produktvorlage beispielsweise Amazon Relational Database Service (Amazon RDS) enthält, müssen Sie den Benutzern Amazon RDS-Berechtigungen zum Starten des Produkts gewähren.

Wenn Sie die Richtlinie **`AWSServiceCatalogEndUserReadOnlyAccess`** anwenden, verfügen Ihre Benutzer zwar über Zugriff auf die Endbenutzerkonsolenansicht, nicht jedoch über die

Berechtigungen, die zum Starten von Produkten und zum Verwalten von bereitgestellten Produkten erforderlich sind. Sie können diese Berechtigungen direkt einem Endbenutzer in IAM gewähren. Wenn Sie jedoch den Zugriff von Endbenutzern auf AWS Ressourcen einschränken möchten, sollten Sie die Richtlinie an eine Startrolle anhängen. Anschließend wenden Sie die Startrolle auf eine Startbeschränkung für das Produkt an. AWS Service Catalog Weitere Informationen zum Anwenden einer Startrolle und zu Startrolleneinschränkungen sowie ein Startrollenbeispiel finden Sie unter AWS Service Catalog-Starteinschränkungen.

Beispielrichtlinien für die Verwaltung bereitgestellter Produkte

Sie können Ihre benutzerdefinierte Richtlinien erstellen, um die Sicherheitsanforderungen Ihrer Organisation zu erfüllen. Die folgenden Beispiele beschreiben, wie Sie die Zugriffsebene für jede Aktion mit Support auf Benutzer-, Rollen- und Kontoebene anpassen. Sie können Benutzern den Zugriff zum Anzeigen, Aktualisieren, Beenden und Verwalten von bereitgestellten Produkten gewähren, die nur von dem entsprechenden Benutzer oder auch von anderen im Rahmen ihrer Rolle oder des Kontos erstellt wurden, bei dem sie angemeldet sind. Dieser Zugriff ist hierarchisch: Wenn Sie Zugriff auf Kontoebene gewähren, erhalten Sie auch Zugriff auf Rollen- und Benutzerebene, während das Hinzufügen von Zugriff auf Rollenebene ebenfalls Zugriff auf Benutzerebene gewährt, jedoch keinen Zugriff auf Kontoebene. Sie können diese in der Richtlinien-JSON unter Verwendung eines `Condition`-Blocks als `accountLevel`, `roleLevel` oder `userLevel` angeben.

Diese Beispiele gelten auch für Zugriffsebenen für AWS Service Catalog API-Schreiboperationen: `UpdateProvisionedProduct` und und `TerminateProvisionedProduct` und Lesevorgänge: `DescribeRecordScanProvisionedProducts`, und`ListRecordHistory`. Die API-Operationen `ScanProvisionedProducts` und `ListRecordHistory` verwenden `AccessLevelFilterKey` als Eingabe. Die Werte dieses Schlüssels entsprechen den hier beschriebenen `Condition`-Blockebenen (`accountLevel` entspricht einem `AccessLevelFilterKey`-Wert von „Account“, `roleLevel` entspricht „Role“, und `userLevel` entspricht „User“). Weitere Informationen finden Sie im Service Catalog Developer Guide.

Beispiele

- Vollständiger Administratorzugriff auf bereitgestellte Produkte
- Zugriff durch Endbenutzer auf bereitgestellte Produkte
- Teilweiser Administratorzugriff auf bereitgestellte Produkte

Vollständiger Administratorzugriff auf bereitgestellte Produkte

Mit der folgenden Richtlinie wird vollständiger Lese- und Schreibzugriff auf bereitgestellte Produkte und Datensätze im Katalog auf Kontoebene erlaubt.

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

Diese Richtlinie entspricht der Funktion der folgenden Richtlinie:

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

Das Nichtangeben eines `Condition` Blocks in einer Richtlinie für AWS Service Catalog wird genauso behandelt wie die Angabe eines `"servicecatalog:accountLevel"` Zugriffs. Beachten Sie, dass der `accountLevel`-Zugriff `roleLevel`- und `userLevel`-Zugriff umfasst.

Zugriff durch Endbenutzer auf bereitgestellte Produkte

Mit der folgenden Richtlinie wird der Zugriff auf Lese- und Schreibvorgänge auf die bereitgestellten Produkte oder verknüpfte Datensätze beschränkt, die der aktuelle Benutzer erstellt hat.

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

Teilweiser Administratorzugriff auf bereitgestellte Produkte

Wenn die beiden unten genannten Richtlinie auf denselben Benutzer angewendet werden, handelt es sich um einen eingeschränkten Administratorzugriff, der vollständigen Lesezugriff und beschränkten Schreibzugriff umfasst. Das bedeutet, dass der Benutzer zwar alle bereitgestellten Produkte oder zugehörigen Datensätze innerhalb des Katalogkontos sehen kann, jedoch keine Aktionen für bereitgestellte Produkte oder einen Datensätze ausführen kann, die nicht im Besitz dieses Benutzers sind.

Die erste Richtlinie erlaubt den Benutzerzugriff auf Schreibvorgänge für die bereitgestellten Produkte, die vom aktuellen Benutzer erstellt wurden, aber nicht für bereitgestellte Produkte, die von anderen Benutzern erstellt wurden. Die zweite Richtlinie fügt vollständigen Zugriff auf Lesevorgänge für bereitgestellte Produkte, die von allen (Benutzer, Rolle oder Konto) erstellt wurden, hinzu.

```
{
    "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 verwaltete Richtlinien für AWS Service Catalog AppRegistry

AWS verwaltete Richtlinie: **AWSServiceCatalogAdminFullAccess**

Sie können eine Verbindung `AWSServiceCatalogAdminFullAccess` zu Ihren IAM-Entitäten herstellen. AppRegistry ordnet diese Richtlinie auch einer Servicerolle zu, mit der Sie Aktionen AppRegistry in Ihrem Namen ausführen können.

Diese Richtlinie gewährt *Administratorberechtigungen*, die vollen Zugriff auf die Ansicht der Administratorkonsole ermöglichen, sowie Berechtigungen zum Erstellen und Verwalten von Produkten und Portfolios.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `servicecatalog`— Ermöglicht Prinzipalen uneingeschränkte Zugriffsrechte auf die Ansicht der Administratorkonsole sowie die Möglichkeit, Portfolios und Produkte zu erstellen und zu verwalten, Einschränkungen zu verwalten, Endbenutzern Zugriff zu gewähren und andere Verwaltungsaufgaben innerhalb AWS Service Catalog der Konsole auszuführen.
- `cloudformation`— Erlaubt AWS Service Catalog uneingeschränkte Rechte zum Auflisten, Lesen, Schreiben und Markieren von AWS CloudFormation Stacks.
- `config`— Ermöglicht AWS Service Catalog eingeschränkte Berechtigungen für Portfolios, Produkte und bereitgestellte Produkte über. AWS Config
- `iam`— Ermöglicht Prinzipalen uneingeschränkte Rechte zum Anzeigen und Erstellen von Servicebenutzern, Gruppen oder Rollen, die für die Erstellung und Verwaltung von Produkten und Portfolios erforderlich sind.
- `ssm`— Ermöglicht AWS Service Catalog das Auflisten AWS Systems Manager und Lesen von Systems Manager Manager-Dokumenten im aktuellen AWS Konto und in der AWS Region.

Richtlinie anzeigen: AWSServiceCatalogAdminFullAccess.

AWS verwaltete Richtlinie: **AWSServiceCatalogAdminReadOnlyAccess**

Sie können eine Verbindung `AWSServiceCatalogAdminReadOnlyAccess` zu Ihren IAM-Entitäten herstellen. AppRegistry ordnet diese Richtlinie auch einer Servicerolle zu, mit der Sie Aktionen AppRegistry in Ihrem Namen ausführen können.

Diese Richtlinie gewährt *nur Leseberechtigungen*, die vollen Zugriff auf die Ansicht der Administratorkonsole ermöglichen. Diese Richtlinie gewährt keinen Zugriff auf die Erstellung oder Verwaltung von Produkten und Portfolios.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `servicecatalog`— Ermöglicht Prinzipalen nur Leseberechtigungen für die Ansicht der Administratorkonsole.
- `cloudformation`— Erlaubt AWS Service Catalog eingeschränkte Berechtigungen zum Auflisten und Lesen von Stacks. AWS CloudFormation
- `config`— Ermöglicht AWS Service Catalog eingeschränkte Berechtigungen für Portfolios, Produkte und bereitgestellte Produkte über. AWS Config
- `iam`— Ermöglicht Prinzipalen eingeschränkte Berechtigungen zum Anzeigen von Servicebenutzern, Gruppen oder Rollen, die für die Erstellung und Verwaltung von Produkten und Portfolios erforderlich sind.
- `ssm`— Ermöglicht AWS Service Catalog das Auflisten AWS Systems Manager und Lesen von Systems Manager Manager-Dokumenten im aktuellen AWS Konto und in der AWS Region.

Richtlinie anzeigen: AWSServiceCatalogAdminReadOnlyAccess.

AWS verwaltete Richtlinie: **AWSServiceCatalogEndUserFullAccess**

Sie können eine Verbindung `AWSServiceCatalogEndUserFullAccess` zu Ihren IAM-Entitäten herstellen. AppRegistry ordnet diese Richtlinie auch einer Servicerolle zu, mit der Sie Aktionen AppRegistry in Ihrem Namen ausführen können.

Diese Richtlinie gewährt *Mitwirkenden* Berechtigungen, die uneingeschränkten Zugriff auf die Konsolenansicht für Endbenutzer ermöglichen, sowie die Erlaubnis, Produkte zu starten und bereitgestellte Produkte zu verwalten.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `servicecatalog`— Ermöglicht Principals uneingeschränkte Zugriffsrechte für die Ansicht der Endbenutzer-Konsole sowie die Möglichkeit, Produkte zu starten und bereitgestellte Produkte zu verwalten.
- `cloudformation`— Erlaubt AWS Service Catalog uneingeschränkte Rechte zum Auflisten, Lesen, Schreiben und Markieren AWS CloudFormation von Stacks.
- `config`— Ermöglicht AWS Service Catalog eingeschränkte Berechtigungen zum Auflisten und Lesen von Details zu Portfolios, Produkten und bereitgestellten Produkten über. AWS Config
- `ssm`— Ermöglicht AWS Service Catalog das Lesen von AWS Systems Manager Systems Manager Manager-Dokumenten im AWS Girokonto und in der AWS Region.

Richtlinie anzeigen: AWSServiceCatalogEndUserFullAccess.

AWS verwaltete Richtlinie: **`AWSServiceCatalogEndUserReadOnlyAccess`**

Sie können eine Verbindung `AWSServiceCatalogEndUserReadOnlyAccess` zu Ihren IAM-Entitäten herstellen. AppRegistry ordnet diese Richtlinie auch einer Servicerolle zu, mit der Sie Aktionen AppRegistry in Ihrem Namen ausführen können.

Diese Richtlinie gewährt *`nur Leseberechtigungen, die nur`* Lesezugriff auf die Konsolenansicht für Endbenutzer ermöglichen. Diese Richtlinie gewährt keine Erlaubnis, Produkte auf den Markt zu bringen oder bereitgestellte Produkte zu verwalten.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `servicecatalog`— Ermöglicht Prinzipalen nur Leseberechtigungen für die Konsolenansicht des Endbenutzers.
- `cloudformation`— Erlaubt AWS Service Catalog eingeschränkte Berechtigungen zum Auflisten und Lesen von Stacks. AWS CloudFormation
- `config`— Ermöglicht AWS Service Catalog eingeschränkte Berechtigungen zum Auflisten und Lesen von Details zu Portfolios, Produkten und bereitgestellten Produkten über. AWS Config
- `ssm`— Ermöglicht AWS Service Catalog das Lesen von AWS Systems Manager Systems Manager Manager-Dokumenten im AWS Girokonto und in der AWS Region.

Richtlinie anzeigen: AWSServiceCatalogEndUserReadOnlyAccess.

AWS verwaltete Richtlinie: **`AWSServiceCatalogSyncServiceRolePolicy`**

AWS Service Catalog fügt diese Richtlinie der `AWSServiceRoleForServiceCatalogSync` serviceverknüpften Rolle (SLR) hinzu, sodass AWS Service Catalog Vorlagen in einem externen Repository mit Produkten synchronisiert werden können. AWS Service Catalog

Diese Richtlinie gewährt Berechtigungen, die eingeschränkten Zugriff auf AWS Service Catalog Aktionen (z. B. API-Aufrufe) und auf andere AWS Serviceaktionen ermöglichen, die AWS Service Catalog davon abhängen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `servicecatalog`— Erlaubt der Rolle „ AWS Service Catalog Artefaktsynchronisierung“ eingeschränkten Zugriff auf AWS Service Catalog öffentliche APIs.
- `codeconnections`— Ermöglicht der Rolle „ AWS Service Catalog Artefaktsynchronisierung“ eingeschränkten Zugriff auf CodeConnections öffentliche APIs.
- `cloudformation`— Ermöglicht der Rolle „ AWS Service Catalog Artefaktsynchronisierung“ eingeschränkten Zugriff auf AWS CloudFormation öffentliche APIs.

Sehen Sie sich die Richtlinie an: AWSServiceCatalogSyncServiceRolePolicy.

Details zur dienstbezogenen Rolle

AWS Service Catalog verwendet die obigen Berechtigungsdetails für die `AWSServiceRoleForServiceCatalogSync` dienstbezogene Rolle, die erstellt wird, wenn ein Benutzer ein AWS Service Catalog Produkt erstellt oder aktualisiert, das verwendet. CodeConnections Sie können diese Richtlinie über die AWS CLI, AWS API oder über die AWS Service Catalog Konsole ändern. Weitere Informationen zum Erstellen, Bearbeiten und Löschen von serviceverknüpften Rollen finden Sie unter Verwenden von serviceverknüpften Rollen (SLRs) für. AWS Service Catalog

Die in der `AWSServiceRoleForServiceCatalogSync` serviceverknüpften Rolle enthaltenen Berechtigungen ermöglichen es AWS Service Catalog , die folgenden Aktionen im Namen des Kunden durchzuführen.

- `servicecatalog:ListProvisioningArtifacts`— Ermöglicht der Rolle „ AWS Service Catalog Artefaktsynchronisierung“, die Bereitstellungsartefakte für ein bestimmtes AWS Service Catalog Produkt aufzulisten, das mit einer Vorlagendatei in einem Repository synchronisiert wurde.
- `servicecatalog:DescribeProductAsAdmin`— Ermöglicht der Rolle für die AWS Service Catalog Artefaktsynchronisierung, die `DescribeProductAsAdmin` API zu verwenden, um Details zu einem AWS Service Catalog Produkt und den zugehörigen bereitgestellten Artefakten abzurufen, die mit einer Vorlagendatei in einem Repository synchronisiert wurden. Die Rolle für die Artefaktsynchronisierung verwendet die Ausgabe dieses Aufrufs, um die Servicekontingentbeschränkung des Produkts für die Bereitstellung von Artefakten zu überprüfen.
- `servicecatalog:DeleteProvisioningArtifact`— Ermöglicht der Rolle für die AWS Service Catalog Artefaktsynchronisierung, ein bereitgestelltes Artefakt zu löschen.
- `servicecatalog:ListServiceActionsForProvisioningArtifact`— Ermöglicht der Rolle für die AWS Service Catalog Artefaktsynchronisierung, festzustellen, ob Serviceaktionen mit einem Bereitstellungsartefakt verknüpft sind, und sicherzustellen, dass das Bereitstellungsartefakt nicht gelöscht wird, wenn eine Serviceaktion zugeordnet ist.
- `servicecatalog:DescribeProvisioningArtifact`— Ermöglicht der AWS Service Catalog Artifact-Synchronisierungsrolle, Details von der `DescribeProvisioningArtifact` API abzurufen, einschließlich der Commit-ID, die in der Ausgabe bereitgestellt wird. `SourceRevisionInfo`
- `servicecatalog:CreateProvisioningArtifact`— Ermöglicht der Rolle für die AWS Service Catalog Artefaktsynchronisierung, ein neues bereitgestelltes Artefakt zu erstellen, wenn eine Änderung an der Quellvorlagendatei im externen Repository erkannt wird (z. B. wenn ein Git-Push festgeschrieben wird).
- `servicecatalog:UpdateProvisioningArtifact`— Ermöglicht der Rolle für die AWS Service Catalog Artefaktsynchronisierung, das bereitgestellte Artefakt für ein verbundenes oder synchronisiertes Produkt zu aktualisieren.
- `codeconnections:UseConnection`— Ermöglicht der Rolle für die AWS Service Catalog Artefaktsynchronisierung, die bestehende Verbindung zum Aktualisieren und Synchronisieren eines Produkts zu verwenden.
- `cloudformation:ValidateTemplate`— Ermöglicht der Rolle für die AWS Service Catalog Artefaktsynchronisierung mit eingeschränktem Zugriff AWS CloudFormation , um das Vorlagenformat für die Vorlage, die im externen Repository verwendet wird, zu überprüfen und zu überprüfen, ob AWS CloudFormation die Vorlage unterstützt wird.

AWS verwaltete Richtlinie: **`AWSServiceCatalogOrgsDataSyncServiceRolePolicy`**

AWS Service Catalog fügt diese Richtlinie der `AWSServiceRoleForServiceCatalogOrgsDataSync` serviceverknüpften Rolle (SLR) hinzu und ermöglicht so AWS Service Catalog die Synchronisierung mit. AWS Organizations

Diese Richtlinie gewährt Berechtigungen, die eingeschränkten Zugriff auf AWS Service Catalog Aktionen (z. B. API-Aufrufe) und auf andere AWS Serviceaktionen ermöglichen, die AWS Service Catalog davon abhängen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `organizations`— Ermöglicht der AWS Service Catalog Datensynchronisierungsrolle eingeschränkten Zugriff auf AWS Organizations öffentliche APIs.

Sehen Sie sich die Richtlinie an: AWSServiceCatalogOrgsDataSyncServiceRolePolicy.

Details zur dienstbezogenen Rolle

AWS Service Catalog verwendet die oben genannten Berechtigungsdetails für die `AWSServiceRoleForServiceCatalogOrgsDataSync` dienstbezogene Rolle, die erstellt wird, wenn ein Benutzer den AWS Organizations gemeinsamen Portfoliozugriff aktiviert oder eine Portfoliofreigabe erstellt. Sie können diese Richtlinie über die AWS CLI, AWS API oder über die AWS Service Catalog Konsole ändern. Weitere Informationen zum Erstellen, Bearbeiten und Löschen von serviceverknüpften Rollen finden Sie unter Verwenden von serviceverknüpften Rollen (SLRs) für. AWS Service Catalog

Die in der `AWSServiceRoleForServiceCatalogOrgsDataSync` serviceverknüpften Rolle enthaltenen Berechtigungen ermöglichen es AWS Service Catalog , die folgenden Aktionen im Namen des Kunden durchzuführen.

- `organizations:DescribeAccount`— Ermöglicht der Rolle AWS Service Catalog Organizations Data Sync, verwandte AWS Organizations Informationen über das angegebene Konto abzurufen.

- `organizations:DescribeOrganization`— Ermöglicht der Rolle AWS Service Catalog Organizations Data Sync, Informationen über die Organisation abzurufen, zu der das Konto des Benutzers gehört.
- `organizations:ListAccounts`— Ermöglicht der Rolle AWS Service Catalog Organizations Data Sync, die Konten in der Organisation des Benutzers aufzulisten.
- `organizations:ListChildren`— Ermöglicht der Rolle AWS Service Catalog Organizations Data Sync, alle Organisationseinheiten (UOs) oder Konten aufzulisten, die in der angegebenen übergeordneten OU oder dem angegebenen Stamm enthalten sind.
- `organizations:ListParents`— Ermöglicht der Rolle AWS Service Catalog Organizations Data Sync, die Root-Organisationseinheiten aufzulisten, die der angegebenen untergeordneten Organisationseinheit oder dem angegebenen untergeordneten Konto als unmittelbare übergeordnete Organisationseinheit dienen.
- `organizations:ListAWSServiceAccessForOrganization`— Ermöglicht der Rolle AWS Service Catalog Organizations Data Sync, eine Liste der AWS Dienste abzurufen, die der Benutzer für die Integration in seine Organisation aktiviert hat.

Veraltete Richtlinien

Die folgenden verwalteten Richtlinien sind veraltete:

- ServiceCatalogAdminFullAccess— Verwenden Sie stattdessen AWSServiceCatalogAdminFullAccess.
- ServiceCatalogAdminReadOnlyAccess— AWSServiceCatalogAdminReadOnlyAccessStattdessen verwenden.
- ServiceCatalogEndUserFullAccess— Verwenden Sie AWSServiceCatalogEndUserFullAccessstattdessen.
- ServiceCatalogEndUserAccess— Verwenden Sie AWSServiceCatalogEndUserReadOnlyAccessstattdessen.

Führen Sie die folgenden Schritte aus, um sicherzustellen, dass Ihre Administratoren und Endbenutzer die Berechtigungen unter Verwendung der aktuellen Richtlinien erhalten.

Informationen zur Migration von den veralteten Richtlinien zu den aktuellen Richtlinien finden Sie unter Hinzufügen und Entfernen von IAM-Identitätsberechtigungen im AWS Identity and Access Management Benutzerhandbuch.

AppRegistry Aktualisierungen der verwalteten Richtlinien AWS

Hier finden Sie Informationen zu Aktualisierungen AWS verwalteter Richtlinien, die AppRegistry seit Beginn der Nachverfolgung dieser Änderungen durch diesen Dienst vorgenommen wurden. Abonnieren Sie den RSS-Feed auf der Seite AppRegistry Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderung	Beschreibung	Datum
AWSServiceCatalogSyncServiceRolePolicy— Verwaltete Richtlinie aktualisieren	AWS Service Catalog hat die `AWSServiceCatalogSyncServiceRolePolicy` Richtlinie aktualisiert, um `codestar-connections` zu wechseln `codeconnections` .	7. Mai 2024
AWSServiceCatalogAdminFullAccess— Verwaltete Richtlinie aktualisieren	AWS Service Catalog Die `AWSServiceCatalogAdminFullAccess` Richtlinie wurde aktualisiert und enthält nun auch die Berechtigungen, die der AWS Service Catalog Administrator benötigt, um die `AWSServiceRoleForServiceCatalogOrgsDataSync` serviceverknüpfte Rolle (SLR) in seinem Konto zu erstellen.	14. April 2023
AWSServiceCatalogOrgsDataSyncServiceRolePolicy— Neue verwaltete Richtlinie	AWS Service Catalog hat die hinzugefügt `AWSServiceCatalogOrgsDataSyncServiceRolePolicy` , die an die `AWSServiceRoleForServiceCatalogOrgsDataSync`	14. April 2023

Änderung	Beschreibung	Datum
	serviceverknüpfte Rolle (SLR) angehängt ist und die Synchronisation mit AWS Service Catalog ermöglicht. AWS Organizations Diese Richtlinie ermöglicht eingeschränkten Zugriff auf AWS Service Catalog Aktionen (z. B. API-Aufrufe) und auf andere AWS Serviceaktionen, die AWS Service Catalog davon abhängen.	
AWSServiceCatalogAdminFullAccess— Verwaltete Richtlinie aktualisieren	AWS Service Catalog Die `AWSServiceCatalogAdminFullAccess` Richtlinie wurde aktualisiert, sodass sie alle Berechtigungen für den AWS Service Catalog Administrator enthält und die Kompatibilität mit gewährleistet AppRegistry.	12. Januar 2023

Änderung	Beschreibung	Datum
AWSServiceCatalogSyncServiceRolePolicy— Neue verwaltete Richtlinie	AWS Service Catalog hat die `AWSServiceCatalogSyncServiceRolePolicy` Richtlinie hinzugefügt, die der `AWSServiceRoleForServiceCatalogSync` serviceverknüpften Rolle (SLR) zugeordnet ist. Diese Richtlinie ermöglicht AWS Service Catalog das Synchronisieren von Vorlagen in einem externen Repository mit AWS Service Catalog Produkten.	18. November 2022
AWSServiceRoleForServiceCatalogSync— Neue serviceverknüpfte Rolle	AWS Service Catalog Die `AWSServiceRoleForServiceCatalogSync` serviceverknüpfte Rolle (SLR) wurde hinzugefügt. Diese Rolle ist erforderlich AWS Service Catalog , um AWS Service Catalog Bereitstellungsartefakte für ein Produkt zu verwenden CodeConnections und zu erstellen, zu aktualisieren und zu beschreiben.	18. November 2022

Änderung	Beschreibung	Datum
AWSServiceCatalogAdminFullAccess— Die verwaltete Richtlinie wurde aktualisiert	AWS Service Catalog Die `AWSServiceCatalogAdminFullAccess` Richtlinie wurde aktualisiert und umfasst nun alle erforderlichen AWS Service Catalog Administratorberechtigungen. Die Richtlinie identifiziert die spezifischen Aktionen, die der Administrator für alle AWS Service Catalog Ressourcen ergreifen kann, z. B. Erstellen, Beschreiben, Löschen und mehr. Darüber hinaus wurde die Richtlinie geändert, um eine kürzlich eingeführte Funktion, die attributebasierte Zugriffskontrolle (ABAC) für AWS Service Catalog, zu unterstützen. ABAC ermöglicht es Ihnen, die `AWSServiceCatalogAdminFullAccess` Richtlinie als Vorlage zu verwenden, um Aktionen an AWS Service Catalog Ressourcen, die auf Tags basieren, zuzulassen oder zu verweigern. Weitere Informationen zu ABAC finden Sie unter Wofür ist ABAC in. AWSAWS Identity and Access Management	30. September 2022

Änderung	Beschreibung	Datum
AppRegistry hat begonnen, Änderungen zu verfolgen	AppRegistry hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	15. September 2022

Verwenden von serviceverknüpften Rollen für AWS Service Catalog

AWS Service Catalog verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, mit der direkt verknüpft ist. AWS Service Catalog Mit Diensten verknüpfte Rollen sind vordefiniert AWS Service Catalog und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstbezogene Rolle AWS Service Catalog erleichtert die Einrichtung, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS Service Catalog definiert die Berechtigungen ihrer dienstbezogenen Rollen und AWS Service Catalog kann, sofern nicht anders definiert, nur ihre Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dadurch werden Ihre AWS Service Catalog Ressourcen geschützt, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entziehen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS -Services, die mit IAM funktionieren. Suchen Sie nach den Services, für die Ja in der Spalte Serviceverknüpfte Rollen angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Rollen für **`AWSServiceRoleForServiceCatalogSync`**

AWS Service Catalog kann die mit dem Dienst verknüpfte Rolle mit dem Namen verwenden **`AWSServiceRoleForServiceCatalogSync`**— Diese dienstverknüpfte Rolle ist erforderlich, AWS Service Catalog um AWS Service Catalog Bereitstellungsartefakte für ein Produkt zu verwenden CodeConnections und zu erstellen, zu aktualisieren und zu beschreiben.

Die serviceverknüpfte Rolle `AWSServiceRoleForServiceCatalogSync` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `sync.servicecatalog.amazonaws.com`

Die genannte Richtlinie für Rollenberechtigungen AWSServiceCatalogSyncServiceRolePolicyermöglicht es AWS Service Catalog , die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktion: `Connection` für `CodeConnections`
- Aktion: `Create, Update, and Describe` aktiviert `ProvisioningArtifact` für ein AWS Service Catalog Produkt

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Erstellen der serviceverknüpfte **`AWSServiceRoleForServiceCatalogSync`**-Rolle

Sie müssen die `AWSServiceRoleForServiceCatalogSync` serviceverknüpfte Rolle nicht manuell erstellen. AWS Service Catalog erstellt die dienstbezogene Rolle automatisch für Sie, wenn Sie sie CodeConnections in der AWS Management Console, der oder der AWS CLI AWS API einrichten.

> **Important**
>
> Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Service abgeschlossen haben, der die von dieser Rolle unterstützten Features verwendet. Außerdem gilt: Wenn Sie den AWS Service Catalog Dienst vor dem 18. November 2022 genutzt haben, als er begann, dienstbezogene Rollen zu unterstützen, haben Sie die `AWSServiceRoleForServiceCatalogSync` Rolle dann in Ihrem Konto AWS Service Catalog erstellt. Weitere Informationen finden Sie unter In meinem IAM-Konto wird eine neue Rolle angezeigt.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Bei der Einrichtung AWS Service Catalog wird CodeConnections die dienstbezogene Rolle erneut für Sie erstellt.

Sie können die IAM-Konsole auch verwenden, um eine serviceverknüpfte Rolle mit dem Anwendungsfall „Synchronisierte AWS Service Catalog Produkte“ zu erstellen. Erstellen Sie in der AWS CLI oder der AWS API eine dienstverknüpfte Rolle mit dem Dienstnamen. `sync.servicecatalog.amazonaws.com` Weitere Informationen finden Sie unter Erstellen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch. Wenn Sie diese serviceverknüpfte Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Berechtigungen von serviceverknüpften Rollen für **`AWSServiceRoleForServiceCatalogOrgsDataSync`**

AWS Service Catalog kann die mit dem Dienst verknüpfte Rolle mit dem Namen verwenden **`AWSServiceRoleForServiceCatalogOrgsDataSync`**— Diese dienstbezogene Rolle ist erforderlich, damit AWS Service Catalog Organisationen auf dem Laufenden bleiben können. AWS Organizations

Die serviceverknüpfte Rolle `AWSServiceRoleForServiceCatalogOrgsDataSync` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `orgsdatasync.servicecatalog.amazonaws.com`

Für die `AWSServiceRoleForServiceCatalogOrgsDataSync` dienstverknüpfte Rolle müssen Sie zusätzlich zur verwalteten Richtlinie die folgende Vertrauensrichtlinie verwenden: `AWSServiceCatalogOrgsDataSyncServiceRolePolicy`

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

Die genannte Richtlinie für Rollenberechtigungen AWSServiceCatalogOrgsDataSyncServiceRolePolicy AWS Service Catalog ermöglicht es, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktion: `DescribeAccountDescribeOrganization`, und `ListAWSServiceAccessForOrganization` weiter `Organizations accounts`
- Aktion: `ListAccountsListChildren`, und `ListParent` weiter `Organizations accounts`

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Erstellen der serviceverknüpfte **`AWSServiceRoleForServiceCatalogOrgsDataSync`**-Rolle

Sie müssen die `AWSServiceRoleForServiceCatalogOrgsDataSync` serviceverknüpfte Rolle nicht manuell erstellen. AWS Service Catalog betrachtet Ihre Aktion der Aktivierung Freigeben für AWS Organizations oder Freigeben eines Portfolios als Erlaubnis, in Ihrem Namen eine Spiegelreflexkamera im Hintergrund AWS Service Catalog zu erstellen.

AWS Service Catalog erstellt die dienstbezogene Rolle automatisch für Sie, wenn Sie `EnableAWSOrganizationsAccess` oder `CreatePortfolioShare` in der AWS Management Console, der oder der AWS CLI AWS API anfordern.

> **Important**
>
> Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Service abgeschlossen haben, der die von dieser Rolle unterstützten Features verwendet. Weitere Informationen finden Sie unter In meinem IAM-Konto wird eine neue Rolle angezeigt.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie `EnableAWSOrganizationsAccess` oder anfordern`CreatePortfolioShare`, AWS Service Catalog wird die serviceverknüpfte Rolle erneut für Sie erstellt.

Bearbeiten einer serviceverknüpften Rolle für AWS Service Catalog

AWS Service Catalog erlaubt Ihnen nicht, die `AWSServiceRoleForServiceCatalogSync` oder die `AWSServiceRoleForServiceCatalogOrgsDataSync` dienstbezogenen Rollen zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für AWS Service Catalog

Sie können die IAM-Konsole, die AWS CLI oder die AWS API verwenden, um die `AWSServiceRoleForServiceCatalogSync` oder `AWSServiceRoleForServiceCatalogOrgsDataSync` SLR manuell zu löschen. Dazu müssen Sie zuerst alle Ressourcen manuell entfernen, die die serviceverknüpfte Rolle verwenden (z. B. alle AWS Service Catalog Produkte, die mit einem externen Repository synchronisiert sind). Anschließend kann die dienstverknüpfte Rolle manuell gelöscht werden.

Unterstützte Regionen für serviceverknüpfte AWS Service Catalog -Rollen

AWS Service Catalog unterstützt die Verwendung von dienstbezogenen Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter AWS -Regionen und -Endpunkte.

Name der Region	Regions-ID	Support in AWS Service Catalog
USA Ost (Nord-Virginia)	us-east-1	Ja
USA Ost (Ohio)	us-east-2	Ja
USA West (Nordkalifornien)	us-west-1	Ja
USA West (Oregon)	us-west-2	Ja
Afrika (Kapstadt)	af-south-1	Ja
Asien-Pazifik (Hongkong)	ap-east-1	Ja
Asien-Pazifik (Jakarta)	ap-southeast-3	Ja

Name der Region	Regions-ID	Support in AWS Service Catalog
Asien-Pazifik (Mumbai)	ap-south-1	Ja
Asien-Pazifik (Osaka)	ap-northeast-3	Ja
Asien-Pazifik (Seoul)	ap-northeast-2	Ja
Asien-Pazifik (Singapore)	ap-southeast-1	Ja
Asien-Pazifik (Sydney)	ap-southeast-2	Ja
Asien-Pazifik (Tokyo)	ap-northeast-1	Ja
Kanada (Zentral)	ca-central-1	Ja
Europa (Frankfurt)	eu-central-1	Ja
Europa (Ireland)	eu-west-1	Ja
Europa (London)	eu-west-2	Ja
Europa (Mailand)	eu-south-1	Ja
Europa (Paris)	eu-west-3	Ja
Europa (Stockholm)	eu-north-1	Ja
Naher Osten (Bahrain)	me-south-1	Ja
Südamerika (São Paulo)	sa-east-1	Ja
AWS GovCloud (US-Ost)	us-gov-east-1	Nein
AWS GovCloud (US-West)	us-gov-west-1	Nein

Problembehandlung bei AWS Service Catalog Identität und Zugriff

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit AWS Service Catalog IAM auftreten können.

Themen

- Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Service Catalog
- Ich bin nicht zur Ausführung von iam:PassRole autorisiert.
- Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine AWS Service Catalog Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion durchzuführen in AWS Service Catalog

Wenn Ihnen AWS Management Console mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion durchzuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt. Der folgende Beispielfehler tritt auf, wenn der Benutzer mateojackson versucht, die Konsole zu verwenden, um Details zu einer fiktiven my-example-widget Ressource anzuzeigen, aber nicht über die fiktiven Berechtigungen verfügt. `aws:GetWidget`

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

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung seiner Richtlinien, um unter Verwendung der Aktion `my-example-widget` auf die Ressource `aws:GetWidget` zugreifen zu können.

Ich bin nicht zur Ausführung von **`iam:PassRole`** autorisiert.

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Ausführung der `iam:PassRole` Aktion autorisiert sind, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator ist die Person, die Ihnen Ihren Benutzernamen und Ihr Passwort bereitgestellt hat. Bitten Sie diese Person um die Aktualisierung Ihrer Richtlinien, um eine Rolle an AWS Service Catalogübergeben zu können.

Bei einigen AWS Diensten können Sie eine bestehende Rolle an diesen Dienst übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein Benutzer namens marymajor versucht, über die Konsole eine Aktion in auszuführen. AWS Service Catalog Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Service-Rolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Service.

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

In diesem Fall bittet Mary ihren Administrator, ihre Richtlinien zu aktualisieren, damit sie die Aktion iam: PassRole ausführen kann.

Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine AWS Service Catalog Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob diese Funktionen AWS Service Catalog unterstützt werden, finden Sie AWS Identity and Access ManagementAWS Service Catalog im AWS Service Catalog Administratorhandbuch.
- Informationen dazu, wie Sie den Zugriff auf Ihre Ressourcen mit Ihren AWS Konten gewähren können, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS Konto, das Sie besitzen.
- Informationen dazu, wie Sie AWS Konten von Drittanbietern Zugriff auf Ihre Ressourcen gewähren, finden Sie im IAM-Benutzerhandbuch unter Zugriff auf AWS Konten, die Dritten gehören.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Zugriffssteuerung

Ein AWS Service Catalog Portfolio bietet Ihren Administratoren ein gewisses Maß an Zugriffskontrolle für Ihre Gruppen von Endbenutzern. Zu einem Portfolio hinzugefügte Benutzer können das Portfolio

nach allen Produkten durchsuchen und diese starten. Weitere Informationen finden Sie unter the section called “Verwalten von Portfolios”.

Beschränkungen

Einschränkungen steuern, welche Regeln auf Ihre Endbenutzer angewendet werden, wenn diese ein Produkt aus einem bestimmten Portfolio starten. Mithilfe von Einschränkungen wenden Sie Grenzwerte für Governance oder Kostenkontrolle auf Produkte an. Weitere Informationen zu den Einschränkungen finden Sie unter the section called “Verwenden von Einschränkungen”.

AWS Service Catalog Mit Startbeschränkungen haben Sie mehr Kontrolle über die Berechtigungen, die ein Endbenutzer benötigt. Wenn Ihr Administrator eine Starteinschränkung für ein Produkt in einem Portfolio erstellt, ordnet die Starteinschränkung einen Rollen-ARN zu, der verwendet wird, wenn Ihre Endbenutzer das Produkt aus diesem Portfolio starten. Mithilfe dieses Musters können Sie den Zugriff auf die AWS Ressourcenerstellung steuern. Weitere Informationen finden Sie unter the section called “Starteinschränkungen”.

Einloggen und Überwachen AWS Service Catalog

AWS Service Catalog integriert mit AWS CloudTrail, einem Service, der alle AWS Service Catalog API-Aufrufe erfasst und die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket übermittelt. Weitere Informationen finden Sie unter Protokollieren von AWS Service Catalog API-Aufrufen mit CloudTrail.

Sie können auch Benachrichtigungsbeschränkungen verwenden, um Amazon SNS SNS-Benachrichtigungen über Stack-Ereignisse einzurichten. Weitere Informationen finden Sie unter the section called “Benachrichtigungseinschränkungen”.

Konformitätsüberprüfung für AWS Service Catalog

Externe Prüfer bewerten die Sicherheit und Einhaltung von Vorschriften im AWS Service Catalog Rahmen mehrerer AWS Compliance-Programme, darunter die folgenden:

- System and Organization Controls (SOC)
- Payment Card Industry Data Security Standard (PCI DSS)
- Federal Risk and Authorization Management Program (FedRAMP)
- Health Insurance Portability and Accountability Act (HIPAA)

Eine Liste der AWS Services im Rahmen bestimmter Compliance-Programme finden Sie unter AWS-Services in Umfang nach Compliance-Programmen. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern herunterladen unter AWS Artifact. Weitere Informationen finden Sie unter Herunterladen von Berichten in AWS -Artifact.

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS Service Catalog hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, um Sie bei der Einhaltung der Vorschriften zu unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Umgebungen beschrieben, auf denen auf Sicherheit und Compliance ausgerichtete Basisumgebungen eingerichtet werden. AWS
- Whitepaper „Architecting for HIPAA Security and Compliance“ — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-konforme Anwendungen entwickeln können. AWS
- AWS Ressourcen zur Einhaltung von Vorschriften — Diese Sammlung von Arbeitsmappen und Leitfäden könnte auf Ihre Branche und Ihren Standort zutreffen.
- AWS Config— Dieser AWS Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Dieser AWS Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus und hilft Ihnen AWS , die Einhaltung der Sicherheitsstandards und bewährten Verfahren der Sicherheitsbranche zu überprüfen.

Resilienz in AWS Service Catalog

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

AWS Service Catalog Bietet zusätzlich zur AWS globalen Infrastruktur AWS Service Catalog Self-Service-Aktionen. Mit Self-Service-Aktionen können Kunden die administrative Wartung und die Schulung von Endbenutzern bei gleichzeitiger Konformität mit Compliance- und Sicherheitsanforderungen reduzieren. Self-Service-Aktionen ermöglichen es Ihnen (als Administrator), Endbenutzern das Ausführen operativer Aufgaben wie Sichern und Wiederherstellen, das Beheben von Problemen, das Ausführen von genehmigten Befehlen und das Ändern von Berechtigungen in AWS Service Catalog zu erlauben. Weitere Informationen hierzu finden Sie unter the section called “Verwenden von Service-Aktionen”.

Sicherheit der Infrastruktur in AWS Service Catalog

Als verwalteter Dienst AWS Service Catalog ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff AWS Service Catalog über das Netzwerk. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Mit AWS Service Catalog können Sie die Regionen steuern, in denen Daten gespeichert werden. Portfolios und Produkte sind nur in den Regionen verfügbar, in denen Sie sie verfügbar gemacht haben. Mit der `CopyProduct`-API können Sie ein Produkt in eine andere Region kopieren.

Bewährte Sicherheitsmethoden für AWS Service Catalog

AWS Service Catalog bietet eine Reihe von Sicherheitsfunktionen, die Sie bei der Entwicklung und Implementierung Ihrer eigenen Sicherheitsrichtlinien berücksichtigen sollten. Die folgenden bewährten Methoden sind allgemeine Richtlinien und keine vollständige Sicherheitslösung. Da diese bewährten Methoden für Ihre Umgebung möglicherweise nicht angemessen oder ausreichend sind, sollten Sie sie als hilfreiche Überlegungen und nicht als bindend ansehen.

Sie können Regeln definieren, die die durch einen Benutzer beim Start eines Produkts eingegebenen Parameterwerte begrenzen. Diese Regeln werden als „Vorlageeinschränkungen“ bezeichnet, da sie die Art der Bereitstellung der AWS CloudFormation -Vorlage für das Produkt einschränken. Die Erstellung von Vorlageeinschränkungen erfolgt mittels eines einfachen Editors. Sie wenden sie dann auf einzelne Produkte an.

AWS Service Catalog wendet Einschränkungen an, wenn ein neues Produkt bereitgestellt oder ein Produkt aktualisiert wird, das bereits verwendet wird. Es wird immer die strengste aller für das Portfolio und das Produkt erstellten Einschränkungen angewendet. Stellen Sie sich beispielsweise ein Szenario vor, in dem das Produkt den Start aller Amazon EC2 EC2-Instances ermöglicht und das Portfolio zwei Einschränkungen hat: eine, die den Start aller EC2-Instances vom Typ GPU ermöglicht, und eine, bei der nur t1.micro- und m1.small EC2-Instances gestartet werden können. In diesem Beispiel AWS Service Catalog gilt die zweite, restriktivere Einschränkung (t1.micro und m1.small).

Sie können den Zugriff von Endbenutzern auf AWS Ressourcen einschränken, wenn Sie einer Startrolle eine IAM-Richtlinie zuordnen. Anschließend erstellen Sie eine Startbeschränkung, um die Rolle beim Start des Produkts zu verwenden. AWS Service Catalog

Weitere Informationen zu verwalteten Richtlinien für AWS Service Catalog finden Sie unter AWS Verwaltete Richtlinien für AWS Service Catalog.

Verwalten von Katalogen

AWS Service Catalog bietet eine Schnittstelle für die Verwaltung von Portfolios, Produkten und Einschränkungen von einer Administratorkonsole aus.

> **Note**
>
> Um die Aufgaben in diesem Abschnitt auszuführen, müssen Sie über Administratorrechte für AWS Service Catalog verfügen. Weitere Informationen finden Sie unter Identity and Access Management in AWS Service Catalog.

Aufgaben

- Verwalten von Portfolios
- Verwalten von Produkten
- Verwenden von AWS Service Catalog-Einschränkungen
- AWS Service Catalog-Service-Aktionen
- Hinzufügen von AWS Marketplace-Produkten zu Ihrem Portfolio
- Verwenden von AWS CloudFormation StackSets
- Verwalten von Budgets

Verwalten von Portfolios

Sie können Portfolios auf der Seite Portfolios in der AWS Service Catalog Administratorkonsole erstellen, anzeigen und aktualisieren.

Aufgaben

- Erstellen, Anzeigen und Löschen von Portfolios
- Anzeigen von Portfoliodetails
- Erstellen und Löschen von Portfolios
- Hinzufügen von Produkten
- Hinzufügen von Einschränkungen
- Gewähren des Zugriffs für Benutzer

- Freigeben eines Portfolios
- Freigeben und Importieren von Portfolios

Erstellen, Anzeigen und Löschen von Portfolios

Auf der Seite Portfolios wird eine Liste der Portfolios angezeigt, die Sie in der aktuellen Region erstellt haben. Verwenden Sie diese Seite, um neue Portfolios zu erstellen, die Details eines Portfolios anzuzeigen oder Portfolios in Ihrem Konto zu löschen.

So zeigen Sie die Seite Portfolios an

1. Öffnen Sie die Service-Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie ggf. eine andere Region aus.
3. Wenn Sie noch nicht mit AWS Service Catalog gearbeitet haben, wird die AWS Service Catalog-Startseite angezeigt. Wählen Sie Get started, um ein Portfolio zu erstellen. Folgen Sie den Anweisungen, um Ihr erstes Portfolio zu erstellen, und fahren Sie dann mit der Portfolios-Seite fort.

Während Sie verwendenAWS Service Catalog, können Sie jederzeit zur Portfolios-Seite zurückkehren. Wählen Sie Service Catalog in der Navigationsleiste und dann Portfolios aus.

Anzeigen von Portfoliodetails

In der AWS Service Catalog-Administratorkonsole werden auf der Seite Portfoliodetails die Einstellungen für ein Portfolio aufgeführt. Verwenden Sie diese Seite, um die Produkte im Portfolio zu verwalten, Benutzern Zugriff auf Produkte zu gewähren und TagOptions - und -Einschränkungen anzuwenden.

So zeigen Sie die Seite Portfolio details an

1. Öffnen Sie die Service-Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie das Portfolio aus, das Sie verwalten möchten.

Erstellen und Löschen von Portfolios

Verwenden Sie die Seite Portfolios, um Portfolios zu erstellen und zu löschen.

So erstellen Sie eine neues Portfolio

1. Wählen Sie im linken Navigationsmenü Portfolios aus.
2. Wählen Sie Portfolio erstellen aus.
3. Geben Sie auf der Seite Portfolio erstellen die angeforderten Informationen ein.
4. Wählen Sie Erstellen. AWS Service Catalog erstellt das Portfolio und zeigt die Portfoliodetails an.

So löschen Sie ein Portfolio

> **Note**
>
> Sie können nur lokale Portfolios löschen. Sie können importierte (freigegebene) Portfolios entfernen, importierte Portfolios können jedoch nicht gelöscht werden.

Bevor Sie ein Portfolio löschen können, müssen Sie alle seine Produkte, Einschränkungen, Gruppen, Rollen, Benutzer, Freigaben und entfernen TagOptions. Öffnen Sie dazu ein Portfolio, um die Portfolio-Details anzuzeigen. Wählen Sie dann eine Registerkarte aus, um sie zu entfernen.

> **Note**
>
> Um Fehler zu vermeiden, entfernen Sie die Einschränkungen aus dem Portfolio, bevor Sie Produkte entfernen.

1. Wählen Sie im linken Navigationsmenü Portfolios aus.
2. Wählen Sie das Portfolio aus, das Sie löschen möchten.
3. Wählen Sie Löschen aus. Sie können nur lokale Portfolios löschen. Wenn Sie versuchen, ein importiertes (freigegebenes) Portfolio zu löschen, ist das Menü Aktionen nicht verfügbar.
4. Wählen Sie im Bestätigungsfenster Delete.

Hinzufügen von Produkten

Sie können einem Portfolio Produkte hinzufügen, indem Sie ein neues Produkt direkt in ein vorhandenes Portfolio hochladen oder ein vorhandenes Produkt aus Ihrem Katalog dem Portfolio zuordnen.

> **Note**
>
> Wenn Sie ein AWS Service Catalog Produkt erstellen, können Sie eine -AWS CloudFormationVorlage oder eine Terraform-Konfigurationsdatei hochladen. Die AWS CloudFormation Vorlage wird in einem Amazon Simple Storage Service (Amazon S3)-Bucket gespeichert und der Bucket-Name beginnt mit „cf-templates-“. Sie müssen auch über die Berechtigung verfügen, Objekte aus zusätzlichen Buckets abzurufen, wenn Sie ein Produkt bereitstellen. Weitere Informationen finden Sie unter Erstellen von Produkten.

Hinzufügen eines neuen Produkts

Sie fügen neue Produkte direkt auf der Seite mit den Portfolio-Details hinzu. Wenn Sie auf dieser Seite ein Produkt erstellen, wird es von AWS Service Catalog dem ausgewählten Portfolio hinzugefügt.

So fügen Sie ein neues Produkt hinzu

1. Navigieren Sie zur Seite Portfolios und wählen Sie dann den Namen des Portfolios aus, dem Sie das Produkt hinzufügen möchten.
2. Erweitern Sie auf der Seite mit den Portfoliodetails den Abschnitt Produkte und wählen Sie dann Neues Produkt hochladen aus.
3. Geben Sie unter Enter product details Folgendes ein:

   - Product name – Der Name des Produkts.
   - Produktbeschreibung (optional) – Die Produktbeschreibung. Diese Beschreibung wird in der Produktauflistung angezeigt, um Ihnen bei der Auswahl des richtigen Produkts zu helfen.
   - Beschreibung – Die vollständige Beschreibung. Diese Beschreibung wird in der Produktauflistung angezeigt, um Ihnen bei der Auswahl des richtigen Produkts zu helfen.
   - Eigentümer oder Distributor – Der Name oder die E-Mail-Adresse des Eigentümers. Die Kontaktinformationen für den Lieferanten sind optional.
   - Anbieter (optional) – Der Name des Herausgebers der Anwendung. In diesem Feld können Sie die Produktliste sortieren, um das Auffinden von Produkten zu erleichtern.
4. Geben Sie auf der Seite Version details die folgenden Informationen ein:

   - Vorlage auswählen – Wählen Sie für -AWS CloudFormationProdukte Ihre eigene Vorlagendatei, eine -AWS CloudFormationVorlage aus einem lokalen Laufwerk oder eine URL

aus, die auf eine in Amazon S3 gespeicherte Vorlage, eine vorhandene AWS CloudFormation Stack-ARN-Vorlage oder eine in einem externen Repository gespeicherte Vorlagendatei verweist.

Wählen Sie für Teraform-Produkte Ihre eigene Vorlagendatei, eine tar.gz-Konfigurationsdatei von einem lokalen Laufwerk oder eine URL aus, die auf eine in Amazon S3 gespeicherte Vorlage verweist, oder eine tar.gz-Konfigurationsdatei, die in einem externen Repository gespeichert ist.

- Versionsname (optional) – Der Name der Produktversion (z. B. „v1“, „v2beta“). Leerzeichen sind nicht zulässig.
- Description (optional) – Eine Beschreibung der Produktversion, einschließlich Unterschiede zur vorherigen Version.

5. Geben Sie unter Enter support details Folgendes ein:

   - Email contact (optional) – Die E-Mail-Adresse zum Melden von Problemen mit dem Produkt.
   - Support-Link (optional) – Eine URL zu einer Website, auf der Benutzer Support-Informationen finden oder Tickets einreichen können. Die URL muss mit `http://` oder `https://` beginnen. Administratoren sind für die Aufrechterhaltung der Genauigkeit und des Zugriffs auf Support-Informationen verantwortlich.
   - Supportbeschreibung (optional) – Eine Beschreibung, wie Sie den Link E-Mail-Kontakt und Support verwenden sollten.

6. Wählen Sie Produkt erstellen aus.

Hinzufügen eines vorhandenen Produkts

Sie können einem Portfolio aus drei Stellen bestehende Produkte hinzufügen: Portfolioliste, Portfoliodetailseite oder Produktliste.

So fügen Sie einem Portfolio ein vorhandenes Produkt hinzu

1. Navigieren Sie zur Seite Portfolios.
2. Wählen Sie ein Portfolio aus. Wählen Sie dann Aktionen – Produkt zum Portfolio hinzufügen aus.
3. Wählen Sie ein Produkt und dann Produkt zum Portfolio hinzufügen aus.

Entfernen eines Produkts aus einem Portfolio

Wenn Sie ein Produkt nicht mehr verwenden möchten, entfernen Sie es aus einem Portfolio. Das Produkt ist weiterhin in Ihrem Katalog auf der Seite Produkte verfügbar, und Sie können es weiterhin zu anderen Portfolios hinzufügen. Sie können mehrere Produkte gleichzeitig aus einem Portfolio entfernen.

So entfernen Sie ein Produkt aus einem Portfolio

1. Navigieren Sie zur Seite Portfolios und wählen Sie dann das Portfolio aus, das das Produkt enthält. Die Seite mit den Portfolio-Details wird geöffnet.
2. Erweitern Sie den Abschnitt Produkte.
3. Wählen Sie ein oder mehrere Produkte und dann Entfernen aus.
4. Bestätigen Sie Ihre Auswahl.

Hinzufügen von Einschränkungen

Sie sollten Einschränkungen hinzufügen, um zu steuern, wie Benutzer mit -Produkten interagieren. Weitere Informationen zu den Arten von Einschränkungen, die AWS Service Catalog unterstützt, finden Sie unter Verwenden von AWS Service Catalog-Einschränkungen.

Einschränkungen werden Produkten hinzugefügt, nachdem sie in ein Portfolio eingefügt wurden.

So fügen Sie einem Produkt eine Einschränkung hinzu

1. Öffnen Sie die Service-Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie Portfolios und dann ein Portfolio aus.
3. Erweitern Sie auf der Seite mit den Portfoliodetails den Abschnitt Einschränkung erstellen und wählen Sie Einschränkungen hinzufügen aus.
4. Wählen Sie für Produkt das Produkt aus, auf das die Einschränkung angewendet werden soll.
5. Wählen Sie für Einschränkungstyp eine der folgenden Optionen aus:

   Start – Ermöglicht Ihnen, dem Produkt eine IAM-Rolle zuzuweisen, die zur Bereitstellung der AWS Ressourcen verwendet wird. Weitere Informationen finden Sie unter AWS Service Catalog-Starteinschränkungen.

Benachrichtigung – Ermöglicht das Streamen von Produktbenachrichtigungen an ein Amazon SNS-Thema. Weitere Informationen finden Sie unter AWS Service Catalog-Benachrichtigungseinschränkungen.

Vorlage – Ermöglicht es Ihnen, die Optionen einzuschränken, die Endbenutzern beim Starten des Produkts zur Verfügung stehen. Eine Vorlage besteht aus einer JSON-formatierten Textdatei, die eine oder mehrere Regeln enthält. Regeln werden der AWS CloudFormation-Vorlage, die vom Produkt verwendet wird, hinzugefügt. Weitere Informationen finden Sie unter Vorlageneinschränkungsregeln.

Stack-Set – Ermöglicht es Ihnen, die Produktbereitstellung über -Konten und -Regionen hinweg mithilfe von zu konfigurierenAWS CloudFormation StackSets. Weitere Informationen finden Sie unter AWS Service Catalog-Stack-Set-Einschränkungen.

Tag-Aktualisierung – Ermöglicht Ihnen, Tags zu aktualisieren, nachdem das Produkt bereitgestellt wurde. Weitere Informationen finden Sie unter AWS Service Catalog Tag-Aktualisierungseinschränkungen.

6. Wählen Sie Weiter und geben Sie die erforderlichen Informationen ein.

So bearbeiten Sie eine Einschränkung

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Service Catalog Administratorkonsole unter https://console.aws.amazon.com/catalog/.
2. Wählen Sie Portfolios und dann ein Portfolio aus.
3. Erweitern Sie auf der Seite Portfoliodetails den Abschnitt Einschränkung erstellen und wählen Sie die zu bearbeitende Einschränkung aus.
4. Wählen Sie Einschränkungen bearbeiten aus.
5. Bearbeiten Sie die Einschränkung nach Bedarf und wählen Sie Speichern aus.

Gewähren des Zugriffs für Benutzer

Gewähren Sie Benutzern über Gruppen oder Rollen Zugriff auf Portfolios. Die beste Möglichkeit, vielen Benutzern Portfoliozugriff zu gewähren, besteht darin, die Benutzer in eine IAM-Gruppe zu platzieren und Zugriff auf diese Gruppe zu gewähren. Auf diese Weise können Sie den Portfoliozugriff verwalten, indem Sie einfach Benutzer hinzufügen und aus der Gruppe entfernen. Weitere Informationen finden Sie unter IAM-Benutzer und -Gruppen im IAM-Benutzerhandbuch.

Zusätzlich zum Zugriff auf ein Portfolio müssen Benutzer auch Zugriff auf die AWS Service Catalog Endbenutzerkonsole haben. Sie gewähren Zugriff auf die Konsole, indem Sie Berechtigungen in IAM anwenden. Weitere Informationen finden Sie unter Identity and Access Management in AWS Service Catalog.

Wenn Sie ein Portfolio und seine Prinzipale für andere Konten freigeben möchten, können Sie dem Portfolio Prinzipalnamen (Gruppen, Rollen oder Benutzer) zuordnen. Prinzipalnamen werden mit dem Portfolio geteilt und in Empfängerkonten verwendet, um Endbenutzern Zugriff zu gewähren.

So gewähren Sie Benutzern oder Gruppen Portfoliozugriff

1. Öffnen Sie die Service-Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie im Navigationsbereich Administration und dann Portfolios aus.
3. Wählen Sie ein Portfolio aus, für das Sie Gruppen, Rollen oder Benutzern Zugriff gewähren möchten. AWS Service Catalog leitet zur Seite mit den Portfolio-Details weiter.
4. Wählen Sie auf der Seite Portfolio-Details die Registerkarte Zugriff aus.
5. Wählen Sie unter Portfoliozugriff die Option Zugriff gewähren aus.
6. Wählen Sie für Typ die Option Prinzipalname und dann die Gruppe/, Rolle/ oder Benutzer/, Typ aus. Sie können bis zu 9 Prinzipalnamen hinzufügen.
7. Wählen Sie Zugriff gewähren, um den Prinzipal dem aktuellen Portfolio zuzuordnen.

So entfernen Sie den Zugriff auf ein Portfolio

1. Wählen Sie auf der Seite Portfolio-Details eine Gruppe, Rolle oder einen Benutzernamen aus.
2. Wählen Sie Zugriff entfernen aus.

Freigeben eines Portfolios

Um einem AWS Service Catalog Administrator für ein anderes AWS Konto zu ermöglichen, Ihre Produkte an Endbenutzer zu verteilen, geben Sie Ihr AWS Service Catalog Portfolio entweder über die account-to-account Freigabe oder für sie freiAWS Organizations.

Wenn Sie ein Portfolio mithilfe account-to-account von Freigabe oder Organizations freigeben, teilen Sie sich eine Referenz dieses Portfolios. Die Produkte und Einschränkungen des importierten Portfolios bleiben mit Änderungen, die Sie am freigegebenen Portfolio, d. h. ursprünglichen Portfolio, vornehmen, synchron.

Der Empfänger kann die Produkte oder Einschränkungen nicht ändern, kann aber den AWS Identity and Access Management Zugriff für Endbenutzer hinzufügen.

> **Note**
>
> Sie können eine freigegebene Ressource nicht freigeben. Dazu gehören Portfolios, die ein freigegebenes Produkt enthalten.

Eine ccount-to-account Freigabe

Um diese Schritte auszuführen, müssen Sie die Konto-ID des AWS Zielkontos abrufen. Sie finden die ID auf der Seite Mein Konto im des AWS Management Console Zielkontos.

So geben Sie ein Portfolio für ein AWS Konto frei

1. Öffnen Sie die Service-Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie im linken Navigationsmenü Portfolios und dann das Portfolio aus, das Sie teilen möchten. Wählen Sie im Menü Aktionen die Option Teilen aus.
3. Geben Sie unter Konto-ID eingeben die Konto-ID des AWS Kontos ein, für das Sie die Freigabe durchführen. (Optional) Wählen Sie TagOption Freigabe aus. Wählen Sie dann Teilen aus.
4. Senden Sie die URL an den AWS Service Catalog-Administrator des Zielkontos. Die URL öffnet die Seite Portfolio importieren mit dem ARN des freigegebenen Portfolios, das automatisch bereitgestellt wird.

Importieren eines Portfolios

Wenn ein AWS Service Catalog Administrator für ein anderes AWS Konto ein Portfolio für Sie freigibt, importieren Sie dieses Portfolio in Ihr Konto, damit Sie seine Produkte an Ihre Endbenutzer verteilen können.

Sie müssen kein Portfolio importieren, wenn das Portfolio über freigegeben wurdeAWS Organizations.

Um das Portfolio zu importieren, müssen Sie die Portfolio-ID vom Administrator abrufen.

Um alle importierten Portfolios anzuzeigen, öffnen Sie die -AWS Service CatalogKonsole unter https://console.aws.amazon.com/servicecatalog/. Wählen Sie auf der Seite Portfolios die Registerkarte Importiert aus. Überprüfen Sie die Tabelle Importierte Portfolios.

Freigeben für AWS Organizations

Sie können AWS Service Catalog-Portfolios mit AWS Organizations freigeben.

Zuerst müssen Sie entscheiden, ob Sie die Freigabe über das Verwaltungskonto oder ein delegiertes Administratorkonto vornehmen. Wenn Sie nicht von Ihrem Verwaltungskonto aus freigeben möchten, registrieren Sie ein delegiertes Administratorkonto, das Sie für die Freigabe verwenden können. Weitere Informationen finden Sie unter Einen delegierten Administrator registrieren im Benutzerhandbuch für AWS CloudFormation.

Als nächstes müssen Sie entscheiden, für wen die Freigabe gelten soll. Sie können Freigaben für die folgenden Entitäten durchführen:

- Ein Organisationskonto.
- Eine Organisationseinheit (OU).
- Die Organisation selbst. (Dabei gilt die Freigabe für jedes Konto in der Organisation.)

Freigabe von einem Verwaltungskonto aus

Sie können ein Portfolio für eine Organisation freigeben, wenn Sie Ihre Organisationsstruktur verwenden oder die ID eines Organisationsknotens eingeben.

So geben Sie ein Portfolio mithilfe der Organisationsstruktur für eine Organisation frei

1. Öffnen Sie die -AWS Service CatalogKonsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie auf der Seite Portfolios das Portfolio aus, das Sie teilen möchten. Wählen Sie im Menü Aktionen die Option Teilen aus.
3. Wählen Sie Ihre Organisationsstruktur aus AWS Organizations und filtern Sie sie.

   Sie können den Root-Knoten auswählen, um das Portfolio für Ihre gesamte Organisation, eine übergeordnete Organisationseinheit (OU), eine untergeordnete Organisationseinheit oder ein AWS Konto innerhalb Ihrer Organisation freizugeben.

   Die Freigabe an eine übergeordnete Organisationseinheit teilt das Portfolio mit allen Konten und untergeordneten Organisationseinheiten innerhalb dieser übergeordneten Organisationseinheit.

   Sie können Nur AWS Konten anzeigen auswählen, um eine Liste aller AWS Konten in Ihrer Organisation anzuzeigen.

So geben Sie ein Portfolio für eine Organisation frei, indem Sie die ID des Organisationsknotens eingeben

1. Öffnen Sie die -AWS Service CatalogKonsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie auf der Seite Portfolios das Portfolio aus, das Sie teilen möchten. Wählen Sie im Menü Aktionen die Option Teilen aus.
3. Wählen Sie Organisationsknoten aus.

   Wählen Sie aus, ob Sie für Ihre gesamte Organisation, ein AWS Konto innerhalb Ihrer Organisation oder eine Organisationseinheit freigeben möchten.

   Geben Sie die ID des ausgewählten Organisationsknotens ein, die Sie in der AWS Organizations Konsole unter https://console.aws.amazon.com/organizations/ finden.

Freigabe von einem delegierten Administratorkonto aus

Das Verwaltungskonto einer Organisation kann andere Konten als delegierte Administratoren für die Organisation registrieren und deren Registrierung aufheben.

Ein delegierter Administrator kann AWS Service Catalog Ressourcen in seiner Organisation genauso freigeben wie ein Verwaltungskonto. Sie sind autorisiert, Portfolios zu erstellen, zu löschen und gemeinsam zu nutzen.

Um einen delegierten Administrator zu registrieren oder abzumelden, müssen Sie die -API oder -CLI aus dem Verwaltungskonto verwenden. Weitere Informationen finden Sie unter RegisterDelegatedAdministrator und DeregisterDelegatedAdministrator in der AWS Organizations-API-Referenz.

> **Note**
>
> Bevor Sie einen Delegierten benennen können, muss der Administrator aufrufen`EnableAWSOrganizationsAccess`.

Das Verfahren zum Freigeben eines Portfolios von einem delegierten Administratorkonto aus ist dasselbe wie das Freigeben von einem Verwaltungskonto, wie oben unter gezeigtthe section called “Freigabe von einem Verwaltungskonto aus”.

Wenn ein Mitglied als delegierter Administrator abgemeldet wird, geschieht Folgendes:

- Portfoliofreigaben, die von diesem Konto erstellt wurden, werden entfernt.
- Sie können keine neuen Portfoliofreigaben mehr erstellen.

> **Note**
>
> Wenn das Portfolio und die von einem delegierten Administrator erstellten Freigaben nicht entfernt werden, nachdem der delegierte Administrator die Registrierung aufgehoben hat, registrieren Sie den delegierten Administrator erneut und heben Sie die Registrierung auf. Diese Aktion entfernt das Portfolio und die von diesem Konto erstellten Freigaben.

Verschieben von Konten innerhalb Ihrer Organisation

Wenn Sie ein Konto innerhalb Ihrer Organisation verschieben, können sich die für das Konto freigegebenen AWS Service Catalog Portfolios ändern.

Konten haben nur Zugriff auf Portfolios, die für ihre Zielorganisation oder Organisationseinheit freigegeben sind.

Freigeben von Portfolios TagOptions beim Freigeben von Portfolios

Als Administrator können Sie eine Freigabe erstellen, die TagOptions. TagOptions are-Schlüssel-Wert-Paare enthält, mit denen Administratoren:

- Definieren und erzwingen Sie die Taxonxie für Tags.
- Definieren Sie Tag-Optionen und verknüpfen Sie sie mit Produkten und Portfolios.
- Teilen Sie Tag-Optionen im Zusammenhang mit Portfolios und Produkten mit anderen Konten.

Wenn Sie Tag-Optionen im Hauptkonto hinzufügen oder entfernen, wird die Änderung automatisch in Empfängerkonten angezeigt. Wenn ein Endbenutzer in Empfängerkonten ein Produkt mit bereitstellt TagOptions, muss er Werte für Tags auswählen, die zu Tags auf dem bereitgestellten Produkt werden.

Administratoren können in Empfängerkonten zusätzliche lokale TagOptions zu ihrem importierten Portfolio zuordnen, um für dieses Konto spezifische Tagging-Regeln zu erzwingen.

> **Note**
>
> Um ein Portfolio freizugeben, benötigen Sie die AWS Konto-ID des Konsumenten. Suchen Sie die AWS Konto-ID in Mein Konto in der -Konsole.

> **Note**
>
> Wenn ein einen einzelnen Wert TagOption hat, erzwingt diesen Wert während des Bereitstellungsprozesses AWS automatisch.

So teilen Sie TagOptions beim Freigeben von Portfolios

1. Wählen Sie im linken Navigationsmenü Portfolios aus.
2. Wählen Sie unter Lokale Portfolios ein Portfolio aus und öffnen Sie es.
3. Wählen Sie Freigabe aus der obigen Liste und dann die Schaltfläche Freigeben aus.
4. Wählen Sie aus, ob Sie für ein anderes AWS Konto oder eine andere Organisation freigeben möchten.
5. Geben Sie die 12-stellige Konto-ID-Nummer ein, wählen Sie Aktivieren und dann Teilen aus.

   Das Konto, das Sie freigegeben haben, wird im Abschnitt Konten, für die freigegeben wurde angezeigt. Es gibt an, ob aktiviert TagOptions wurden.

Sie können eine Portfoliofreigabe auch aktualisieren, um einzuschließen TagOptions. Alle TagOptions , die zum Portfolio und Produkt gehören, teilen sich jetzt mit diesem Konto.

So aktualisieren Sie eine Portfoliofreigabe, um sie einzuschließen TagOptions

1. Wählen Sie im linken Navigationsmenü Portfolios aus.
2. Wählen Sie unter Lokales Portfolio ein Portfolio aus und öffnen Sie es.
3. Wählen Sie Freigabe aus der obigen Liste aus.
4. Wählen Sie unter Konten, die für freigegeben sind eine Konto-ID und dann Aktionen aus.
5. Wählen Sie Aufheben der Freigabe aktualisieren oder Aufheben der Freigabe aus.

Wenn Sie Aufheben der Freigabe aktualisieren auswählen, wählen Sie Aktivieren, um die Freigabe zu initiieren TagOptions. Das Konto, das Sie freigegeben haben, wird im Abschnitt Mit freigegebene Konten angezeigt.

Wenn Sie Freigabe aufheben auswählen, bestätigen Sie, dass Sie das Konto nicht mehr freigeben möchten.

Freigeben von Prinzipalnamen beim Freigeben von Portfolios

Als Administrator können Sie eine Portfoliofreigabe erstellen, die Prinzipalnamen enthält. Prinzipalnamen sind Namen für Gruppen, Rollen und Benutzer, die Administratoren in einem Portfolio angeben und dann mit dem Portfolio teilen können. Wenn Sie das Portfolio freigeben, AWS Service Catalog überprüft , ob diese Prinzipalnamen bereits vorhanden sind. Wenn sie vorhanden sind, ordnet die übereinstimmenden IAM-Prinzipale AWS Service Catalog automatisch dem freigegebenen Portfolio zu, um Benutzern Zugriff zu gewähren.

> **Note**
>
> Wenn Sie einen Prinzipal einem Portfolio zuordnen, kann es zu einer möglichen Ausweitung der Rechte kommen, wenn dieses Portfolio dann mit anderen Konten geteilt wird. Für einen Benutzer in einem Empfängerkonto, der kein AWS Service Catalog Administrator ist, aber immer noch Prinzipale (Benutzer/Rollen) erstellen kann, könnte dieser Benutzer einen IAM-Prinzipal erstellen, der einer Prinzipalnamenzuordnung für das Portfolio entspricht. Obwohl dieser Benutzer möglicherweise nicht weiß, welche Prinzipalnamen durch AWS Service Catalog zugeordnet sind, kann er den Benutzer möglicherweise erraten. Wenn dieser potenzielle Eskalationspfad ein Problem darstellt, empfiehlt AWS Service Catalog die Verwendung von `PrincipalType` als `IAM`. Bei dieser Konfiguration muss das `PrincipalARN` bereits im Empfängerkonto vorhanden sein, bevor es zugeordnet werden kann.

Wenn Sie Prinzipalnamen im Hauptkonto hinzufügen oder entfernen, wendet diese Änderungen AWS Service Catalog automatisch im Empfängerkonto an. Benutzer im Empfängerkonto können dann Aufgaben basierend auf ihrer Rolle ausführen:

- Endbenutzer können das Produkt des Portfolios bereitstellen, aktualisieren und beenden.

- Administratoren können ihrem importierten Portfolio zusätzliche IAM-Prinzipale zuordnen, um Endbenutzern, die für dieses Konto spezifisch sind, Zugriff zu gewähren.

> **Note**
>
> Die Freigabe von Prinzipalnamen ist nur für verfügbarAWS Organizations.

So geben Sie Prinzipalnamen frei, wenn Sie Portfolios freigeben

1. Wählen Sie im linken Navigationsmenü Portfolios aus.
2. Wählen Sie unter Lokale Portfolios das Portfolio aus, das Sie teilen möchten.
3. Wählen Sie im Menü Aktionen die Option Teilen aus.
4. Wählen Sie eine Organisation in ausAWS Organizations.
5. Wählen Sie den gesamten Organisationsstamm , eine Organisationseinheit (OU) oder ein Organisationsmitglied aus.
6. Aktivieren Sie unter Freigabeeinstellungen die Option Prinzipalfreigabe.

Sie können eine Portfoliofreigabe auch aktualisieren, um die Freigabe von Prinzipalnamen einzuschließen. Dadurch werden alle Prinzipalnamen, die zu diesem Portfolio gehören, mit dem Empfängerkonto geteilt.

So aktualisieren Sie eine Portfoliofreigabe, um Prinzipalnamen zu aktivieren oder zu deaktivieren

1. Wählen Sie im linken Navigationsmenü Portfolios aus.
2. Wählen Sie unter Lokales Portfolio das Portfolio aus, das Sie aktualisieren möchten.
3. Wählen Sie die Registerkarte Teilen aus.
4. Wählen Sie die Freigabe aus, die Sie aktualisieren möchten, und wählen Sie dann Teilen aus.
5. Wählen Sie Freigabe aktualisieren und dann Aktivieren aus, um die Freigabe des Prinzipals zu initiieren. gibt AWS Service Catalog dann Prinzipalnamen in Empfängerkonten frei.

Deaktivieren Sie die Freigabe des Prinzipals, wenn Sie die Freigabe der Prinzipalnamen für Empfängerkonten beenden möchten.

Verwenden von Platzhaltern bei der Freigabe von Prinzipalnamen

AWS Service Catalog unterstützt die Gewährung von Portfoliozugriff auf IAM-Prinzipalnamen (Benutzer, Gruppe oder Rolle) mit Platzhaltern wie „*“ oder „?“. Mithilfe von Platzhaltermustern können Sie mehrere IAM-Prinzipalnamen gleichzeitig abdecken. Der ARN-Pfad und der Prinzipalname lassen unbegrenzte Platzhalterzeichen zu.

Beispiele für einen akzeptablen Platzhalter-ARN:

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

Beispiele für einen inakzeptablen Platzhalter-ARN:

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

Gültige Werte im ARN-Format des IAM-Prinzipals (**`arn:partition:iam:::resource-type/resource-path/resource-name`**) sind user/, group/ oder role/. Die „?“ und „*“ sind nur nach dem Ressourcentyp im Ressourcen-ID-Segment zulässig. Sie können Sonderzeichen überall innerhalb der Ressourcen-ID verwenden.

Das Zeichen „*“ entspricht auch dem Zeichen „/“, sodass Pfade innerhalb der Ressourcen-ID gebildet werden können. Beispielsweise:

`arn:aws:iam:::role/*/ResourceName_?` entspricht **`arn:aws:iam:::role/pathA/pathB/ResourceName_1`** sowohl als auch **`arn:aws:iam:::role/pathA/ResourceName_1`**.

Freigeben und Importieren von Portfolios

Um Ihre AWS Service Catalog Produkte Benutzern verfügbar zu machen, die sich nicht in Ihrem befindenAWS-Konten, z. B. Benutzern, die zu anderen Organisationen oder zu anderen AWS-Konten in Ihrer Organisation gehören, geben Sie Ihre Portfolios für sie frei. Sie können auf verschiedene Arten freigeben, einschließlich der account-to-account Freigabe, der Freigabe durch die Organisation und der Bereitstellung von Katalogen mithilfe von Stack-Sets.

Bevor Sie Ihre Produkte und Portfolios für andere Konten freigeben, müssen Sie entscheiden, ob Sie eine Referenz des Katalogs freigeben oder eine Kopie des Katalogs in jedem Empfängerkonto bereitstellen möchten. Beachten Sie, dass Sie beim Bereitstellen einer Kopie die Bereitstellung erneut

durchführen müssen, wenn Updates vorhanden sind, die Sie an die Empfängerkonten weitergeben möchten.

Sie können Stack-Sets verwenden, um Ihren Katalog für viele Konten gleichzeitig bereitzustellen. Wenn Sie eine Referenz (eine importierte Version Ihres Portfolios, die mit dem Original synchron bleibt) freigeben möchten, können Sie die account-to-account Freigabe verwenden oder mit freigebenAWS Organizations.

Informationen zur Verwendung von Stack-Sets zum Bereitstellen einer Kopie Ihres Katalogs finden Sie unter So richten Sie einen regionsübergreifenden Katalog mit AWS Service Catalog Standardprodukten des Unternehmens ein.

Wenn Sie ein Portfolio mit der account-to-account Freigabe von oder teilenAWS Organizations, erlauben Sie einem AWS Service Catalog Administrator eines anderen AWS Kontos, Ihr Portfolio in sein Konto zu importieren und die Produkte an Endbenutzer in diesem Konto zu verteilen.

Dieses importierte Portfolio ist keine unabhängige Kopie. Die Produkte und Einschränkungen des importierten Portfolios bleiben mit Änderungen, die Sie am freigegebenen Portfolio, d. h. ursprünglichen Portfolio, vornehmen, synchron. Der Empfängeradministrator , der Administrator, mit dem Sie ein Portfolio teilen, kann die Produkte oder Einschränkungen nicht ändern, kann aber AWS Identity and Access Management (IAM)-Zugriff für Endbenutzer hinzufügen. Weitere Informationen finden Sie unter Gewähren des Zugriffs für Benutzer.

Der Empfängeradministrator kann die Produkte auf folgende Weise an Endbenutzer verteilen, die zu seinem AWS Konto gehören:

- Durch Hinzufügen von Benutzern, Gruppen und Rollen zum importierten Portfolio.
- Durch das Hinzufügen von Produkten aus dem importierten Portfolio zu einem lokalen Portfolio , einem separaten Portfolio, das der Empfängeradministrator erstellt und zu seinem AWS Konto gehört. Der Empfängeradministrator fügt dann Benutzer, Gruppen und Rollen zu diesem lokalen Portfolio hinzu. Alle Einschränkungen, die ursprünglich auf Produkte im freigegebenen Portfolio angewendet wurden, sind auch im lokalen Portfolio vorhanden. Der lokale Administrator des Portfolioempfängers kann zusätzliche Einschränkungen hinzufügen, die ursprünglich aus dem freigegebenen Portfolio importiert wurden, jedoch nicht entfernen.

Wenn Sie dem freigegebenen Portfolio Produkte oder Einschränkungen hinzufügen oder Produkte oder Einschränkungen daraus entfernen, wird die Änderung auf alle importierten Instances des Portfolios verteilt. Wenn Sie beispielsweise ein Produkt aus dem freigegebenen Portfolio entfernen,

wird dieses Produkt auch aus dem importierten Portfolio entfernt. Außerdem wird es aus allen lokalen Portfolios entfernt, denen das importierte Produkt hinzugefügt wurde. Wenn ein Endbenutzer ein Produkt gestartet hat, bevor Sie es entfernt haben, wird das bereitgestellte Produkt des Endbenutzers weiter ausgeführt, aber das Produkt ist für künftige Starts nicht mehr verfügbar.

Wenn Sie eine Starteinschränkung auf ein Produkt in einem freigegebenen Portfolio anwenden, wird sie auf alle importierten Instances des Produkts übertragen. Um diese Starteinschränkung außer Kraft zu setzen, fügt der Empfänger-Administrator das Produkt einem lokalen Portfolio hinzu und wendet eine andere Starteinschränkung dafür an. Die Starteinschränkung, die in Kraft ist, legt eine Startrolle für das Produkt fest.

Eine Startrolle ist eine IAM-Rolle, die AWS Service Catalog verwendet, um AWS Ressourcen (wie Amazon EC2-Instances oder Amazon-RDS-Datenbanken) bereitzustellen, wenn ein Endbenutzer das Produkt startet. Als Administrator können Sie einen bestimmten Startrollen-ARN oder einen lokalen Rollennamen festlegen. Wenn Sie den Rollen-ARN verwenden, wird die Rolle auch dann verwendet, wenn der Endbenutzer zu einem anderen AWS Konto gehört als das, dem die Startrolle gehört. Wenn Sie einen lokalen Rollennamen verwenden, wird die IAM-Rolle mit diesem Namen im Konto des Endbenutzers verwendet.

Weitere Informationen zu Starteinschränkungen und -rollen finden Sie unter AWS Service Catalog-Starteinschränkungen. Das AWS-Konto, das die Startrolle besitzt, stellt die AWS-Ressourcen bereit. Für dieses Konto fallen nutzungsabhängige Gebühren für diese Ressourcen an. Weitere Informationen finden Sie unter AWS Service Catalog-Preisgestaltung.

Dieses Video zeigt Ihnen, wie Sie Portfolios für mehrere Konten in freigebenAWS Service Catalog.

Teilen Sie (https://www.youtube.com/embed/BVSohYOppjk%22%3EShare) Portfolios über Konten in hinwegAWS Service Catalog.

> **Note**
>
> Sie können Produkte aus einem Portfolio, das importiert oder freigegeben wurde, nicht erneut freigeben.

> **Note**
>
> Portfolioimporte müssen in derselben Region zwischen den Verwaltungs- und abhängigen Konten erfolgen.

Beziehung zwischen freigegebenen und importierten Portfolios

Diese Tabelle fasst die Beziehung zwischen einem importierten Portfolio und einem gemeinsamen Portfolio zusammen und die Aktionen, die ein Administrator, der ein Portfolio importiert, mit diesem Portfolio und den darin enthaltenen Produkten ausführen kann und nicht.

Element des freigegebenen Portfolios	Beziehung zu dem importierten Portfolio	Empfänger-Administrator kann	Empfänger-Administrator kann nicht
Produkte und Produktversionen	Geerbt Wenn der Ersteller des Portfolios Produkte hinzufügt oder aus dem freigegebenen Portfolio entfernt, wird die Änderung auf das importierte Portfolio übertragen.	Importierte Produkte lokalen Portfolios hinzufügen. Die Produkte werden mit dem freigegebenen Portfolio synchronisiert.	Produkte hochladen oder dem importierten Portfolio Produkte hinzufügen bzw. Produkte aus dem importierten Portfolio entfernen.
Starteinschränkungen	Geerbt Wenn der Portfolioersteller Starteinschränkungen zu einem freigegebenen Produkt hinzufügt oder Starteinschränkungen daraus entfernt, wird die Änderung an alle importierten Instances des Produkts weitergegeben.	In einem lokalen Portfolio kann der Administrator Starteinschränkungen anwenden, die sich auf den lokalen Start des Produkts auswirken.	Starteinschränkungen hinzufügen oder aus dem importierten Portfolio entfernen.

Element des freigegebenen Portfolios	Beziehung zu dem importierten Portfolio	Empfänger-Administrator kann	Empfänger-Administrator kann nicht
	Wenn der Empfängeradministrator seinem lokalen Portfolio ein importiertes Produkt hinzufügt, wird diese importierte Starteinschränkung nicht auf das freigegebene Portfolio übertragen.		
Vorlageneinschränkungen	Geerbt Wenn der Ersteller des Portfolios eine Vorlageneinschränkung hinzufügt oder aus einem freigegebenen Produkt entfernt, wird die Änderung auf alle importierten Instances des Produkts verteilt. Wenn der Empfängeradministrator einem lokalen Portfolio ein importiertes Produkt hinzufügt, werden die importierten Vorlageneinschränkungen nicht in das lokale Portfolio übertragen.	In einem lokalen Portfolio kann der Administrator Vorlageneinschränkungen hinzufügen, die das lokale Produkt einschränken.	Die importierten Vorlageneinschränkungen entfernen.

Element des freigegebenen Portfolios	Beziehung zu dem importierten Portfolio	Empfänger-Administrator kann	Empfänger-Administrator kann nicht
Benutzer, Gruppen und Rollen	Nicht geerbt	Fügen Sie Benutzer, Gruppen und Rollen hinzu, die sich im AWS Administratorkonto befinden.	Nicht zutreffend.

Verwalten von Produkten

Sie können Produkte erstellen, Produkte aktualisieren, indem Sie eine neue Version basierend auf einer aktualisierten Vorlage erstellen und Produkte in Portfolios gruppieren, um sie an Benutzer zu verteilen.

Neue Versionen von Produkten werden an alle Benutzer verteilt, die über ein Portfolio Zugriff auf das Produkt haben. Wenn Sie ein Update verteilen, können Endbenutzer vorhandene bereitgestellte Produkte aktualisieren.

Aufgaben

- Anzeigen der Produktseite
- Erstellen von Produkten
- Hinzufügen von Produkten zu Portfolios
- Aktualisieren von Produkten
- Produkte mit Vorlagendateien von GitHub GitHub Enterprise oder Bitbucket synchronisieren
- Löschen von Produkten
- Verwalten von Versionen

Anzeigen der Produktseite

Sie verwalten Produkte auf der Seite Produktliste in der AWS Service Catalog Administratorkonsole.

So zeigen Sie die Seite mit der Produktliste an

1. Öffnen Sie die Service-Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.

2. Wählen Sie Produktliste aus.

Erstellen von Produkten

Sie erstellen Produkte auf der Seite Products (Produkte) in der AWS Service Catalog-Administratorkonsole.

> **Note**
>
> Für die Erstellung von Terraform-Produkten ist eine zusätzliche Konfiguration erforderlich, darunter eine Terraform-Bereitstellungs-Engine und eine Startrolle. Weitere Informationen finden Sie unter Erste Schritte mit einem Terraform-Produkt.

So erstellen Sie ein neues AWS Service Catalog-Produkt

1. Navigieren Sie zur Seite Produktliste.
2. Wählen Sie Produkt erstellen und dann Produkt erstellen aus.
3. Produktdetails – Ermöglicht Ihnen die Auswahl des Produkttyps, den Sie erstellen möchten. AWS Service Catalog unterstützt die Produkttypen AWS CloudFormation, Terraform Cloud und External (unterstützt die Terraform Community Edition). Produktdetails enthalten auch die Metadaten, die angezeigt werden, wenn Sie in einer Liste oder Detailseite nach Produkten suchen und diese anzeigen. Geben Sie Folgendes ein:
   - Product name – Der Name des Produkts.
   - Produktbeschreibung – Die Beschreibung wird in der Produktliste angezeigt, um Ihnen bei der Auswahl des richtigen Produkts zu helfen.
   - Besitzer – Die Person oder Organisation, die dieses Produkt veröffentlicht. Der Eigentümer könnte der Name Ihrer IT-Organisation oder der Administrator sein.
   - Distributor (optional) – Der Name des Herausgebers der Anwendung. In diesem Feld können Sie die Produktliste sortieren, um das Auffinden von Produkten zu erleichtern.
4. Mit Versionsdetails können Sie Ihre Vorlagendatei hinzufügen und Ihr Produkt erstellen. Geben Sie Folgendes ein:
   - Methode auswählen – Es gibt vier Möglichkeiten, eine Vorlagendatei hinzuzufügen.

- Verwenden einer lokalen Vorlagendatei – Laden Sie eine -AWS CloudFormationVorlage oder eine Terraform tar.gz-Konfigurationsdatei von einem lokalen Laufwerk hoch.
- Verwenden einer Amazon S3-URL – Geben Sie eine URL an, die auf eine -AWS CloudFormationVorlage oder eine in Amazon S3 gespeicherte Terraform-tar.gz-Konfigurationsdatei verweist. Wenn Sie eine Amazon S3-URL angeben, muss diese mit beginnen`https://`.
- Verwenden eines externen Repositorys – Geben Sie Ihr GitHub-, GitHub Enterprise- oder Bitbucket-Code-Repository an. AWS Service Catalog ermöglicht es Ihnen, Produkte mit Vorlagendateien zu synchronisieren. Für Terraform-Produkte muss das Vorlagendateiformat eine einzelne Datei sein, die in Tar archiviert und in Gzip komprimiert wird.
- Verwenden eines vorhandenen CloudFormation Stacks – Geben Sie den ARN für einen vorhandenen CloudFormation Stack ein. Diese Methode unterstützt keine Terraform Cloud- oder externen Produkte.

- Versionsname (optional) – Der Name der Produktversion (z. B. „v1“, „v2beta“). Leerzeichen sind nicht zulässig.
- Beschreibung (optional) – Eine Beschreibung der Produktversion, einschließlich der Unterschiede zwischen dieser Version und den anderen Versionen.
- Anleitung – Verwaltet auf der Registerkarte Versionen auf einer Produktdetailseite. Wenn eine Produktversion während des Workflows zum Erstellen eines Produkts erstellt wird, wird die Unterstützung für diese Version auf den Standardwert festgelegt. Weitere Informationen zu Anleitungen finden Sie unter Verwalten von -Versionen.

5. Support-Details identifizieren die Organisation in Ihrem Unternehmen und bieten einen Ansprechpartner für den Support. Geben Sie Folgendes ein:

   - Email contact (optional) – Die E-Mail-Adresse zum Melden von Problemen mit dem Produkt.
   - Support-Link (optional) – Eine URL zu einer Website, auf der Benutzer Support-Informationen oder Dateitickets finden können. Die URL muss mit `http://` oder `https://` beginnen. Administratoren sind für die Aufrechterhaltung der Genauigkeit und des Zugriffs auf Support-Informationen verantwortlich.
   - Supportbeschreibung (optional) – Eine Beschreibung, wie Sie den Link E-Mail-Kontakt und Support verwenden sollten.

6. Verwalten von Tags (optional) – Sie können Tags nicht nur zur Kategorisierung Ihrer Ressourcen verwenden, sondern sie auch zur Authentifizierung Ihrer Berechtigungen zum Erstellen dieser Ressource verwenden.

7. Produkt erstellen – Wenn Sie das Formular ausgefüllt haben, wählen Sie Produkt erstellen aus. Nach einigen Sekunden wird das Produkt auf der Seite Produktliste angezeigt. Möglicherweise müssen Sie Ihren Browser aktualisieren, um das Produkt zu sehen.

Sie können auch verwenden CodePipeline , um eine Pipeline zu erstellen und zu konfigurieren, um Ihre Produktvorlage für bereitzustellen AWS Service Catalog und Änderungen bereitzustellen, die Sie in Ihrem Quell-Repository vorgenommen haben. Weitere Informationen finden Sie unter Tutorial: Erstellen einer einfachen Pipeline für Bereitstellungen auf AWS Service Catalog.

Sie können Parametereigenschaften in Ihrer AWS CloudFormation oder Terraform-Vorlage definieren und diese Regeln während der Bereitstellung erzwingen. Diese Eigenschaften können die minimale und maximale Länge, minimale und maximale Werte, zulässige Werte und einen regulären Ausdruck für den Wert definieren. AWS Service Catalog gibt während der Bereitstellung eine Warnung aus, wenn der angegebene Wert nicht der Parametereigenschaft entspricht. Weitere Informationen zu Parametereigenschaften finden Sie unter Parameter im AWS CloudFormation -Benutzerhandbuch.

Fehlerbehebung

Sie müssen über die Berechtigung zum Abrufen von Objekten aus Amazon S3-Buckets verfügen. Andernfalls kann beim Starten oder Aktualisieren eines Produkts der folgende Fehler auftreten.

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

Wenn Sie auf diese Meldung stoßen, stellen Sie sicher, dass Sie über die Berechtigung zum Abrufen von Objekten aus den folgenden Buckets verfügen:

- Der Bucket, in dem die Bereitstellungsartefaktvorlage gespeichert ist.
- Der Bucket, der mit „cf-templates-*“ beginnt und in dem die Bereitstellungsartefaktvorlage AWS Service Catalog speichert.
- Der interne Bucket, der mit „sc-*“ beginnt und in dem Metadaten AWS Service Catalog speichert. Sie können diesen Bucket in Ihrem Konto nicht sehen.

Die folgende Beispielrichtlinie zeigt die Mindestberechtigungen, die zum Abrufen von Objekten aus den zuvor genannten Buckets erforderlich sind.

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

Hinzufügen von Produkten zu Portfolios

Sie können Produkte zu einer beliebigen Anzahl von Portfolios hinzufügen. Wenn ein Produkt aktualisiert wird, erhalten alle Portfolios (einschließlich freigegebener Portfolios), die das Produkt enthalten, automatisch die neue Version.

So fügen Sie einem Portfolio ein Produkt aus Ihrem Katalog hinzu

1. Navigieren Sie zur Seite Produktliste.
2. Wählen Sie ein Produkt und dann Aktionen aus. Wählen Sie im Dropdown-Menü Produkt zum Portfolio hinzufügen aus. Sie werden zur Seite ***name-of-product*** Zum Portfolio hinzufügen weitergeleitet.
3. Wählen Sie ein Portfolio und dann Produkt zum Portfolio hinzufügen aus.

Wenn Sie einem Portfolio ein Terraform-Produkt hinzufügen, erfordert das Produkt eine Starteinschränkung. Sie müssen eine IAM-Rolle aus Ihrem Konto auswählen, einen IAM-Rollen-ARN oder einen Rollennamen eingeben. Wenn Sie einen Rollennamen angeben und ein Konto die Starteinschränkung verwendet, verwendet das Konto diesen Namen für die IAM-Rolle. Auf diese Weise können Einschränkungen für Startrollen kontounabhängig sein, sodass Sie weniger Ressourcen pro gemeinsam genutztem Konto erstellen können. Einzelheiten und Anweisungen finden Sie unter Schritt 6: Hinzufügen einer Starteinschränkung zu Ihrem Terraform-Produkt

Ein Portfolio kann zahlreiche Produkte enthalten, die eine Mischung aus - AWS CloudFormation und Terraform-Produkttypen sind.

Aktualisieren von Produkten

Wenn Sie die Vorlage eines Produkts aktualisieren, erstellen Sie eine neue Version des Produkts. Neue Produktversionen sind automatisch für alle Benutzer verfügbar, die Zugriff auf ein Portfolio haben, das das Produkt enthält.

> **Note**
>
> Wenn Sie ein vorhandenes Produkt aktualisieren, können Sie den Produkttyp (AWS CloudFormation oder Teraform) nicht ändern. Wenn Sie beispielsweise ein AWS CloudFormation Produkt aktualisieren, können Sie die vorhandene AWS CloudFormation Vorlage nicht durch eine Terraform-tar.gz-Konfigurationsdatei ersetzen. Sie müssen die vorhandene AWS CloudFormation Vorlagendatei mit einer neuen AWS CloudFormation Vorlagendatei aktualisieren.

Endbenutzer, die derzeit ein bereitgestelltes Produkt der vorherigen Produktversion ausführen, können ihr bereitgestelltes Produkt auf die neue Version aktualisieren. Wenn eine neue Version eines Produkts verfügbar ist, können Benutzer den Befehl Bereitgestelltes Produkt aktualisieren auf der Liste Bereitgestellte Produkte oder auf der Seite Bereitgestellte Produktdetails verwenden.

Bevor Sie eine neue Version eines Produkts erstellen, AWS Service Catalog empfiehlt , Ihre Produkt-Updates in AWS CloudFormation oder in der Terraform-Engine zu testen, um sicherzustellen, dass sie ordnungsgemäß funktionieren.

Erstellen einer neuen Produktversion

1. Navigieren Sie zur Seite Produktliste.
2. Wählen Sie das Produkt aus, das Sie aktualisieren möchten. Sie werden zur Seite Produktdetails weitergeleitet.
3. Erweitern Sie auf der Seite Produktdetails die Registerkarte Versionen und wählen Sie dann Neue Version erstellen aus.
4. Führen Sie unter Versionsdetails die folgenden Schritte aus:

   - Vorlage auswählen – Es gibt vier Möglichkeiten, eine Vorlagendatei hinzuzufügen.

     Verwenden einer lokalen Vorlagendatei – Laden Sie eine -AWS CloudFormationVorlage oder eine Terraform tar.gz-Konfigurationsdatei von einem lokalen Laufwerk hoch.

Verwenden einer Amazon S3-URL – Geben Sie eine URL an, die auf eine -AWS CloudFormationVorlage oder eine in Amazon S3 gespeicherte Terraform-tar.gz-Konfigurationsdatei verweist. Wenn Sie eine Amazon S3-URL angeben, muss diese mit https://. beginnen.

Verwenden eines externen Repositorys – Geben Sie Ihr GitHub-, GitHub Enterprise- oder Bitbucket-Code-Repository an. AWS Service Catalog ermöglicht es Ihnen, Produkte mit Vorlagendateien zu synchronisieren. Für Terraform-Produkte muss das Vorlagendateiformat eine einzelne Datei sein, die in Tar archiviert und in Gzip komprimiert wird.

Verwenden eines vorhandenen CloudFormation Stacks – Geben Sie den ARN für einen vorhandenen CloudFormation Stack ein. Diese Methode unterstützt keine Terraform Cloud- oder externen Produkte.

- Versionstitel – Der Name der Produktversion (z. B. „v1“, „v2beta“). Leerzeichen sind nicht zulässig.
- Beschreibung (optional) – Eine Beschreibung der Produktversion, einschließlich der Unterschiede zwischen dieser Version und der vorherigen Version.

5. Wählen Sie Produktversion erstellen aus.

Sie können auch verwenden CodePipeline , um eine Pipeline zu erstellen und zu konfigurieren, um Ihre Produktvorlage in bereitzustellen AWS Service Catalogund Ihre Änderungen in Ihrem Quell-Repository bereitzustellen. Weitere Informationen finden Sie unter Tutorial: Erstellen einer einfachen Pipeline für Bereitstellungen auf AWS Service Catalog.

Produkte mit Vorlagendateien von GitHub GitHub Enterprise oder Bitbucket synchronisieren

AWS Service Catalog ermöglicht es Ihnen, Produkte mit Vorlagendateien zu synchronisieren, die über einen externen Repository-Anbieter verwaltet werden. AWS Service Catalog bezeichnet Produkte mit dieser Art von Template-Verbindung als Git-synchronisierte Produkte. Zu den Repository-Optionen gehören GitHub GitHub Enterprise oder Bitbucket. Nachdem du dein Konto AWS-Konto mit einem externen Repository-Konto autorisiert hast, kannst du neue AWS Service Catalog Produkte erstellen oder bestehende Produkte aktualisieren, um sie mit einer Vorlagendatei im Repository zu synchronisieren. Wenn Änderungen an der Vorlagendatei vorgenommen und im Repository gespeichert werden (z. B. mithilfe von Git-Push), AWS Service Catalog werden die Änderungen automatisch erkannt und eine neue Produktversion (Artefakt) erstellt.

Themen

- Erforderliche Berechtigungen zum Synchronisieren von Produkten mit externen Vorlagendateien
- Erstellen Sie eine Kontoverbindung
- Git-synchronisierte Produktverbindungen anzeigen
- Aktualisierung von Git-synchronisierten Produktverbindungen
- Löschen von Git-synchronisierten Produktverbindungen
- Synchronisieren von Terraform-Produkten mit Vorlagendateien von GitHub Enterprise oder GitHub Bitbucket
- AWS-Region Unterstützung für GIT-synchronisierte Produkte

Erforderliche Berechtigungen zum Synchronisieren von Produkten mit externen Vorlagendateien

Sie können die folgende AWS Identity and Access Management (IAM-) Richtlinie als Vorlage verwenden, damit AWS Service Catalog Administratoren Produkte mit Vorlagendateien aus einem externen Repository synchronisieren können. Diese Richtlinie umfasst die erforderlichen Berechtigungen sowohl von als CodeConnections auch AWS Service Catalog. AWS Service Catalog empfiehlt, dass Sie die unten stehende Vorlagenrichtlinie kopieren und bei der Aktivierung von Produkten, die mit dem Repository synchronisiert werden, auch die AWS Service Catalog `AWSServiceCatalogAdminFullAccess` verwaltete Richtlinie verwenden.

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

Erstellen Sie eine Kontoverbindung

Bevor Sie eine Vorlagendatei mit einem AWS Service Catalog Produkt synchronisieren, müssen Sie eine einmalige Verbindung erstellen und autorisieren. account-to-account Sie verwenden diese Verbindung, um die Details des Repositorys anzugeben, das die gewünschte Vorlagendatei enthält. Sie können eine Verbindung mithilfe der AWS Service Catalog Konsole, CodeConnections Konsole AWS Command Line Interface (CLI) oder CodeConnections APIs herstellen.

Nachdem Sie eine Verbindung hergestellt haben, können Sie die AWS Service Catalog Konsole, AWS Service Catalog API oder CLI verwenden, um ein synchronisiertes AWS Service Catalog Produkt zu erstellen. AWS Service Catalog Administratoren können auf der Grundlage einer Vorlagendatei in einem Repository und einer Filiale neue AWS Service Catalog Produkte erstellen oder bestehende Produkte aktualisieren. Wenn eine Änderung im Repository festgeschrieben wird, AWS Service Catalog wird die Änderung automatisch erkannt und eine neue Produktversion erstellt. Frühere Produktversionen werden bis zum vorgeschriebenen Versionslimit verwaltet und ihnen wird der Status „Veraltet“ zugewiesen.

Außerdem AWS Service Catalog wird automatisch eine serviceverknüpfte Rolle (SLR) erstellt, nachdem die Verbindung hergestellt wurde. Diese Spiegelreflexkamera ermöglicht es AWS Service Catalog , alle Änderungen an der Vorlagendatei zu erkennen, die in das Repository übernommen wurden. Die Spiegelreflexkamera ermöglicht auch AWS Service Catalog die automatische Erstellung

neuer Produktversionen für synchronisierte Produkte. Weitere Informationen zu den Berechtigungen und Funktionen von SLR finden Sie unter Mit dem Dienst verknüpfte Rollen für. AWS Service Catalog

Um ein neues Git-synchronisiertes Produkt zu erstellen

1. Wählen Sie im linken Navigationsbereich Produktliste und dann Produkt erstellen aus.
2. Geben Sie die Produktdetails ein.
3. Wählen Sie unter Versionsdetails die Option Geben Sie Ihr Code-Repository mithilfe eines AWS CodeStar Anbieters an und wählen Sie dann den Link Neue AWS CodeStar Verbindung erstellen aus.
4. Nachdem Sie die Verbindung erstellt haben, aktualisieren Sie die Verbindungsliste und wählen Sie dann die neue Verbindung aus. Geben Sie die Repository-Details an, einschließlich des Repositorys, des Branches und des Pfads der Vorlagendatei.

   Informationen zur Verwendung einer Terraform-Konfigurationsdatei finden Sie unter. Synchronisieren von Terraform-Produkten mit Vorlagendateien von GitHub Enterprise oder GitHub Bitbucket

   a. (Optional beim Erstellen einer neuen AWS Service Catalog Produktressource) Fügen Sie im Abschnitt Support-Details Metadaten für das Produkt hinzu.
   b. (Optional beim Erstellen einer neuen AWS Service Catalog Produktressource) Wählen Sie im Abschnitt Tags die Option Neues Tag hinzufügen aus und geben Sie die Schlüssel - und Wertepaare ein.
5. Wählen Sie Neues Produkt erstellen aus.

Um mehrere GIT-synchronisierte Produkte zu erstellen

1. Wählen Sie im linken Navigationsbereich der AWS Service Catalog Konsole die Option Produktliste und dann Mehrere von Git verwaltete Produkte erstellen aus.
2. Geben Sie die allgemeinen Produktdetails ein.
3. Wählen Sie unter Details zum externen Repository eine AWS CodeStar Verbindung aus, und geben Sie dann das Repository und den Branch an.
4. Geben Sie im Bereich Produkte hinzufügen den Pfad zur Vorlagendatei und den Produktnamen ein. Wählen Sie Neuen Artikel hinzufügen und fügen Sie weitere Produkte wie gewünscht hinzu.
5. Nachdem Sie alle gewünschten Produkte hinzugefügt haben, wählen Sie Produkte gleichzeitig erstellen.

Um ein vorhandenes AWS Service Catalog Produkt mit einem externen Repository zu verbinden

1. Wählen Sie im linken Navigationsbereich der AWS Service Catalog Konsole die Option Produktliste und dann Produkte mit einem externen Repository verbinden aus.
2. Wählen Sie auf der Seite Produkte auswählen die Produkte aus, die Sie mit einem externen Repository verbinden möchten, und klicken Sie dann auf Weiter.
3. Wählen Sie auf der Seite Quelldetails angeben eine bestehende AWS CodeStar Verbindung aus und geben Sie dann das Repository, den Zweig und den Pfad der Vorlagendatei an.
4. Wählen Sie Weiter aus.
5. Überprüfen Sie auf der Seite Überprüfen und Absenden die Verbindungsdetails und wählen Sie dann Produkte mit einem externen Repository verbinden aus.

Git-synchronisierte Produktverbindungen anzeigen

Sie können die AWS Service Catalog Konsole, die API oder AWS CLI zum Anzeigen der Repository-Verbindungsdetails verwenden. Bei AWS Service Catalog Produkten, die mit einer Vorlagendatei verknüpft sind, können Sie Informationen über die Repository-Verbindung und den Zeitpunkt, zu dem die Vorlage zuletzt mit dem Produkt synchronisiert wurde, über den Status „Letzte Synchronisierung“ abrufen.

> **Note**
>
> Sie können Repository-Informationen und den Status der letzten Synchronisierung auf Produktebene einsehen. Benutzer müssen über IAM-Berechtigungen in den CodeConnections APIs verfügen, um Repository-Details anzeigen zu können. Weitere Informationen zu den erforderlichen Richtlinien für diese IAM-Berechtigungen finden Sie unter Erforderliche Berechtigungen für die Synchronisierung von AWS Service Catalog Produkten mit Vorlagendateien.

Um Verbindungs- und Repository-Details anzuzeigen, verwenden Sie AWS Management Console

1. Wählen Sie im linken Navigationsbereich die Option Produktliste aus.
2. Wählen Sie das Produkt aus der Liste aus.
3. Navigieren Sie auf der Produktseite zum Abschnitt Details zur Produktquelle.

4. Um die Quell-Revision-ID für eine Produktversion anzuzeigen, wählen Sie den Link Letzte Version erstellt. Im Abschnitt Versionsdetails wird die Quellrevisions-ID angezeigt.

Um Verbindungs- und Repository-Details anzuzeigen, verwenden Sie AWS CLI

Führen Sie von der AWS CLI aus die folgenden Befehle aus:

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

$ aws servicecatalog describe-provisioning-artifact

$ aws servicecatalog search-product-as-admin

$ aws servicecatalog list-provisioning-artifacts
```

Aktualisierung von Git-synchronisierten Produktverbindungen

Sie können bestehende Kontoverbindungen und mit Git-synchronisierte Produkte mithilfe der AWS Service Catalog Konsole, der AWS Service Catalog API oder aktualisieren. AWS CLI

Wie Sie ein vorhandenes AWS Service Catalog Produkt mit einer Vorlagendatei verbinden, erfahren Sie unter Neue Git-synchronisierte Produktverbindungen erstellen.

Um bestehende Produkte auf GIT-synchronisierte Produkte zu aktualisieren

1. Wählen Sie im linken Navigationsbereich die Option Produktliste und dann eine der folgenden Optionen aus:
   - Um ein einzelnes Produkt zu aktualisieren, wählen Sie das Produkt aus, navigieren Sie zum Abschnitt Produktquellendetails und wählen Sie dann Details bearbeiten aus.
   - Um mehrere Produkte zu aktualisieren, wählen Sie Produkte mit einem externen Repository verbinden, wählen Sie bis zu zehn Produkte aus und klicken Sie dann auf Weiter.
2. Führen Sie im Abschnitt Details zur Produktquelle die folgenden Aktualisierungen durch:
   - Geben Sie die Verbindung an.
   - Geben Sie das Repository an.
   - Geben Sie den Zweig an.
   - Benennen Sie die Vorlagendatei.
3. Wählen Sie Änderungen speichern aus.

> **Note**
>
> Für Produkte, die noch nicht mit einem externen Repository verbunden sind, können Sie die Option Mit einem externen Repository Connect verwenden, die in der Warnung oben auf der Produktinformationsseite angezeigt wird, nachdem Sie das Produkt ausgewählt haben.

Sie können auch die AWS Service Catalog Konsole oder AWS CLI das

- Ein vorhandenes AWS Service Catalog Produkt mit einer Vorlagendatei in einem externen Repository Connect
- Aktualisieren Sie die Produktmetadaten, einschließlich des Produktnamens, der Beschreibung und der Tags.
- Konfigurieren Sie eine Verbindung für ein zuvor verbundenes AWS Service Catalog Produkt neu (aktualisieren Sie die Synchronisierung, um eine andere Repository-Quelle zu verwenden).

Um die Verbindungs- und Repository-Details mithilfe AWS Service Catalog der Konsole zu aktualisieren

1. Wählen Sie im linken Navigationsbereich der AWS Service Catalog Konsole die Option Produktliste und wählen Sie dann ein Produkt aus, das derzeit mit einem externen Repository verbunden ist.
2. Wählen Sie im Abschnitt Details zur Produktquelle die Option Produktquelle bearbeiten aus.
3. Geben Sie im Abschnitt Details zur Produktquelle das neue gewünschte Repository an.
4. Wählen Sie Änderungen speichern aus.

Um Verbindungs- und Repository-Details zu aktualisieren, verwenden Sie AWS CLI

Aus der AWS CLI Ausführung der `$ aws servicecatalog update-provisioning-artifact` Befehle `$ aws servicecatalog update-product` und.

Löschen von Git-synchronisierten Produktverbindungen

Sie können eine Verbindung zwischen einem AWS Service Catalog Produkt und einer Vorlagendatei mithilfe der AWS Service Catalog Konsole, der CodeConnections API oder löschen. AWS CLI Wenn Sie ein Produkt von einer Vorlagendatei trennen, wechselt das synchronisierte AWS Service

Catalog Produkt zu einem regelmäßig verwalteten Produkt. Wenn nach dem Trennen der Verbindung zum Produkt die Vorlagendatei geändert und im zuvor verbundenen Repository gespeichert wird, werden die Änderungen nicht übernommen. Informationen zum erneuten Verbinden eines AWS Service Catalog Produkts mit einer Vorlagendatei in einem externen Repository finden Sie unter Verbindungen und AWS Service Catalog synchronisierte Produkte aktualisieren.

So trennen Sie die Verbindung zu einem mit Git-synchronisierten Produkt über die Konsole AWS Service Catalog

1. Wählen Sie im AWS Management Console linken Navigationsbereich die Option Produktliste aus.
2. Wählen Sie ein Produkt aus der Liste aus.
3. Navigieren Sie auf der Produktseite zum Abschnitt Details zur Produktquelle.
4. Wählen Sie „Trennen“.
5. Bestätigen Sie die Aktion und wählen Sie dann Trennen.

Um die Verbindung zu einem Git-synchronisierten Produkt zu trennen, verwenden Sie AWS CLI

Führen Sie von der aus den AWS CLI Befehl aus. `$ aws servicecatalog update-product` Entfernen Sie in der `ConnectionParameters` Eingabe die angegebene Verbindung.

Um eine Verbindung mithilfe der CodeConnections API zu löschen oder AWS CLI

Führen Sie in der CodeConnections API oder AWS CLI den `$ aws codestar-connections delete-connection` Befehl aus.

Synchronisieren von Terraform-Produkten mit Vorlagendateien von GitHub Enterprise oder GitHub Bitbucket

Wenn Sie ein Git-synchronisiertes Produkt mit einer Terraform-Konfigurationsdatei erstellen, akzeptiert der Dateipfad nur das Format tar.gz. Terraform-Ordnerformate werden im Dateipfad nicht akzeptiert.

AWS-Region Unterstützung für GIT-synchronisierte Produkte

AWS Service Catalog unterstützt GIT-synchronisierte Produkte AWS-Regionen wie in der Tabelle unten angegeben.

AWS-Region Name	AWS-Region Identität	Support für GIT-synchronisierte Produkte
USA Ost (Nord-Virginia)	us-east-1	Ja
USA Ost (Ohio)	us-east-2	Ja
USA West (Nordkalifornien)	us-west-1	Ja
USA West (Oregon)	us-west-2	Ja
Afrika (Kapstadt)	af-south-1	Nein
Asien-Pazifik (Hongkong)	ap-east-1	Nein
Asien-Pazifik (Jakarta)	ap-southeast-3	Nein
Asien-Pazifik (Mumbai)	ap-south-1	Ja
Asien-Pazifik (Osaka)	ap-northeast-3	Nein
Asien-Pazifik (Seoul)	ap-northeast-2	Ja
Asien-Pazifik (Singapore)	ap-southeast-1	Ja
Asien-Pazifik (Sydney)	ap-southeast-2	Ja
Asien-Pazifik (Tokyo)	ap-northeast-1	Ja
Kanada (Zentral)	ca-central-1	Ja
Europa (Frankfurt)	eu-central-1	Ja
Europa (Ireland)	eu-west-1	Ja
Europa (London)	eu-west-2	Ja
Europa (Mailand)	eu-south-1	Nein
Europa (Paris)	eu-west-3	Ja
Europa (Stockholm)	eu-north-1	Ja

AWS-Region Name	AWS-Region Identität	Support für GIT-synchronisierte Produkte
Naher Osten (Bahrain)	me-south-1	Nein
Südamerika (São Paulo)	sa-east-1	Ja
AWS GovCloud (US-Ost)	us-gov-east-1	Nein
AWS GovCloud (US-West)	us-gov-west-1	Nein

Löschen von Produkten

Wenn Sie ein Produkt löschen, AWS Service Catalog entfernt alle Produktversionen aus jedem Portfolio, das das Produkt enthält.

AWS Service Catalog ermöglicht das Löschen eines Produkts über die AWS Service CatalogKonsole oder AWS CLI. Um ein Produkt erfolgreich zu löschen, müssen Sie zuerst alle dem Produkt zugeordneten Ressourcen trennen. Beispiele für Produktressourcenzuordnungen sind Portfoliozuordnungen TagOptions, Budgets und Serviceaktionen.

> **Important**
>
> Sie können ein Produkt nicht wiederherstellen, nachdem es gelöscht wurde.

So löschen Sie ein Produkt mithilfe der AWS Service Catalog Konsole

1. Navigieren Sie zur Seite Portfolios und wählen Sie das Portfolio aus, das das Produkt enthält, das Sie löschen möchten.
2. Wählen Sie das Produkt aus, das Sie löschen möchten, und klicken Sie dann oben rechts im Produktbereich auf Löschen.
3. Bestätigen Sie für Produkte ohne zugeordnete Ressourcen das Produkt, das Sie löschen möchten, indem Sie Löschen in das Textfeld eingeben, und wählen Sie dann Löschen aus.

   Fahren Sie für Produkte mit zugehörigen Ressourcen mit Schritt 4 fort.

4. Überprüfen Sie im Fenster Produkt löschen die Tabelle Zuordnungen, in der alle zugehörigen Ressourcen des Produkts angezeigt werden. AWS Service Catalog versucht, diese Ressourcen zu trennen, wenn Sie das Produkt löschen.
5. Bestätigen Sie, dass Sie das Produkt löschen möchten, und entfernen Sie alle zugehörigen Ressourcen, indem Sie Löschen in das Textfeld eingeben.
6. Wählen Sie Zuordnung aufheben und löschen Sie .

Wenn nicht in der AWS Service Catalog Lage ist, die Zuordnung aller Produktressourcen aufzuheben, wird das Produkt nicht gelöscht. Das Fenster Produkt löschen zeigt die Anzahl der fehlgeschlagenen Zuordnungen und eine Beschreibung für jeden Fehler an. Weitere Informationen zum Beheben fehlgeschlagener Ressourcenaufhebungen beim Löschen eines Produkts finden Sie unten unter Beheben fehlgeschlagener Ressourcenaufhebungen beim Löschen eines Produkts.

Themen

- Löschen von Produkten mit der AWS CLI
- Behebung fehlgeschlagener Ressourcenaufhebungen beim Löschen eines Produkts

Löschen von Produkten mit der AWS CLI

AWS Service Catalog ermöglicht Ihnen die Verwendung von AWS Command Line Interface (AWS CLI), um Produkte aus Ihrem Portfolio zu löschen. Die AWS CLI ist ein Open-Source-Tool, mit dem Sie über Befehle in Ihrer Befehlszeilen-Shell mit den AWS-Services interagieren können. Die Funktion zum Löschen AWS Service Catalogerzwingen erfordert einen AWS CLI Alias . Dabei handelt es sich um eine Verknüpfung, die Sie in der erstellen können, AWS CLI um Befehle oder Skripts zu verkürzen, die Sie häufig verwenden.

Voraussetzungen

- Installieren und Konfigurieren der AWS CLI. Weitere Informationen finden Sie unter Installieren oder Aktualisieren der neuesten Version von AWS CLI und Konfigurationsgrundlagen. Verwenden Sie eine AWS CLI-Mindestversion von 1.11.24 oder 2.0.0.
- Der CLI-Alias für das Löschen von Produkten erfordert ein Bash-kompatibles Terminal und den JQ-Befehlszeilen-JSON-Prozessor. Weitere Informationen zur Installation des Befehlszeilen-JSON-Prozessors finden Sie unter Download jq.
- Erstellen Sie einen AWS CLI Alias für Batch`Disassociation`-API-Aufrufe, sodass Sie ein Produkt in einem einzigen Befehl löschen können.

Um ein Produkt erfolgreich zu löschen, müssen Sie zuerst alle dem Produkt zugeordneten Ressourcen trennen. Beispiele für Produktressourcenzuordnungen sind Portfoliozuordnungen, Budgets, Tag-Optionen und Service-Aktionen. Wenn Sie die CLI zum Löschen eines Produkts verwenden, können Sie mit dem CLI`force-delete-product`-Alias die `Disassociate` API aufrufen, um die Zuordnung aller Ressourcen aufzuheben, die die `DeleteProduct` API verhindern würden. Dadurch wird ein separater Aufruf für einzelne Zuordnungen vermieden.

> **Note**
>
> Die in den folgenden Verfahren gezeigten Dateipfade können je nachdem, welches Betriebssystem Sie für die Ausführung dieser Aktionen verwenden, variieren.

Erstellen eines AWS CLI Alias zum Löschen von AWS Service Catalog Produkten

Wenn Sie die AWS CLI zum Löschen eines AWS Service Catalog Produkts verwenden, können Sie mit dem CLI`force-delete-product`-Alias die `Disassociate` API aufrufen, um die Zuordnung aller Ressourcen aufzuheben, die den `DeleteProduct` Aufruf verhindern würden.

Erstellen einer -**`alias`**Datei in Ihrem AWS CLI Konfigurationsordner

1. Navigieren Sie in der -AWS CLIKonsole zum Konfigurationsordner. Standardmäßig ist der Konfigurationsordnerpfad `~/.aws/` unter Linux und macOS oder `%USERPROFILE%\.aws\` unter Windows.
2. Erstellen Sie mithilfe der `cli` Dateinavigation oder durch Eingabe des folgenden Befehls in Ihrem bevorzugten Terminal einen Unterordner mit dem Namen :

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

   Der resultierende Standardpfad für den `cli` Ordner ist `~/.aws/cli/` unter Linux und MacOS oder `%USERPROFILE%\.aws\cli` unter Windows.
3. Erstellen Sie im neuen `cli` Ordner eine Textdatei `alias` mit dem Namen ohne Dateierweiterung. Sie können die `alias` Datei mithilfe der Dateinavigation oder durch Eingabe des folgenden Befehls in Ihrem bevorzugten Terminal erstellen:

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

4. Geben Sie `[toplevel]` in die erste Zeile ein.
5. Speichern Sie die Datei.

Als Nächstes können Sie den force-delete-product Alias zu Ihrer `alias` Datei hinzufügen, indem Sie das Aliasskript manuell in die Datei einfügen oder einen Befehl im Terminalfenster verwenden.

Manuelles Hinzufügen des force-delete-product Alias zu Ihrer **`alias`** Datei

1. Navigieren Sie in der -AWS CLIKonsole zu Ihrem AWS CLI Konfigurationsordner und öffnen Sie die -`alias`Datei.
2. Geben Sie den folgenden Code-Alias in die Datei unter der `[toplevel]` Zeile ein:

```
 [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. Speichern Sie die Datei.

Verwenden Sie das Terminalfenster, um den force-delete-product Alias zu Ihrer **`alias`** Datei hinzuzufügen

1. Öffnen Sie Ihr Terminalfenster und führen Sie den folgenden Befehl aus

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

2. Fügen Sie das Aliasskript in das Terminalfenster ein und drücken Sie dann STRG+D, um den `cat` Befehl zu beenden.

Aufrufen des force-delete-product Alias

1. Führen Sie in Ihrem Terminalfenster den folgenden Befehl aus, um den Alias Produkt löschen aufzurufen

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

   Das folgende Beispiel zeigt den `force-delete-product` Aliasbefehl und die daraus resultierende Antwort

   ```
   $ 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. Geben Sie einy, um zu bestätigen, dass Sie das Produkt löschen möchten.

Nach erfolgreichem Löschen des Produkts werden im Terminalfenster die folgenden Ergebnisse angezeigt

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

Weitere Ressourcen

Weitere Informationen zu AWS CLI, zur Verwendung von Aliassen und zum Löschen von AWS Service Catalog Produkten finden Sie in den folgenden Ressourcen:

- Erstellen und Verwenden von AWS CLI Aliassen im AWS Command Line Interface (CLI)-Benutzerhandbuch.
- Git-RepositoryAWS CLI für Alias-Repository.
- Löschen von AWS Service Catalog Produkten .
- AWS re:Invent 2016: Der effektive AWS CLI Benutzer auf YouTube.

Behebung fehlgeschlagener Ressourcenaufhebungen beim Löschen eines Produkts

Wenn Ihr früherer Versuch, ein Produkt zu löschen, aufgrund von Ausnahmen bei der Ressourcentrennung fehlgeschlagen ist, überprüfen Sie die Liste der Ausnahmen und deren Lösungen unten.

> **Note**
>
> Wenn Sie das Fenster Löschen von Produkten geschlossen haben, bevor Sie die Meldung zur fehlgeschlagenen Ressourcentrennung erhalten haben, können Sie die Schritte eins bis drei im Abschnitt Produkt löschen ausführen, um das Fenster erneut zu öffnen.

So beheben Sie eine fehlgeschlagene Ressourcenzuordnung

Überprüfen Sie im Fenster Produkt löschen die Spalte Status der Zuordnungstabelle. Identifizieren Sie die fehlgeschlagene Ausnahme bei der Trennung von Ressourcen und die vorgeschlagenen Lösungen:

Statusausnahmetyp	Ursache	Auflösung
Produkt prod-****	AWS Service Catalog konnte das Produkt nicht löschen, da dem Produkt immer noch TagOptions, Budgets, mindestens eines `ProvisioningArtifact` mit zugehörigen Aktionen, das Produkt immer einem Portfolio zugewiesen ist, das Produkt Benutzer hat oder das Produkt Einschränkungen hat.	Versuchen Sie erneut, das Produkt zu löschen.
Benutzer: `username` ist nicht autorisiert, Folgendes auszuführen:	Der Benutzer, der versucht, das Produkt zu löschen, verfügt nicht über die erforderlichen Berechtigungen, um die Zuordnung der Produktressourcen aufzuheben.	AWS Service Catalog empfiehlt, sich an Ihren Kontoadministrator zu wenden, um weitere Informationen zum Aufheben der Zuordnung von Produktressourcen zu erhalten, für die Sie derzeit keine Berechtigungen zum Aufheben der Zuordnung haben.

Verwalten von Versionen

Sie weisen Produktversionen beim Anlegen eines Produkts zu und können Produktversionen jederzeit aktualisieren.

Versionen verfügen über eine AWS CloudFormation-Vorlage, einen Titel, eine Beschreibung, einen Status und eine Anleitung.

Versionsstatus

Eine Version kann über einen von drei Status verfügen:

- Aktiv – eine aktive Version wird in der Versionsliste angezeigt und ermöglicht es Benutzern, diese zu starten.
- Inaktiv – eine inaktive Version wird in der Versionsliste ausgeblendet. Vorhandene bereitgestellte Produkte, die von dieser Version gestartet werden, sind nicht betroffen.
- Gelöscht – Eine gelöschte Version wird aus der Versionsliste entfernt. Das Löschen einer Version kann nicht rückgängig gemacht werden.

Versionsanleitung

Sie können eine Versionsanleitung festlegen, um Endbenutzern Informationen zur Produktversion bereitzustellen. Versionsanleitungen betreffen nur aktive Produktversionen.

Es stehen zwei Optionen für die Versionsanleitung zur Verfügung:

- Keine – Standardmäßig haben Produktversionen keine Anleitungen. Endbenutzer können diese Version verwenden, um bereitgestellte Produkte zu aktualisieren und zu starten.
- Veraltet – Benutzer können keine neuen bereitgestellten Produkte mit einer veralteten Produktversion starten. Wenn ein zuvor eingeführtes bereitgestelltes p-Produkt eine jetzt veraltete Version verwendet, können Benutzer dieses bereitgestellte Produkt nur mit der vorhandenen Version oder einer neuen Version aktualisieren.

Aktualisieren von Versionen

Sie weisen Produktversionen beim Anlegen eines Produkts zu und können Produktversionen zudem jederzeit aktualisieren. Weitere Informationen zum Erstellen eines Produkts finden Sie unter Erstellen von Produkten.

So aktualisieren Sie eine Produktversion

1. Wählen Sie in der AWS Service Catalog-Konsole die Option Products (Produkte)aus.
2. Wählen Sie in der Produktliste das Produkt aus, dessen Version Sie aktualisieren möchten.

3. Wählen Sie auf der Seite Product details (Produktdetails) die Registerkarte Versions (Versionen) aus und wählen Sie anschließend die Version aus, die Sie aktualisieren möchten.
4. Bearbeiten Sie auf der Seite Version details (Versionsdetails) die Produktversion und wählen Sie dann Save changes (Änderungen speichern)aus.

Verwenden von AWS Service Catalog-Einschränkungen

Sie wenden Einschränkungen an, um die Regeln zu steuern, die auf ein Produkt in einem bestimmten Portfolio angewendet werden, wenn Endbenutzer es starten. Wenn Endbenutzer das Produkt starten, sehen sie die Regeln, die Sie unter Verwendung von Einschränkungen angewendet haben. Sie können Einschränkungen auf ein Produkt anwenden, sobald es in ein Portfolio aufgenommen wurde. Einschränkungen sind aktiv, sobald Sie sie erstellen, und sie werden auf alle aktuellen Versionen eines Produkts angewendet, die noch nicht gestartet wurden.

Beschränkungen

- AWS Service Catalog-Starteinschränkungen
- AWS Service Catalog-Benachrichtigungseinschränkungen
- Einschränkungen für die AWS Service Catalog-Tag-Aktualisierung
- AWS Service Catalog-Stack-Set-Einschränkungen
- AWS Service Catalog-Vorlageneinschränkungen

AWS Service Catalog-Starteinschränkungen

Eine Starteinschränkung gibt die AWS Identity and Access Management (IAM)-Rolle an, die AWS Service Catalog annimmt, wenn ein Endbenutzer ein Produkt startet, aktualisiert oder beendet. Eine IAM-Rolle ist eine Sammlung von Berechtigungen, die ein Benutzer oder AWS Service vorübergehend annehmen kann, um -AWSServices zu nutzen. Ein einführendes Beispiel finden Sie unter:

- AWS CloudFormation -Produkttyp: Schritt 6: Hinzufügen einer Starteinschränkung zum Zuweisen einer IAM-Rolle
- Produkttyp Terraform Open Source oder Terraform Cloud: Schritt 5: Erstellen von Startrollen

Starteinschränkungen gelten für Produkte im Portfolio (Produkt-Portfolio-Zuordnung). Starteinschränkungen gelten nicht auf Portfolioebene oder für ein Produkt in allen Portfolios. Um eine

Starteinschränkungen allen Produkten in einem Portfolio zuzuweisen, müssen Sie die Einschränkung auf jedes Produkt einzeln anwenden.

Ohne eine Starteinschränkung müssen Endbenutzer Produkte mit ihren eigenen IAM-Anmeldeinformationen starten und verwalten. Dazu müssen sie über Berechtigungen für , AWS ServicesAWS CloudFormation, die die Produkte verwenden, und verfügenAWS Service Catalog. Durch die Verwendung einer Startrolle können Sie stattdessen die Berechtigungen der Endbenutzer auf das Minimum beschränken, das sie für dieses Produkt benötigen. Weitere Informationen zu Endbenutzerberechtigungen finden Sie unter Identity and Access Management in AWS Service Catalog.

Um IAM-Rollen zu erstellen und zuzuweisen, benötigen Sie die folgenden IAM-Administratorberechtigungen:

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

Konfigurieren einer Startrolle

Die IAM-Rolle, die Sie einem Produkt als Starteinschränkung zuweisen, muss über Berechtigungen verfügen, um Folgendes zu verwenden:

Für Cloudformation-Produkte

- Die `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess` AWS CloudFormation von verwaltete Richtlinie
- Services in der AWS CloudFormation Vorlage für das Produkt
- Lesezugriff auf die AWS CloudFormation Vorlage in einem serviceeigenen Amazon S3-Bucket.

Für Terraform-Produkte

- Services in der Amazon S3-Vorlage für das Produkt
- Lesezugriff auf die Amazon S3-Vorlage in einem serviceeigenen Amazon S3-Bucket.

- `resource-groups:Tag`zum Markieren in einer Amazon EC2-Instance (von der Terraform-Bereitstellungs-Engine angenommen, wenn Bereitstellungsvorgänge ausgeführt werden)
- `resource-groups:CreateGroup` für das Markieren von Ressourcengruppen (angenommen von AWS Service Catalog, um Ressourcengruppen zu erstellen und Tags zuzuweisen)

Die Vertrauensrichtlinie der IAM-Rolle muss zulassenAWS Service Catalog, dass die Rolle übernimmt. Im folgenden Verfahren wird die Vertrauensrichtlinie automatisch festgelegt, wenn Sie AWS Service Catalog als Rollentyp auswählen. Wenn Sie die Konsole nicht verwenden, lesen Sie den Abschnitt Erstellen von Vertrauensrichtlinien für AWS Services, die Rollen übernehmen unter So verwenden Sie Vertrauensrichtlinien mit IAM-Rollen .

> **Note**
>
> Die Berechtigungen `servicecatalog:ProvisionProduct`, `servicecatalog:TerminateProvisionedProduct` und `servicecatalog:UpdateProvisionedProduct` können nicht in einer Startrolle zugewiesen werden. Sie müssen IAM-Rollen verwenden, wie in den Inline-Richtlinienschritten im Abschnitt Berechtigungen an AWS Service Catalog Endbenutzer erteilen gezeigt.

> **Note**
>
> Um bereitgestellte Cloudformation-Produkte und -Ressourcen in der AWS Service Catalog Konsole anzuzeigen, benötigen Endbenutzer AWS CloudFormation Lesezugriff. Das Anzeigen bereitgestellter Produkte und Ressourcen in der Konsole verwendet die Startrolle nicht.

So erstellen Sie eine Startrolle

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.

   Terraform-Produkte erfordern zusätzliche Konfigurationen von Startrollen. Weitere Informationen finden Sie unter Schritt 5: Erstellen von Startrollen in Erste Schritte mit einem Terraform-Open-Source-Produkt.
2. Wählen Sie Roles.
3. Klicken Sie auf Create New Role.

4. Geben Sie einen Rollennamen ein und wählen Sie Next Step aus.
5. Wählen Sie unter AWS Servicerollen neben die AWS Service CatalogOption Auswählen aus.
6. Klicken Sie auf der Seite Attach Policy auf Next Step.
7. Zum Erstellen der Rolle wählen Sie Create Role aus.

So fügen Sie der neuen Rolle eine Richtlinie an

1. Wählen Sie die Rolle aus, die Sie erstellt haben, um die Seite der Rollendetails anzuzeigen.
2. Wählen Sie die Registerkarte Permissions aus und erweitern Sie den Abschnitt Inline Policies. Klicken Sie dann auf click here.
3. Wählen Sie Custom Policy und dann Select aus.
4. Geben Sie einen Namen für die Richtlinie ein und fügen Sie Folgendes im Editor Policy Document ein:

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

> **Note**
>
> Wenn Sie eine Startrolle für eine Starteinschränkung konfigurieren, müssen Sie diese Zeichenfolge verwenden: `"s3:ExistingObjectTag/servicecatalog:provisioning":"true"`.

5. Fügen Sie der Richtlinie für jeden zusätzlichen Service, den das Produkt verwendet, eine Zeile hinzu. Um beispielsweise die Berechtigung für Amazon Relational Database Service (Amazon RDS) hinzuzufügen, geben Sie ein Komma am Ende der letzten Zeile in der `Action` Liste ein und fügen Sie dann die folgende Zeile hinzu:

   ```
   "rds:*"
   ```

6. Klicken Sie auf Apply Policy (Richtlinie anwenden).

Anwenden einer Startbeschränkung

Nachdem Sie die Startrolle konfiguriert haben, weisen Sie die Rolle dem Produkt als Starteinschränkung zu. Diese Aktion weist anAWS Service Catalog, die Rolle zu übernehmen, wenn ein Endbenutzer das Produkt startet.

So weisen Sie die Rolle einem Produkt zu

1. Öffnen Sie die Service-Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie das Portfolio aus, das das Produkt enthält.
3. Wählen Sie die Registerkarte Constraints (Einschränkungen) und dann Create constraint (Einschränkung erstellen).
4. Wählen Sie das Produkt unter Produkt und unter Einschränkungstyp die Option Starten aus. Klicken Sie auf Weiter.
5. Im Abschnitt Starteinschränkung können Sie eine IAM-Rolle aus Ihrem Konto auswählen und einen IAM-Rollen-ARN oder den Rollennamen eingeben.

   Wenn Sie den Rollennamen angeben und ein Konto die Starteinschränkung verwendet, verwendet das Konto diesen Namen für die IAM-Rolle. Dieser Ansatz ermöglicht es, dass Einschränkungen für Startrollen kontounabhängig sind, sodass Sie weniger Ressourcen pro gemeinsam genutztem Konto erstellen können.

   > **Note**
   >
   > Der angegebene Rollenname muss in dem Konto vorhanden sein, das die Starteinschränkung erstellt hat, und im Konto des Benutzers, der ein Produkt mit dieser Starteinschränkung startet.

6. Wählen Sie Create (Erstellen), wenn Sie die IAM-Rolle angegeben haben.

Hinzufügen des verwirrten Stellvertreters zur Starteinschränkung

AWS Service Catalog unterstützt den Schutz des verwirrten Stellvertreters für die APIs, die mit einer Assume Role-Anforderung ausgeführt werden. Wenn Sie eine Starteinschränkung hinzufügen, können Sie den Zugriff auf die Startrolle einschränken, indem Sie die `sourceArn` Bedingungen `sourceAccount` und in der Vertrauensrichtlinie der Startrolle verwenden. Es stellt sicher, dass die Startrolle von einer vertrauenswürdigen Quelle aufgerufen wird.

Im folgenden Beispiel gehört der AWS Service Catalog Endbenutzer zum Konto 111111111111. Wenn der AWS Service Catalog Administrator ein `LaunchConstraint` für ein Produkt erstellt, kann der Endbenutzer die folgenden Bedingungen in der Vertrauensrichtlinie der Startrolle angeben, um die Übernahmerolle auf das Konto 111111111111 zu beschränken.

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

}
```

Ein Benutzer, der ein Produkt mit dem bereitstellt, `LaunchConstraint` muss denselben `AccountId` (111111111111 haben). Andernfalls schlägt der Vorgang mit einem `AccessDenied` Fehler fehl und verhindert so den Missbrauch der Startrolle.

Die folgenden AWS Service Catalog APIs sind für den Schutz des verwirrten Stellvertreters gesichert:

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

Der `sourceArn` Schutz für unterstützt AWS Service Catalog nur Vorlagen-ARNs, z. B. „`arn:<aws-partition>:servicecatalog:<region>:<accountId>:`“, unterstützt keine spezifischen Ressourcen-ARNs.

Überprüfen der Starteinschränkung

Um zu überprüfen, ob die Rolle zum Starten des Produkts AWS Service Catalog verwendet und das Produkt erfolgreich bereitgestellt hat, starten Sie das Produkt über die AWS Service Catalog Konsole. Zum Testen einer Einschränkung vor der Freigabe für die Benutzer erstellen Sie ein Testportfolio mit den gleichen Produkten und testen Sie die Einschränkungen mit diesem Portfolio.

So starten Sie das Produkt

1. Wählen Sie im Menü für die AWS Service CatalogKonsole Service Catalog ,Endbenutzer aus.
2. Wählen Sie das Produkt aus, um die Seite Produktdetails zu öffnen. Überprüfen Sie in der Tabelle Startoptionen, ob der Amazon-Ressourcenname (ARN) der Rolle angezeigt wird.
3. Wählen Sie Produkt starten aus.
4. Führen Sie die Schritte zum Starten aus und geben Sie die erforderlichen Informationen ein.
5. Überprüfen Sie, ob das Produkt erfolgreich gestartet wird.

AWS Service Catalog-Benachrichtigungseinschränkungen

> **Note**
>
> AWS Service Catalog unterstützt keine Benachrichtigungseinschränkungen für Terraform Open Source- oder Terraform Cloud-Produkte.

Eine Benachrichtigungseinschränkung gibt ein Amazon SNS-Thema an, um Benachrichtigungen über Stack-Ereignisse zu erhalten.

Führen Sie die folgenden Schritte aus, um ein SNS-Thema zu erstellen und zu abonnieren.

So erstellen Sie ein SNS-Thema und ein Abonnement

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie Thema erstellen aus.
3. Geben Sie einen Namen für das Thema ein und klicken Sie dann auf Create Topic.

4. Wählen Sie Create subscription (Abonnement erstellen) aus.
5. Wählen Sie unter Protocol die Option Email aus. Geben Sie unter Endpoint eine E-Mail-Adresse ein, um die Benachrichtigungen zu empfangen. Wählen Sie Create subscription.
6. Sie erhalten eine Bestätigungs-E-Mail mit der Betreffzeile `AWS Notification - Subscription Confirmation`. Öffnen Sie die E-Mail und befolgen Sie die Anweisungen, um Ihr Abonnement abzuschließen.

Führen Sie die folgenden Schritte aus, um mithilfe des SNS-Themas, das Sie erstellt haben, eine Benachrichtigungseinschränkung anzuwenden.

So wenden Sie eine Benachrichtigungseinschränkung auf ein Produkt an

1. Öffnen Sie die Service-Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie das Portfolio aus, das das Produkt enthält.
3. Erweitern Sie Constraints (Einschränkungen) und wählen Sie Add constraints (Constraints hinzufügen).
4. Wählen Sie das Produkt unter Produkt aus und legen Sie den Einschränkungstyp auf Benachrichtigung fest. Klicken Sie auf Weiter.
5. Wählen Sie Choose a topic from your account aus und klicken Sie auf das SNS-Thema, das Sie unter Topic Name erstellt haben.
6. Wählen Sie Absenden aus.

Einschränkungen für die AWS Service Catalog-Tag-Aktualisierung

> **Note**
>
> AWS Service Catalog unterstützt keine Tag-Aktualisierungseinschränkungen für Terraform-Open-Source-Produkte.

Mit Einschränkungen bei der Tag-Aktualisierung können AWS Service Catalog Administratoren Endbenutzern erlauben oder verbieten, Tags für Ressourcen zu aktualisieren, die einem bereitgestellten Produkt zugeordnet sind. Wenn die Tag-Aktualisierung zulässig ist, werden während einer bereitgestellten Produktaktualisierung neue Tags, die dem Produkt oder Portfolio zugeordnet sind, auf bereitgestellte Ressourcen angewendet.

So aktivieren Sie Tag-Aktualisierungen für ein Produkt

1. Öffnen Sie die Service-Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie das Portfolio aus, das das Produkt enthält, das Sie aktualisieren möchten.
3. Wählen Sie die Registerkarte Einschränkungen und dann Einschränkungen hinzufügen aus.
4. Wählen Sie unter Constraint type (Einschränkungstyp) die Option Tag Update (Tag-Aktualisierung) aus.
5. Wählen Sie unter Product (Produkt) das Produkt aus und klicken Sie anschließend auf Continue (Weiter).
6. Wählen Sie auf der Seite Tag Updates die Option Enable Tag Updates (Tag-Aktualisierungen aktivieren) aus.
7. Wählen Sie Absenden aus.

AWS Service Catalog-Stack-Set-Einschränkungen

> **Note**
>
> - AWS Service Catalog unterstützt keine Stack-Set-Einschränkungen für Terraform-Open-Source-Produkte.
> - AutoTags werden derzeit mit nicht unterstütztAWS CloudFormation StackSets.

Eine Stack-Set-Einschränkung ermöglicht es Ihnen, Optionen für die Produktbereitstellung mit AWS CloudFormation zu konfigurieren StackSets. Sie können mehrere Konten und Regionen für den Produktstart angeben. Endbenutzer können diese Konten verwalten und bestimmen, wo Produkte bereitgestellt werden, und die Reihenfolge der Bereitstellung bestimmen.

So wenden Sie eine Stack-Set-Einschränkung auf ein Produkt an

1. Öffnen Sie die Service-Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie das Portfolio mit dem gewünschten Produkt aus.
3. Wählen Sie die Registerkarte Einschränkungen und dann Einschränkungen erstellen aus.
4. Wählen Sie unter Produkt das Produkt aus. Wählen Sie unter Einschränkungstyp die Option Stack-Set aus.

5. Konfigurieren Sie die Konten, Regionen und Berechtigungen für Ihre Stack-Set-Einschränkungen.

   - Identifizieren Sie unter Kontoeinstellungen die Konten, in denen Sie Produkte erstellen möchten.
   - Wählen Sie unter Regionseinstellungen die geografischen Regionen aus, in denen Produkte bereitgestellt werden sollen, und die Reihenfolge, in der diese Produkte in diesen Regionen bereitgestellt werden sollen.
   - Wählen Sie unter Berechtigungen eine IAM StackSet-Administratorrolle aus, um Ihre Zielkonten zu verwalten. Wenn Sie keine Rolle auswählen, StackSets verwendet den Standard-ARN. Erfahren Sie mehr über das Einrichten von Stack-Set-Berechtigungen.

6. Wählen Sie Create (Erstellen) aus.

AWS Service Catalog-Vorlageneinschränkungen

> **Note**
>
> AWS Service Catalog unterstützt keine Vorlageneinschränkungen für Terraform Open Source- oder Terraform Cloud-Produkte.

Um die Optionen für Endbenutzer zu beschränken, wenn sie ein Produkt starten, wenden Sie Vorlageneinschränkungen an. Wenden Sie Vorlageneinschränkungen an, um sicherzustellen, dass die Endbenutzer die Produkte verwenden können, ohne gegen die Compliance-Anforderungen Ihrer Organisation zu verstoßen. Sie wenden Vorlageneinschränkungen auf ein Produkt in einem AWS Service Catalog Portfolio an. Ein Portfolio muss ein oder mehrere Produkte enthalten, damit Sie Vorlageneinschränkungen definieren können.

Eine Vorlageneinschränkung besteht aus einer oder mehreren Regeln, die die zulässigen Werte für Parameter, die in der zugrunde liegenden AWS CloudFormation-Vorlage des Produkts definiert sind, beschränken. Die Parameter in einer AWS CloudFormation-Vorlage definieren die Menge von Werten, die Benutzer beim Erstellen eines Stacks angeben können. Ein Parameter kann z. B. die verschiedenen Instance-Typen definieren, die Benutzer beim Starten eines Stack mit EC2 Instances auswählen können.

Wenn die Menge der Parameterwerte in einer Vorlage für die Zielgruppe Ihres Portfolios zu ungenau ist, können Sie Vorlageneinschränkungen festlegen, um die Werte, die Benutzer beim Start eines

Produkts auswählen können, zu begrenzen. Wenn die Vorlagenparameter z. B. EC2 Instance-Typen umfassen, die zu groß für Benutzer sind, die nur Small Instance-Typen (wie `t2.micro` oder `t2.small`) verwenden sollen, können Sie eine Vorlageneinschränkung hinzufügen, um die Auswahl der Instance-Typen für Endbenutzer einzuschränken. Weitere Informationen über AWS CloudFormation-Vorlagenparameter finden Sie unter Parameter im AWS CloudFormation-Benutzerhandbuch.

Vorlageneinschränkungen sind in einem Portfolio gebunden. Wenn Sie Vorlageneinschränkungen auf ein Produkt in einem Portfolio anwenden und dann das Produkt in ein anderes Portfolio einschließen, gelten die Einschränkungen nicht für das Produkt im zweiten Portfolio.

Wenn Sie eine Vorlageneinschränkung auf ein Produkt anwenden, das bereits für Benutzer freigegeben ist, ist die Einschränkung sofort für alle nachfolgenden Produktstarts und für alle Versionen des Produkts im Portfolio aktiv.

Sie definieren Vorlageneinschränkungen mithilfe eines Regeleditors oder durch Schreiben von Regeln als JSON-Text in der AWS Service Catalog-Administratorkonsole. Weitere Informationen über Regeln, einschließlich Syntax und Beispiele, finden Sie unter Vorlageneinschränkungsregeln.

Zum Testen einer Einschränkung vor der Freigabe für die Benutzer erstellen Sie ein Testportfolio mit den gleichen Produkten und testen Sie die Einschränkungen mit diesem Portfolio.

So wenden Sie Vorlageneinschränkungen auf ein Produkt an

1. Öffnen Sie die Service-Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie auf der Seite Portfolios das Portfolio aus, das das Produkt enthält, auf das Sie eine Vorlageneinschränkung anwenden möchten.
3. Erweitern Sie den Abschnitt Einschränkungen und wählen Sie Einschränkungen hinzufügen aus.
4. Wählen Sie im Fenster Produkt und Typ auswählen für Produkt das Produkt aus, für das Sie die Vorlageneinschränkungen definieren möchten. Wählen Sie dann für Einschränkungstyp die Option Vorlage aus. Klicken Sie auf Weiter.
5. Bearbeiten Sie auf der Seite Vorlagen-Einschränkungs-Builder die Einschränkungsregeln mithilfe des JSON-Editors oder der Regel-Builder-Schnittstelle.

   - Um den JSON-Code für die Regel zu bearbeiten, wählen Sie die Registerkarte Texteditor der Einschränkung. Auf dieser Registerkarte stehen mehrere Beispiele zur Verfügung, die Sie bei den ersten Schritten unterstützen.

Um die Regeln mithilfe einer Rule Builder-Schnittstelle zu erstellen, wählen Sie die Registerkarte Rule Builder. Auf dieser Registerkarte können Sie jeden beliebigen Parameter auswählen, der in der Vorlage für das Produkt angegeben ist. Außerdem können Sie die zulässigen Werte für diese Parameter angeben. Abhängig von der Art des Parameter geben Sie die zulässigen Werte an, indem Sie Elemente in einer Checkliste auswählen, eine Zahl angeben oder eine Reihe von Werten in einer durch Komma getrennten Liste festlegen.

Wenn Sie mit der Erstellung einer Regel fertig sind, wählen Sie Regel hinzufügen aus. Die Regel wird in der Tabelle auf der Registerkarte Rule Builder angezeigt. Um die JSON-Ausgabe zu überprüfen und zu bearbeiten, wählen Sie die Registerkarte Texteditor der Einschränkung.

6. Wenn Sie mit der Bearbeitung der Regeln für Ihre Einschränkung fertig sind, wählen Sie Absenden aus. Um die Einschränkung anzuzeigen, gehen Sie zur Seite mit den Portfoliodetails und erweitern Sie Einschränkungen.

Vorlageneinschränkungsregeln

Die Regeln, die Vorlageneinschränkungen in einem AWS Service Catalog Portfolio definieren, beschreiben, wann Endbenutzer die Vorlage verwenden können und welche Werte sie für Parameter angeben können, die in der AWS CloudFormation Vorlage deklariert sind, die zum Erstellen des Produkts verwendet wird, das sie verwenden möchten. Regeln sind nützlich, um zu verhindern, dass Endbenutzer unabsichtlich einen falschen Wert angeben. Sie können beispielsweise eine Regel hinzufügen, um zu überprüfen, ob Endbenutzer ein gültiges Subnetz in einer bestimmten VPC angegeben oder `m1.small`-Instance-Typen für Testumgebungen verwendet haben. AWS CloudFormation verwendet Regeln, um Parameterwerte zu validieren, bevor die Ressourcen für das Produkt erstellt werden.

Jede Regel besteht aus zwei Eigenschaften: eine Regelbedingung (optional) und Assertions (erforderlich). Die Regelbedingung bestimmt, wann eine Regel wirksam wird. Die Assertions beschreiben, welche Werte Benutzer für einen bestimmten Parameter angeben können. Wenn Sie keine Regelbedingung definieren, werden die Assertions der Regel immer wirksam. Zum Definieren einer Regelbedingung und von Assertions verwenden Sie regelspezifische intrinsische Funktionen. Dies sind Funktionen, die nur im Abschnitt `Rules` einer Vorlage verwendet werden können. Sie können Funktionen verschachteln, aber das Endergebnis einer Regelbedingung oder Assertion muss entweder "true" oder "false" lauten.

Beispiel: Angenommen, Sie haben eine VPC und einen Subnetzparameter im Abschnitt `Parameters` deklariert. Sie können eine Regel erstellen, die validiert, das sich ein angegebenes Subnetz in einer

bestimmten VPC befindet. Wenn ein Benutzer eine VPC angibt, wertet AWS CloudFormation die Assertion aus, um zu überprüfen, ob sich der Subnetzparameterwert in dieser VPC befindet, bevor der Stack erstellt oder aktualisiert wird. Wenn der Parameterwert ungültig ist, tritt sofort ein Fehler auf und AWS CloudFormation erstellt oder aktualisiert den Stack nicht. Wenn Benutzer keine VPC angeben, überprüft AWS CloudFormation den Subnetzparameterwert nicht.

Syntax

Der Abschnitt `Rules` einer Vorlage besteht aus dem Schlüsselnamen `Rules`, gefolgt von einem einzigen Doppelpunkt. Regeldeklarationen werden durch Klammern eingeschlossen. Wenn Sie mehrere Regeln deklarieren, werden sie durch Kommas getrennt. Für jede Regel deklarieren Sie einen logischen Namen in Anführungszeichen gefolgt von einem Doppelpunkt und Klammern, die die Regelbedingung und Assertionen umschließen.

Eine Regel kann eine `RuleCondition`-Eigenschaft enthalten und muss eine `Assertions`-Eigenschaft einschließen. Für jede Regel können Sie nur eine Regelbedingung definieren. Innerhalb der `Assertions`-Eigenschaft können Sie eine oder mehrere Assertionen definieren. Sie definieren eine Regelbedingung und Assertionen mit regelspezifischen intrinsischen Funktionen, wie in der folgenden Pseudovorlage dargestellt:

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

Die Pseudovorlage zeigt einen `Rules`-Abschnitt mit zwei Regeln namens `Rule01` und `Rule02` an. `Rule01` enthält eine Regelbedingung und zwei Assertionen. Wenn die Funktion in der Regelbedingung mit "true" ausgewertet wird, werden beide Funktionen in jeder Assertion ausgewertet und angewendet. Wenn die Regelbedingung "false" ergibt, wird die Regel nicht wirksam. `Rule02` ist stets wirksam, da sie über keine Regelbedingung verfügt. Dies bedeutet, dass die eine Assertion immer ausgewertet und angewendet wird.

Informationen zu regelspezifischen intrinsischen Funktionen zum Definieren von Regelbedingungen und Assertionen finden Sie unter AWS Regelfunktionen im AWS CloudFormation - Benutzerhandbuch.

Beispiel: Bedingtes Überprüfen eines Parameterwerts

Die beiden folgenden Regeln überprüfen den Wert des Parameters `InstanceType`. Je nach Wert des Environment-Parameters (`test` oder `prod`) muss der Benutzer `m1.small` oder `m1.large` für den `InstanceType`-Parameter angeben. Die Parameter `InstanceType` und `Environment` müssen im `Parameters`-Abschnitt derselben Vorlage deklariert sein.

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

```
      {
        "Assert" :  { "Fn::Contains" : [ ["m1.large"], {"Ref" : "InstanceType"} ] },
        "AssertDescription" : "For the prod environment, the instance type must be
 m1.large"
      }
    ]
  }
}
```

AWS Service Catalog-Service-Aktionen

> **Note**
>
> AWS Service Catalog unterstützt keine Serviceaktionen für Terraform Open Source- oder Terraform Cloud-Produkte.

AWS Service Catalog ermöglicht es Ihnen, die administrative Wartung und das Training von Endbenutzern bei gleichzeitiger Konformität mit Compliance- und Sicherheitsanforderungen zu reduzieren. Service-Aktionen ermöglichen es Ihnen (als Administrator), Endbenutzern das Ausführen operativer Aufgaben, das Beheben von Problemen, das Ausführen von genehmigten Befehlen oder das Ändern von Berechtigungen in AWS Service Catalog zu erlauben. Sie verwenden AWS Systems Manager-Dokumente, um Service-Aktionen durchzuführen. Die AWS Systems Manager Dokumente bieten Zugriff auf vordefinierte Aktionen, die AWS bewährte Methoden implementieren, z. B. Amazon EC2 beenden und neu starten, und Sie können auch benutzerdefinierte Aktionen definieren.

In diesem Tutorial bieten Sie Endbenutzern die Möglichkeit, eine Amazon EC2 neu zu starten. Sie fügen die erforderlichen Berechtigungen hinzu, definieren die Service-Aktion, ordnen die Service-Aktion einem Produkt zu und testen die Endbenutzererfahrung mit der Aktion mit einem bereitgestellten Produkt.

Voraussetzungen

In diesem Tutorial wird davon ausgegangen, dass Sie über vollständigen AWS-Verwaltungszugriff auf Berechtigungen verfügen, bereits mit AWS Service Catalog vertraut sind und dass Sie bereits über eine Reihe von Produkten, Portfolios und Benutzern verfügen. Wenn Sie mit AWS Service Catalog nicht vertraut sind, schließen Sie die Einrichtung und Erste Schritte-Aufgaben ab, bevor Sie dieses Tutorial verwenden.

Themen

- Schritt 1: Konfigurieren von Berechtigungen für Endbenutzer
- Schritt 2: Erstellen einer Service-Aktion
- Schritt 3: Verknüpfen der Service-Aktion mit einer Produktversion
- Schritt 4: Testen der Endbenutzerumgebung
- Schritt 5: Verwalten von Service-Aktionen mit AWS CloudFormation
- Schritt 6: Fehlerbehebung

Schritt 1: Konfigurieren von Berechtigungen für Endbenutzer

Endbenutzer müssen über die erforderlichen Berechtigungen verfügen, um bestimmte Service-Aktionen anzuzeigen und auszuführen. In diesem Beispiel benötigt der Endbenutzer die Berechtigung für den Zugriff auf die AWS Service Catalog Service-Aktionsfunktion und zum Durchführen eines Amazon EC2-Neustarts.

Aktualisieren von Berechtigungen

1. Öffnen Sie die AWS Identity and Access Management (IAM)-Konsole unter https://console.aws.amazon.com/iam/.
2. Suchen Sie im Menü Benutzergruppen.
3. Wählen Sie die Gruppen aus, die Endbenutzer für den Zugriff auf -AWS Service CatalogRessourcen verwenden werden. In diesem Beispiel wählen wir die Endbenutzergruppe. Wählen Sie in Ihrer eigenen Implementierung die Gruppe aus, die von den relevanten Endbenutzern verwendet wird.
4. Auf der Registerkarte Berechtigungen der Detailseite Ihrer Gruppe erstellen Sie entweder eine neue Richtlinie oder bearbeiten eine bereits bestehende. In diesem Beispiel fügen wir einer bereits bestehenden Richtlinie Berechtigungen hinzu, indem wir die benutzerdefinierte Richtlinie auswählen, die für AWS Service Catalog-Berechtigungen der Gruppe zum Bereitstellen und Beenden erstellt wurde.
5. Auf der Seite Richtlinie wählen Sie Edit Policy (Richtlinie bearbeiten) aus, um notwendige Berechtigungen hinzuzufügen. Sie können entweder den visuellen Editor oder den JSON-Editor verwenden, um die Richtlinie zu bearbeiten. In diesem Beispiel verwenden wir den JSON-Editor, um die Berechtigungen hinzuzufügen. Bei diesem Tutorial fügen Sie folgende Berechtigungen der Richtlinie hinzu:

```
{
 "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. Nachdem Sie die Richtlinie bearbeitet haben, überprüfen und genehmigen Sie die Änderung der Richtlinie. Benutzer in der Endbenutzergruppe verfügen jetzt über die erforderlichen Berechtigungen, um die Amazon EC2-Neustartaktion in durchzuführenAWS Service Catalog.

Schritt 2: Erstellen einer Service-Aktion

Als Nächstes erstellen Sie eine Serviceaktion zum Neustarten von Amazon EC2.

1. Öffnen Sie die -AWS Service CatalogKonsole unter https://console.aws.amazon.com/sc/.
2. Wählen Sie im Menü die Option Service Actions (Service-Aktionen) aus.
3. Wählen Sie auf der Seite Serviceaktionen die Option Aktion erstellen aus.
4. Wählen Sie auf der Seite Create Action (Aktion erstellen) ein AWS Systems Manager-Dokument zur Definition der Service-Aktion aus. Die Amazon EC2 Instance Restart-Aktion wird durch ein -AWS Systems ManagerDokument definiert. Daher behalten wir die Standardoption im Dropdown-Menü bei, Amazon-Dokumente .

5. Suchen Sie nach der Aktion AWS-RestartEC2Instance und wählen Sie sie aus.
6. Geben Sie für Ihr Team und Ihre Umgebung einen sinnvollen Namen und eine sinnvolle Beschreibung für die Aktion an. Für den Endbenutzer ist diese Beschreibung sichtbar. Wählen Sie also eine Beschreibung, die dem Benutzer hilft, die Auswirkung der Aktion zu verstehen.
7. Wählen Sie unter Parameter- und Zielkonfiguration den SSM-Dokumentparameter aus, der das Ziel der Aktion sein soll (z. B. die Instance-ID), und wählen Sie das Ziel des Parameters aus. Wählen Sie Add parameter (Parameter hinzufügen) aus, um weitere Parameter hinzuzufügen.
8. Wählen Sie unter Permissions (Berechtigungen) eine Rolle aus. Wir verwenden in diesem Beispiel Standardberechtigungen. Andere Berechtigungskonfigurationen sind möglich und werden auf dieser Seite definiert.
9. Nachdem Sie die Konfiguration überprüft haben, wählen Sie die Option Create action (Aktion erstellen).
10. Auf der nächsten Seite wird eine eine Bestätigung angezeigt, sobald die Aktion erstellt wurde und einsatzbereit ist.

Schritt 3: Verknüpfen der Service-Aktion mit einer Produktversion

Nachdem Sie eine Aktion definiert haben, müssen Sie ein Produkt mit dieser Aktion verknüpfen.

1. Wählen Sie auf der Seite Service-Aktionen die Option AWS-RestartEC2instance und dann Aktion zuordnen aus.
2. Wählen Sie auf der Seite Associate action (Aktion zuordnen) das Produkt aus, auf dem Endbenutzer die Service-Aktion durchführen sollen. In diesem Beispiel wählen wir Linux Desktop (Linux-Desktop).
3. Wählen Sie eine Produktversion aus. Hinweis: Verwenden Sie das oberste Kontrollkästchen, um alle Versionen auszuwählen.
4. Wählen Sie Associate action (Aktion zuordnen) aus.
5. Auf der nächsten Seite erscheint eine Bestätigungsmitteilung.

Sie haben nun eine Service Aktion in AWS Service Catalog erstellt. Der nächste Schritt dieses Tutorials ist die Verwendung der Service-Aktion als Endbenutzer.

Schritt 4: Testen der Endbenutzerumgebung

Endbenutzer können Service-Aktionen auf bereitgestellten Produkten ausführen. Zum Zweck dieses Tutorials muss der Endbenutzer über mindestens ein bereitgestelltes Produkt verfügen. Das bereitgestellte Produkt muss von der Produktversion gestartet werden, die Sie im vorherigen Schritt mit der Service-Aktion verknüpft haben.

Zugriff des Endbenutzers auf die Service-Aktion

1. Melden Sie sich als Endbenutzer an der AWS Service Catalog-Konsole an.
2. Wählen Sie auf dem AWS Service Catalog-Dashboard im Navigationsbereich Provisioned products list (Liste der bereitgestellten Produkte) aus. Die Liste zeigt die Produkte, die für das Konto des Endbenutzers bereitgestellt werden.
3. Wählen Sie auf der Seite Provisioned products list (Liste der bereitgestellten Produkte) die bereitgestellte Instance aus.
4. Wählen Sie auf der Seite Bereitgestellte Produktdetails oben rechts Aktionen und dann die Aktion AWS-RestartEC2instance aus.
5. Bestätigen Sie, dass Sie die benutzerdefinierte Aktion ausführen möchten. Sie erhalten eine Bestätigung über das Senden der Aktion.

Schritt 5: Verwalten von Service-Aktionen mit AWS CloudFormation

Sie können Serviceaktionen und deren Zuordnungen zu -AWS CloudFormationRessourcen erstellen. Weitere Informationen finden Sie in folgenden Themen im AWS CloudFormation-Benutzerhandbuch:

- AWS::ServiceCatalog::CloudFormationProdukt ProvisioningArtifactProperties
- AWS::ServiceCatalog::ServiceActionZuordnung

> **Note**
>
> Wenn Sie Service-Aktionszuordnungen mit -AWS CloudFormationRessourcen verwalten, fügen Sie Service-Aktionen nicht über die oder hinzu AWS Command Line Interface oder entfernen Sie sieAWS Management Console. Wenn Sie eine Stack-Aktualisierung durchführen, AWS CloudFormation werden alle Änderungen an den -Bereinigungsaktionen, die außerhalb von vorgenommen werden, ersetzt.

Schritt 6: Fehlerbehebung

Wenn die Ausführung Ihrer Service-Aktion fehlschlägt, finden Sie die Fehlermeldung im Abschnitt Outputs (Ausgaben) des Service-Aktionsereignisses auf der Seite Provisioned product (Bereitgestelltes Produkt) . Im Folgenden finden Sie Erläuterungen zu häufig auftretenden Fehlermeldungen.

> **Note**
>
> Der genaue Text der Fehlermeldung kann sich ändern, daher sollten Sie diese nicht in automatisierten Prozessen irgendwelcher Art verwenden.

Internal failure (Interner Fehler)

In AWS Service Catalog ist ein interner Fehler aufgetreten. Bitte versuchen Sie es später erneut. Wenn das Problem bestehen bleibt, wenden Sie sich an den Kundenservice.

Beim Aufrufen der - StartAutomationExecution Operation ist ein Fehler aufgetreten (ThrottlingException)

Die Ausführung der Service-Aktion wurde vom Backend-Service wie SSM gedrosselt.

Access denied while assuming the role (Zugriff beim Übernehmen der Rolle)

AWS Service Catalog konnte die in der Service-Aktionsdefinition angegebene Rolle nicht übernehmen. Stellen Sie sicher, dass der servicecatalog.amazonaws.com-Prinzipal oder ein regionaler Prinzipal wie servicecatalog.us-east-1.amazonaws.com in der Vertrauensrichtlinie der Rolle auf die Zulassungsliste gesetzt ist.

Beim Aufrufen der - StartAutomationExecution Operation ist ein Fehler (AccessDeniedException) aufgetreten: Der Benutzer ist nicht berechtigt, Folgendes auszuführen: ssm:StartAutomationExecution auf der Ressource.

Die in der Serviceaktionsdefinition angegebene Rolle verfügt nicht über Berechtigungen zum Aufrufen von ssm:StartAutomationExecution. Stellen Sie sicher, dass die Rolle über die entsprechenden SSM-Berechtigungen verfügt.

Ressourcen mit dem Typ ***`TargetType`*** im bereitgestellten Produkt können nicht gefunden werden

Das bereitgestellte Produkt enthält keine Ressourcen, die dem im SSM-Dokument angegebenen Zieltyp entsprechen, z. B. AWS::EC2::Instance. Überprüfen Sie das bereitgestellte Produkt auf diese Ressourcen, bzw., ob das Dokument korrekt ist.

Document with that name does not exist (Ein Dokument mit diesem Namen ist nicht vorhanden)

Das in der Service-Aktionsdefinition angegebene Dokument ist nicht vorhanden.

Failed to describe SSM Automation document (Das SSM Automation-Dokument konnte nicht beschrieben werden)

AWS Service Catalog ist beim Versuch, das angegebene Dokument zu beschreiben, auf eine unbekannte Ausnahme von SSM gestoßen.

Failed to retrieve credentials for role (Anmeldeinformationen für die Rolle konnten nicht angerufen werden)

Bei AWS Service Catalog ist bei der Übernahme der angegebenen Rolle ein unbekannter Fehler aufgetreten.

Der Parameter hat den Wert "***InvalidValue***" wurde in ***{ValidValue1}, {ValidValue2}*** nicht gefunden

Der an SSM übergebene Parameterwert befindet sich nicht in der Liste der zulässigen Werte für das Dokument. Überprüfen Sie, ob die angegebenen Parameter gültig sind, und versuchen Sie es erneut.

Fehler beim Parametertyp. Der für angegebene Wert ***ParameterName*** ist keine gültige Zeichenfolge.

Der Wert des an SSM übergebenen Parameters ist für den Typ im Dokument nicht gültig.

Parameter is not defined in service action definition (Parameter ist in der Service-Aktionsdefinition nicht definiert)

Es wurde ein Parameter an AWS Service Catalog übergeben, der in der Service-Aktionsdefinition nicht definiert ist. Sie können nur Parameter verwenden, die in der Service-Aktionsdefinition definiert sind.

Der Schritt schlägt fehl, wenn er ausgeführt wird/die Aktion beendet. ***Fehlermeldung.*** Weitere Diagnosedetails finden Sie im Automation Service-Fehlerbehebungshandbuch.

Ein Schritt im SSM-Automatisierungsdokument ist fehlgeschlagen. Vgl. den Fehler in der Meldung zur weiteren Problembehandlung.

Die folgenden Werte für den Parameter sind nicht zulässig, da sie sich nicht im bereitgestellten Produkt befinden: ***InvalidResourceId***

Der Benutzer hat die Aktion für eine Ressource angefordert, die sich nicht im bereitgestellten Produkt befindet.

TargetType nicht für SSM-Automatisierungsdokument definiert

Serviceaktionen erfordern, dass SSM-Automatisierungsdokumente über eine TargetType definierte verfügen. Überprüfen Sie Ihr SSM-Automatisierungsdokument.

Hinzufügen von AWS Marketplace-Produkten zu Ihrem Portfolio

Sie können Sie Ihren Portfolios AWS Marketplace-Produkte hinzufügen, um sie Ihren AWS Service Catalog-Endbenutzern verfügbar zu machen.

AWS Marketplace ist ein Online-Shop, in dem Sie eine große Auswahl von Software und Services finden, abonnieren und sofort nutzen können. Die Arten von Produkten in AWS Marketplace umfassen Datenbanken, Anwendungsserver, Test-, Überwachungs-und Content Management-Tools sowie Business Intelligence-Software. AWS Marketplace ist erhältlich unter https://aws.amazon.com/marketplace. Beachten Sie, dass Sie keine Software as a Service (SaaS)-Produkte von AWS Marketplace zu hinzufügen könnenAWS Service Catalog.

Sie verteilen ein -AWS MarketplaceProdukt an AWS Service Catalog EndbenutzerAWS Service Catalog, indem Sie das Produkt mit der AWS CloudFormation Vorlage in kopieren und dann das Produkt einem Portfolio hinzufügen.

> **Note**
>
> AWS Service Catalog unterstützt nicht die Verteilung von AWS Marketplace Produkten an AWS Service Catalog Endbenutzer mithilfe einer Terraform Open Source- oder Terraform Cloud-Produktvorlage.

AWS Marketplace unterstützt AWS Service Catalog direkt. Sie können Produkte auch abonnieren und mit der manuellen Option hinzufügen. Wir empfehlen das Hinzufügen von Produkten mithilfe der Funktionalität, die speziell für AWS Service Catalog entwickelt wurde.

Verwalten von AWS Marketplace-Produkten mithilfe von AWS Service Catalog

Sie können Ihre abonnierten AWS Marketplace-Produkte AWS Service Catalog mithilfe einer benutzerdefinierten Schnittstelle direkt hinzufügen. Wählen Sie unter AWS Marketplace die Option Service Catalog aus. Weitere Informationen finden Sie unter Kopieren von Produkten in AWS Service Catalog im AWS Marketplace Hilfehandbuch und unter Häufig gestellte Fragen zu .

Verwalten und manuelles Hinzufügen von AWS Marketplace-Produkten

Führen Sie die folgenden Schritte aus, um ein -AWS MarketplaceProdukt zu abonnieren, dieses Produkt in einer -AWS CloudFormationVorlage zu definieren und die Vorlage einem AWS Service Catalog Portfolio hinzuzufügen.

So abonnieren Sie ein AWS Marketplace-Produkt

1. Rufen Sie AWS Marketplace unter https://aws.amazon.com/marketplace auf.
2. Durchsuchen Sie die Produkte oder führen Sie eine Suche nach dem Produkt durch, das Sie Ihrem AWS Service Catalog-Portfolio hinzufügen möchten. Wählen Sie das Produkt aus, um die Seite mit den Produktdetails zu öffnen.
3. Wählen Sie Weiter aus, um die -Erfüllungsseite anzuzeigen, und wählen Sie dann die Registerkarte Manueller Start.

   Die Informationen auf der -Erfüllungsseite umfassen die unterstützten Instance-Typen von Amazon Elastic Compute Cloud (Amazon EC2), die AWS-Regionenunterstützten und die Amazon Machine Image (AMI)-ID, die das Produkt für jede AWS Region verwendet. Beachten Sie, dass bei einigen Optionen Kosten anfallen. Sie benötigen diese Informationen, um die AWS CloudFormation-Vorlage später anzupassen.
4. Wählen Sie Accept Terms aus, um das Produkt zu abonnieren.

   Nachdem Sie ein Produkt abonnieren, können Sie jederzeit auf die Informationen auf der Produktbereitstellungsseite in AWS Marketplace zugreifen, indem Sie Ihre Software und dann das Produkt auswählen.

So definieren Sie Ihr AWS Marketplace-Produkt in einer AWS CloudFormation-Vorlage

Für die folgenden Schritte verwenden Sie eine der AWS CloudFormation-Beispielvorlagen als Ausgangspunkt und passen die Vorlage an, sodass sie Ihr AWS Marketplace-Produkt repräsentiert.

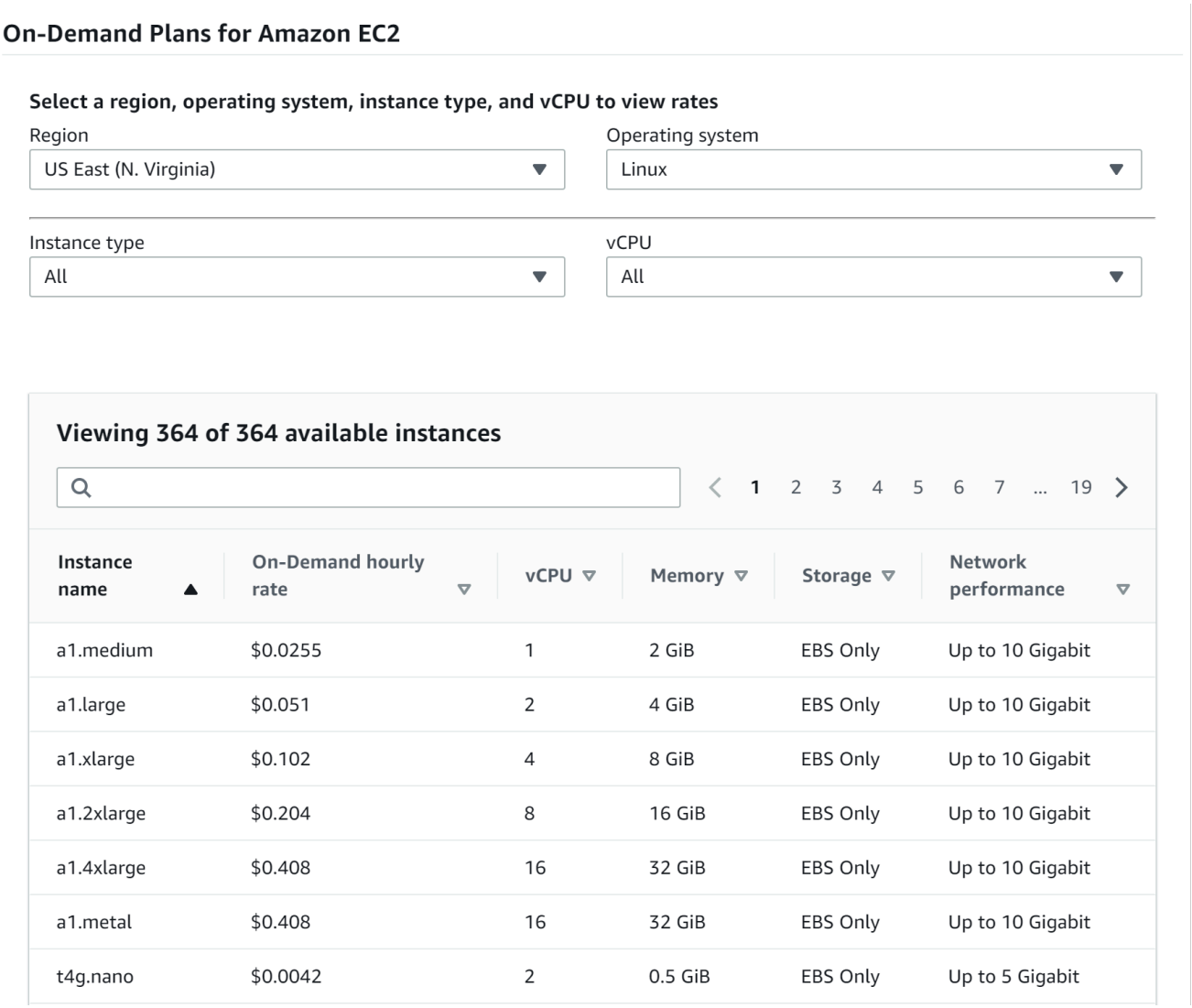
Informationen zum Zugriff auf die Beispielvorlagen finden Sie unter Mustervorlagen im AWS CloudFormation-Benutzerhandbuch.

1. Wählen Sie auf der Seite Beispielvorlagen im AWS CloudFormation-Benutzerhandbuch eine -AWSRegion für Ihr Produkt aus. Die AWS Region muss von Ihrem AWS Marketplace Produkt unterstützt werden. Sie können die unterstützten Regionen auf der Produktbereitstellungsseite in AWS Marketplace anzeigen.
2. Um eine Liste der für die Region geeigneten Servicebeispielvorlagen anzuzeigen, wählen Sie den Link Services.
3. Sie können ein beliebiges Beispiel, das für Ihre Zwecke geeignet ist, als Ausgangspunkt verwenden. Für die Schritte in diesem Verfahren wird die Vorlage Amazon EC2 instance in a security group genutzt. Zum Anzeigen der Beispielvorlage wählen Sie View aus und speichern Sie eine Kopie der Vorlage lokal, sodass Sie sie bearbeiten können. Ihre lokale Datei muss die Erweiterung `.template` haben.
4. Öffnen Sie die Vorlagendatei in einem Texteditor.
5. Passen Sie die Beschreibung oben in der Vorlage an. Ihre Beschreibung kann folgendermaßen aussehen:

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

6. Passen Sie den Parameter `InstanceType` an, so dass er nur die EC2 Instance-Typen umfasst, die von Ihrem Produkt unterstützt werden. Wenn Ihre Vorlage nicht unterstützte EC2 Instance-Typen enthält, kann das Produkt für Ihre Endbenutzer nicht gestartet werden.

   a. Zeigen Sie auf der Produkterfüllungsseite in die AWS Marketplaceunterstützten EC2-Instance-Typen im Abschnitt Preisdetails an.



b. Ändern Sie den standardmäßigen Instance-Typ in Ihrer Vorlage in einen unterstützten EC2 Instance-Typ Ihrer Wahl.

c. Bearbeiten Sie die Liste `AllowedValues`, so dass sie nur die EC2 Instance-Typen umfasst, die von Ihrem Produkt unterstützt werden.

d. Entfernen Sie alle EC2 Instance-Typen, die Ihre Endbenutzer beim Starten des Produkts von der Liste `AllowedValues` aus nicht verwenden sollen.

Der bearbeitete Parameter `InstanceType` kann wie im folgenden Beispiel dargestellt aussehen:

```
"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. Bearbeiten Sie im Bereich `Mappings` Ihrer Vorlage die `AWSInstanceType2Arch`-Zuweisungen so, dass nur unterstützte EC2 Instance-Typen und Architekturen enthalten sind.

   a. Bearbeiten Sie die Liste der Zuweisungen, indem Sie alle EC2 Instance-Typen entfernen, die nicht in der Liste `AllowedValues` des Parameters `InstanceType` enthalten sind.

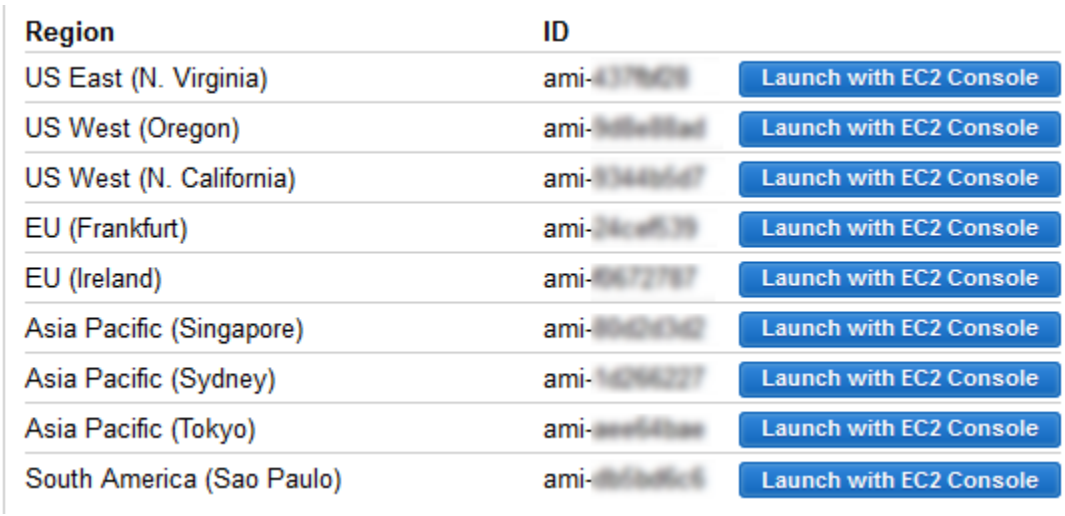
   b. Legen Sie den Wert `Arch` für jeden einzelnen EC2 Instance-Typ auf den Architekturtyp fest, der von Ihrem Produkt unterstützt wird. Gültige Werte sind `PV64`, `HVM64` und `HVMG2`. Informationen darüber, welche Architektur von Ihrem Produkt unterstützt wird, finden Sie auf der Produktdetailseite in AWS Marketplace. Informationen dazu, welche Architekturen von EC2 Instance-Familien unterstützt werden, finden Sie unter Amazon Linux-AMI-Instance-Typ-Matrix.

   Die bearbeiteten `AWSInstanceType2Arch`-Zuweisungen können wie im folgenden Beispiel dargestellt aussehen:

```
    "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. Bearbeiten Sie im `Mappings` Abschnitt Ihrer Vorlage die `AWSRegionArch2AMI` Zuordnungen, um jede AWS Region der entsprechenden Architektur und AMI-ID für Ihr Produkt zuzuordnen.

   a. Zeigen Sie auf der Produkterfüllungsseite in die AMI-ID anAWS Marketplace, die Ihr Produkt für jede AWS Region verwendet, wie im folgenden Beispiel:



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. Entfernen Sie in Ihrer Vorlage die Zuordnungen für alle AWS Regionen, die Sie nicht unterstützen.

   c. Bearbeiten Sie die Zuweisungen für jede Region, um die nicht unterstützten Architekturen (`PV64`, `HVM64` oder `HVMG2`) und die zugehörigen AMI-IDs zu entfernen.

   d. Geben Sie für jede verbleibende AWS Region und Architekturzuordnung die entsprechende AMI-ID auf der Produktdetailseite in anAWS Marketplace.

   Nach der Bearbeitung der `AWSRegionArch2AMI`-Zuweisungen kann Ihr Code wie im folgenden Beispiel dargestellt aussehen:

```
"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"}
```

```
    }
```

Sie können jetzt die Vorlage verwenden, um das Produkt einem AWS Service Catalog Portfolio hinzuzufügen. Wenn Sie weitere Änderungen vornehmen möchten, lesen Sie die Informationen über Vorlagen unter Arbeiten mit AWS CloudFormation-Vorlagen.

So fügen Sie Ihr AWS Marketplace Produkt einem AWS Service Catalog Portfolio hinzu

1. Melden Sie sich bei der an AWS Management Console und navigieren Sie zur AWS Service Catalog Administratorkonsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie auf der Seite Portfolios das Portfolio aus, dem Sie Ihr AWS Marketplace Produkt hinzufügen möchten.
3. Wählen Sie auf der Seite mit den Portfoliodetails die Option Neues Produkt hochladen aus.
4. Geben Sie die angeforderten Produkt- und Support-Details an.
5. Klicken Sie auf der Seite Version details auf Upload a template file, wählen Sie Durchsuchen und dann die Vorlagendatei aus.
6. Geben Sie einen Versionstitel und eine Beschreibung ein.
7. Wählen Sie Weiter aus.
8. Überprüfen Sie auf der Seite Überprüfen, ob die Zusammenfassung korrekt ist, und wählen Sie dann Bestätigen und hochladen aus. Das Produkt wird Ihrem Portfolio hinzugefügt. Es ist jetzt für Endbenutzer verfügbar, die Zugriff auf das Portfolio haben.

Verwenden von AWS CloudFormation StackSets

> **Note**
>
> AutoTags werden derzeit mit nicht unterstütztAWS CloudFormation StackSets.

Sie können verwendenAWS CloudFormation StackSets , um AWS Service Catalog Produkte über mehrere - AWS-Regionen und -Konten hinweg zu starten. Sie können die Reihenfolge angeben, in der Produkte sequenziell in bereitgestellt werdenAWS-Regionen. In Konten werden Produkte parallel bereitgestellt. Beim Start können Benutzer die Fehlertoleranz und die maximale Anzahl der Konten angeben, in denen die Bereitstellung parallel erfolgen soll. Weitere Informationen finden Sie unter Arbeiten mit AWS CloudFormation StackSets.

Stack-Sets und Stack-Instances

Mit einem Stack-Set können Sie mithilfe einer einzigen AWS CloudFormation Vorlage Stacks in AWS Konten über -AWSRegionen hinweg erstellen.

Eine Stack-Instance bezieht sich auf einen Stack in einem Zielkonto innerhalb einer -AWSRegion und ist nur einem Stack-Set zugeordnet.

Weitere Informationen finden Sie unter StackSets-Konzepte.

Stack-Set-Einschränkungen

In AWS Service Catalog können Sie mittels Stack-Set-Einschränkungen Produktbereitstellungsoptionen konfigurieren.

AWS Service Catalog unterstützt Stack-Set-Einschränkungen für Produkte in zwei AWS GovCloud (US) Regions: AWS GovCloud (USA-West) und AWS GovCloud (USA-Ost).

Weitere Informationen finden Sie unter AWS Service Catalog Stack-Set-Einschränkungen.

Verwalten von Budgets

Sie können AWS-Budgets verwenden, um Ihre Servicekosten und -nutzung in AWS Service Catalog nachzuverfolgen. Sie können Budgets mit AWS Service Catalog-Produkten und -Portfolios verknüpfen.

> **Note**
>
> AWS Service Catalog unterstützt keine Budgets für Terraform-Open-Source-Produkte.

Durch AWS-Budgets können Sie benutzerdefinierte Budgets festlegen und sich benachrichtigen lassen, sobald Ihre Kosten oder Ihre Nutzung den veranschlagten Betrag überschreiten (oder voraussichtlich überschreiten). Informationen zu AWS-Budgets finden Sie unter https://aws.amazon.com/aws-cost-management/aws-budgets.

Aufgaben

- Voraussetzungen
- Erstellen eines Budgets

- Ein Budget zuordnen
- Ein Budget anzeigen
- Die Zuordnung eines Budgets aufheben

Voraussetzungen

Bevor Sie AWS-Budgets verwenden, müssen Sie Kostenzuordnungs-Tags in der AWS Billing and Cost Management-Konsole aktivieren. Weitere Informationen finden Sie unter Benutzerdefinierte Kostenzuordnungs-Tags aktivieren im AWS Billing and Cost Management-Benutzerhandbuch.

> **Note**
>
> Die Aktivierung von Tags dauert bis zu 24 Stunden.

Darüber hinaus müssen Sie den Benutzerzugriff auf die AWS Billing and Cost Management-Konsole für alle Benutzer oder Gruppen aktivieren, die die Funktion Budgets verwenden werden. Sie können dies tun, indem Sie eine neue Richtlinie für Ihre Benutzer erstellen.

Damit -Benutzer Budgets erstellen können, müssen Sie Benutzern auch erlauben, Fakturierungsinformationen anzuzeigen. Wenn Sie Amazon SNS-Benachrichtigungen verwenden möchten, können Sie Benutzern die Möglichkeit geben, Amazon SNS-Benachrichtigungen zu erstellen, wie im folgenden Richtlinienbeispiel gezeigt.

So erstellen Sie die Budgets-Richtlinie

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Policies aus.
3. Wählen Sie im Inhaltsbereich die Option Create policy (Richtlinie erstellen).
4. Wählen Sie die Registerkarte JSON aus und kopieren Sie den Text aus dem folgenden JSON-Richtliniendokument. Fügen Sie den folgenden Text in das JSON-Eingabefeld ein.

```
{
    "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. Wählen Sie, wenn Sie fertig sind, Review policy (Richtlinie überprüfen). Die Richtlinienvalidierung meldet mögliche Syntaxfehler.
6. Geben Sie Ihrer Richtlinie auf der Seite Review (Überprüfen) einen Namen. Überprüfen Sie die Summary (Übersicht) der Richtlinie, um die durch Ihre Richtlinie erteilten Berechtigungen zu sehen und wählen Sie dann zum Speichern Create policy (Richtlinie erstellen).

   Die neue Richtlinie wird in der Liste der verwalteten Richtlinien angezeigt und kann Ihren Benutzern und Gruppen angefügt werden. Weitere Informationen finden Sie unter Erstellen und Anfügen einer vom Kunden verwalteten Richtlinie im AWS Identity and Access Management-Benutzerhandbuch.

Erstellen eines Budgets

In der AWS Service Catalog Administratorkonsole werden auf den Seiten Produktliste und Portfolios Informationen zu vorhandenen Produkten und Portfolios aufgeführt und Sie können Maßnahmen

für sie ergreifen. Um ein Budget zu erstellen, entscheiden Sie zunächst, mit welchem Produkt oder Portfolio Sie das Budget verknüpfen möchten.

Ein Budget erstellen

1. Öffnen Sie die Service-Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie Produktliste oder Portfolios aus.
3. Wählen Sie das Produkt oder Portfolio aus, dem Sie ein Budget hinzufügen möchten.
4. Öffnen Sie das Menü Aktionen und wählen Sie dann Budget erstellen aus.
5. Ordnen Sie Ihrem Budget auf der Seite Budget creation (Budgeterstellung) einen Tag-Typ zu.

   Es gibt zwei Arten von Tags: AutoTags und TagOptions. AutoTags identifizieren das Portfolio, das Produkt und den Benutzer, der ein Produkt gestartet hat. AWS Service Catalog wendet diese Tags automatisch auf bereitgestellte Ressourcen an. Ein TagOption ist ein vom Administrator definiertes Schlüssel-Wert-Paar, das in verwaltet wirdAWS Service Catalog.

   Damit Ausgaben, die für ein Portfolio oder Produkt entstehen, das zugehörige Budget berücksichtigen, müssen sie über das gleiche Tag verfügen. Beachten Sie, dass die Aktivierung eines erstmalig verwendeten Tag-Schlüssels 24 Stunden in Anspruch nehmen kann. Weitere Informationen finden Sie unter the section called “Voraussetzungen”.
6. Wählen Sie Erstellen in ausAWS Budgets. Sie werden zur Seite Budget festlegen weitergeleitet. Fahren Sie mit der Einrichtung Ihres Budgets fort, indem Sie die Schritte unter Erstellen eines Budgets befolgen.

> **Note**
>
> Nachdem Sie ein Budget erstellt haben, müssen Sie es dem Produkt oder Portfolio zuordnen.

Ein Budget zuordnen

Jedem Portfolio oder Produkt kann ein Budget zugeordnet sein. Jedes Budget kann mehreren Portfolios und Produkten zugeordnet werden.

Wenn Sie einem Portfolio oder Produkt ein Budget zuordnen, können Sie Informationen über das Budget auf der Detailseite dieses Portfolios oder Produkts anzeigen. Damit Ausgaben, die für das

Portfolio oder Produkt anfallen, im Budget berücksichtigt werden, müssen Sie dieselben Tags im Budget und Portfolio oder Produkt zuordnen.

> **Note**
>
> Wenn Sie ein Budget aus löschenAWS Budgets, bestehen weiterhin bestehende Verknüpfungen mit AWS Service Catalog Produkten und Portfolios. kann keine Informationen über das AWS Service Catalog gelöschte Budget anzeigen.

So ordnen Sie ein Budget zu

1. Öffnen Sie die Service-Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie Produktliste oder Portfolios aus.
3. Wählen Sie das Produkt oder Portfolio aus, dem Sie ein Budget zuordnen möchten.
4. Öffnen Sie das Menü Aktionen und wählen Sie dann Budget zuordnen aus.
5. Wählen Sie auf der Seite Budgetzuordnung ein vorhandenes Budget aus und wählen Sie dann Weiter aus.
6. Die Tabelle Produkte oder Portfolios enthält jetzt Daten für das Budget, das Sie gerade hinzugefügt haben.

Ein Budget anzeigen

Wenn einem Produkt ein Budget zugeordnet ist, können Sie Informationen über das Budget auf den Seiten Produktdetails und Produktliste anzeigen. Wenn einem Portfolio ein Budget zugeordnet ist, können Sie Informationen über das Budget auf den Seiten Portfolios und Portfoliodetails anzeigen.

Auf den Seiten Portfolios und Produktliste werden Budgetinformationen für vorhandene Ressourcen angezeigt. Sie können Spalten mit den Bezeichnungen Current vs. budget (Ist im Vegleich mit Budget) und Forecast vs. budget (Prognose im Vergleich mit Budget) anzeigen.

Wenn Sie ein Produkt oder Portfolio auswählen, werden Sie zu einer Detailseite weitergeleitet. Die Seiten Portfoliodetails und Produktdetails enthalten Abschnitte mit detaillierten Informationen zu den zugehörigen Budgets. Sie können den veranschlagten Betrag, die aktuellen Ausgaben und die prognostizierten Ausgaben anzeigen. Sie haben auch die Möglichkeit, Budgetdetails anzuzeigen und das Budget zu bearbeiten.

Die Zuordnung eines Budgets aufheben

Sie können die Zuordnung eines Budgets zu einem Portfolio oder Produkt aufheben.

> **Note**
>
> Wenn Sie ein Budget aus AWS Budgets löschen, bestehen weiterhin bestehende Zuordnungen zu AWS Service Catalog Produkten und Portfolios. AWS Service Catalog kann keine Informationen über das gelöschte Budget anzeigen.

So heben Sie die Zuordnung eines Budgets auf

1. Öffnen Sie die Service-Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie Produktliste oder Portfolios aus.
3. Wählen Sie das Produkt oder Portfolio aus, von dem Sie ein Budget trennen möchten.
4. Wählen Sie Aktionen. Wählen Sie in der Dropdownliste Budget aufheben aus. Eine Bestätigungswarnung wird angezeigt.
5. Nachdem Sie bestätigt haben, dass Sie das Budget vom Produkt oder Portfolio trennen möchten, wählen Sie Bestätigen aus.

Verwalten von bereitgestellten Produkten

AWS Service Catalog bietet eine Schnittstelle für die Verwaltung von bereitgestellten Produkten. Sie können alle bereitgestellten Produkte für Ihren Katalog basierend auf der Zugriffsebene anzeigen, aktualisieren und beenden. Beispiele zur Vorgehensweise finden Sie in den folgenden Abschnitten.

Themen

- Verwalten von bereitgestellten Produkten als Administrator
- Ändern des Besitzers des bereitgestellten Produkts
- Aktualisieren von Vorlagen für bereitgestellte Produkte
- Tutorial: Identifizieren der Benutzerressourcenzuordnung
- Verwalten von Terraform-Open-Source-Produktstatusfehlern
- Verwalten der Terraform-Open-Source-Produktstatusdatei

Verwalten von bereitgestellten Produkten als Administrator

Um alle bereitgestellten Produkte für ein Konto zu verwalten, benötigen Sie `AWSServiceCatalogAdminFullAccess` oder eine entsprechende IAM-Berechtigung für den Zugriff auf Schreibvorgänge für bereitgestellte Produkte. Weitere Informationen finden Sie unter Identity and Access Management in AWS Service Catalog.

> **Tip**
>
> Für die statische Verkettung bereitgestellter Produkte müssen Sie in einer Product-Artifact-Vorlage auf Outputs bereitgestellter Produkte verweisen, bevor das bereitgestellte Produkt bereitgestellt wird. Weitere Informationen, einschließlich eines Beispiels, finden Sie im Folgenden:
>
> - AWS::ServiceCatalog::CloudFormationProvisionedProduct im AWS CloudFormation-Benutzerhandbuch.
> - DescribeProvisioningParameters (ProvisioningArtifactOutputKeys) im AWS Service Catalog Entwicklerhandbuch für .

So zeigen Sie alle bereitgestellten Produkte an und verwalten sie

1. Öffnen Sie die -AWS Service CatalogKonsole unter https://console.aws.amazon.com/servicecatalog/.

   Wenn Sie bereits bei der AWS Service Catalog Konsole angemeldet sind, wählen Sie Service Catalog und dann Endbenutzer aus.
2. Scrollen Sie bei Bedarf nach unten zum Abschnitt Bereitgestellte Produkte.
3. Wählen Sie im Abschnitt Bereitgestellte Produkte die Liste Anzeigen: und wählen Sie die gewünschte Zugriffsebene aus: Benutzer , Rolle oder Konto . Diese Aktion zeigt alle bereitgestellten Produkte im Katalog an.
4. Wählen Sie ein bereitgestelltes Produkt zum Anzeigen, Aktualisieren oder Beenden aus. Weitere Informationen zu den Daten in dieser Ansicht finden Sie unter Anzeigen von bereitgestellten Produktinformationen.

Ändern des Besitzers des bereitgestellten Produkts

Sie können den Besitzer eines bereitgestellten Produkts jederzeit ändern. Sie müssen den ARN des Benutzers oder der Rolle kennen, den bzw. die Sie als neuen Besitzer festlegen möchten.

Standardmäßig ist diese Funktion für Administratoren verfügbar, die die -`AWSServiceCatalogAdminFullAccess`verwaltete Richtlinie verwenden. Sie können es für Endbenutzer aktivieren, indem Sie ihnen die `-servicecatalog:UpdateProvisionedProductProperties`Berechtigung in AWS Identity and Access Management (IAM) erteilen.

So ändern Sie den Besitzer eines bereitgestellten Produkts

1. Wählen Sie in der AWS Service Catalog-Konsole die Liste der bereitgestellten Produkte aus.
2. Suchen Sie das bereitgestellte Produkt, das Sie aktualisieren möchten, wählen Sie dann die drei Punkte daneben und wählen Sie Bereitgestellten Produktbesitzer ändern. Sie finden die Option Change owner (Besitzer ändern) auch auf der Detailseite des bereitgestellten Produkts im Menü Aktionen .
3. Geben Sie im Dialogfeld den ARN des Benutzers oder der Rolle ein, den bzw. die Sie als neuen Besitzer festlegen möchten. Ein ARN beginnt mit `arn:` und enthält weitere Informationen, die durch Doppelpunkte oder Schrägstriche getrennt sind, z. B. `arn:aws:iam::123456789012:user/NewOwner`.

4. Wählen Sie Absenden aus. Sie erhalten eine Erfolgsmeldung, wenn der Besitzer aktualisiert wurde.

Weitere Informationen finden Sie unter:

- UpdateProvisionedProductProperties

Aktualisieren von Vorlagen für bereitgestellte Produkte

Sie können die aktuelle Vorlage eines bereitgestellten Produkts in eine andere Vorlage ändern. Wenn Sie beispielsweise ein EC2-Produkt im Service Catalog haben, können Sie dieses EC2-Produkt aktualisieren, um dieselbe bereitgestellte Produkt-ID beizubehalten, aber die Vorlage in einen S3-Bucket zu ändern.

> **Note**
>
> Das Aktualisieren von Vorlagen wird für bereitgestellte Produkte von Terraform Open Source oder Terraform Cloud nicht unterstützt. Wenn Sie eine andere Vorlage für ein vorhandenes Terraform-Produkt verwenden möchten, müssen Sie das Produkt löschen und dann mithilfe der gewünschten Vorlage ein neues Produkt erstellen.

So aktualisieren Sie eine Vorlage für ein bereitgestelltes Produkt

1. Wählen Sie im linken Navigationsmenü Bereitgestellte Produkte aus.
2. Wählen Sie unter Bereitgestellte Produkte ein bereitgestelltes Produkt und dann Aktionen , Aktualisieren aus.

   Beachten Sie, dass Sie auch Aktionen , Aktualisieren auf der Seite Bereitgestellte Produktdetails auswählen können.
3. (Optional) Wählen Sie unter Produktdetails die Option Produkt ändern aus.

   Beachten Sie unter Produkt ändern diese Warnung:

   Wenn Sie das Produkt ändern, wird dieses bereitgestellte Produkt auf eine andere Produktvorlage aktualisiert. Dadurch können Ressourcen beendet und neue erstellt werden.

Sie können ein bereitgestelltes Produkt auf eine andere Version innerhalb desselben Produkts aktualisieren.

4. (Optional) Wählen Sie unter Produkte das Produkt aus, das Sie mit einer anderen Vorlage aktualisieren möchten. Wählen Sie dann Ändern aus.

   Beachten Sie unter Produktdetails diese Warnung:

   [Produktname] wird von [aktueller Vorlagenname] auf [neuer Vorlagenname] aktualisiert. Der Name Ihres bereitgestellten Produkts, [Name des bereitgestellten Produkts], ändert sich jedoch nicht.

   Sie können ein bereitgestelltes Produkt auf eine andere Version innerhalb desselben Produkts aktualisieren.
5. Wählen Sie unter Produktversionen die gewünschte Version des Produkts aus.
6. Wählen Sie unter Parameter die entsprechenden Parameter aus.
7. Wählen Sie Aktualisieren.

   In Bereitgestellte Produktdetails sehen Sie die Details des Updates. Der Name des bereitgestellten Produkts ändert sich nicht, aber das bereitgestellte Produkt hat jetzt eine andere Vorlage.

Tutorial: Identifizieren der Benutzerressourcenzuordnung

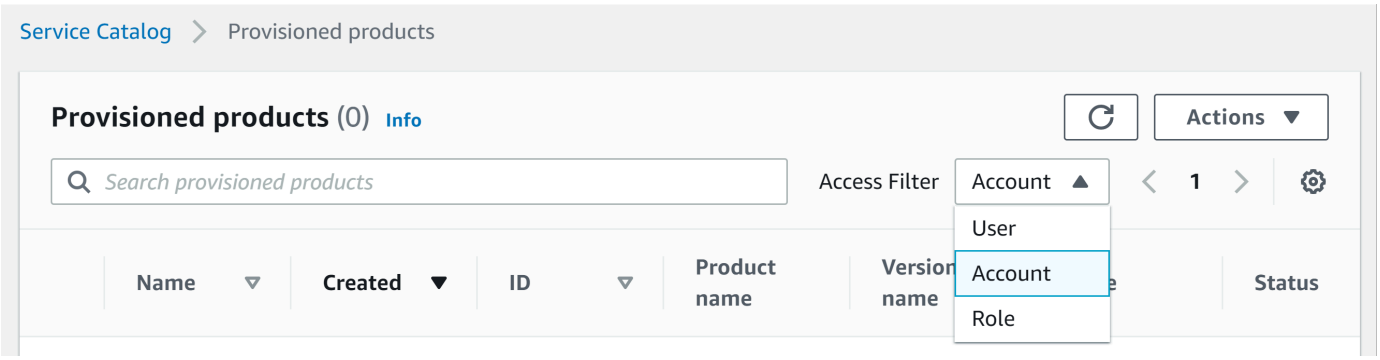
Sie können den Benutzer identifizieren, der ein Produkt und die damit verbundenen Ressourcen bereitgestellt hat. Verwenden Sie dazu die AWS Service Catalog-Konsole. In diesem Tutorial lernen Sie, wie Sie dieses Beispiel auf Ihre spezifischen bereitgestellten Produkte übertragen.

Um alle bereitgestellten Produkte für das Konto zu verwalten, benötigen Sie `AWSServiceCatalogAdminFullAccess`- oder entsprechenden Zugriff auf die Schreibvorgänge des bereitgestellten Produkts. Weitere Informationen finden Sie unter Identity and Access Management im -AWS Service CatalogAdministratorhandbuch.

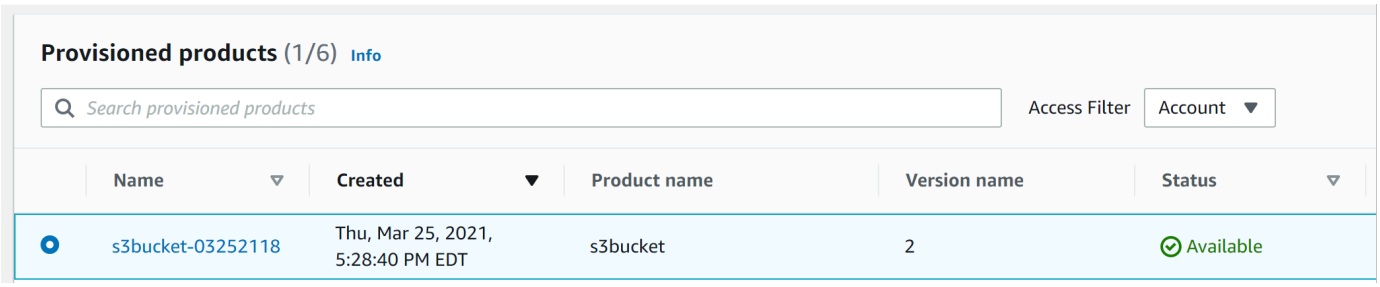
So identifizieren Sie den Benutzer, der ein Produkt und die damit verbundenen Ressourcen bereitgestellt hat

1. Öffnen Sie https://console.aws.amazon.com/servicecatalog.
2. Wählen Sie im linken Navigationsmenü Bereitgestelltes Produkt aus.

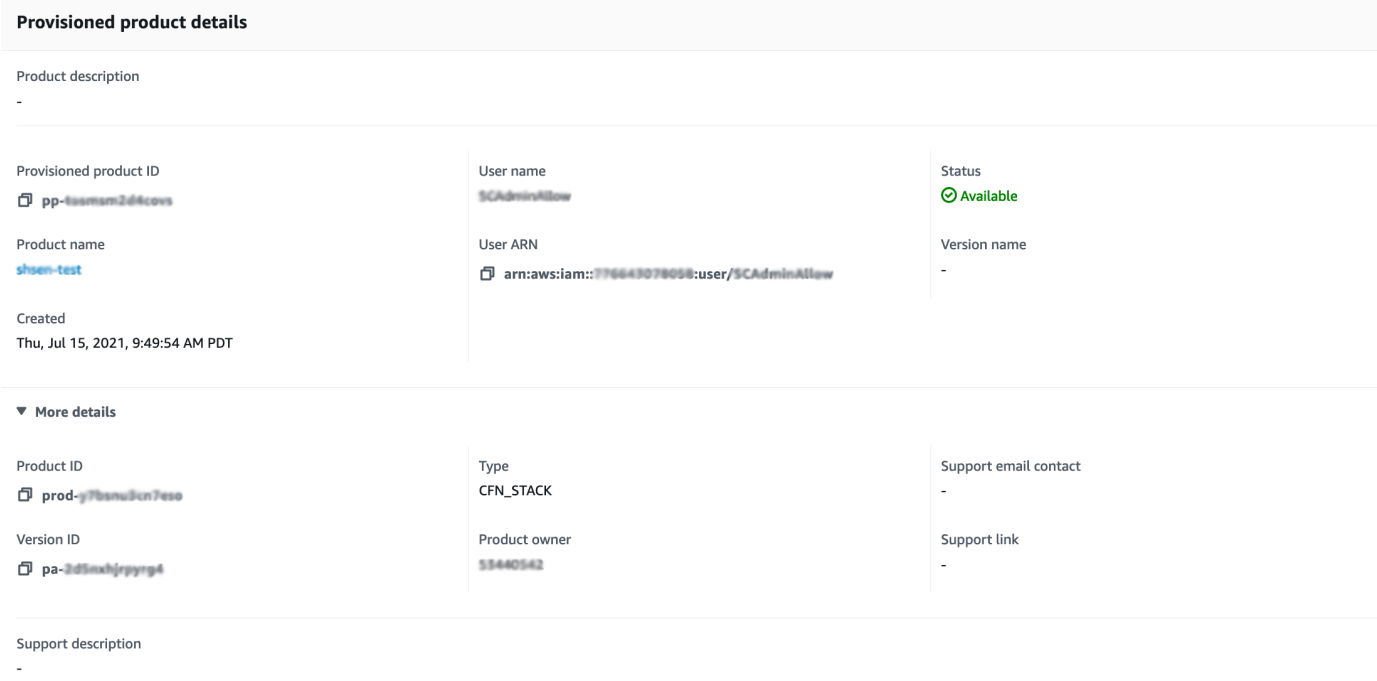
3. Wählen Sie im Dropdown-Menü Zugriffsfilter die Option Konto aus.



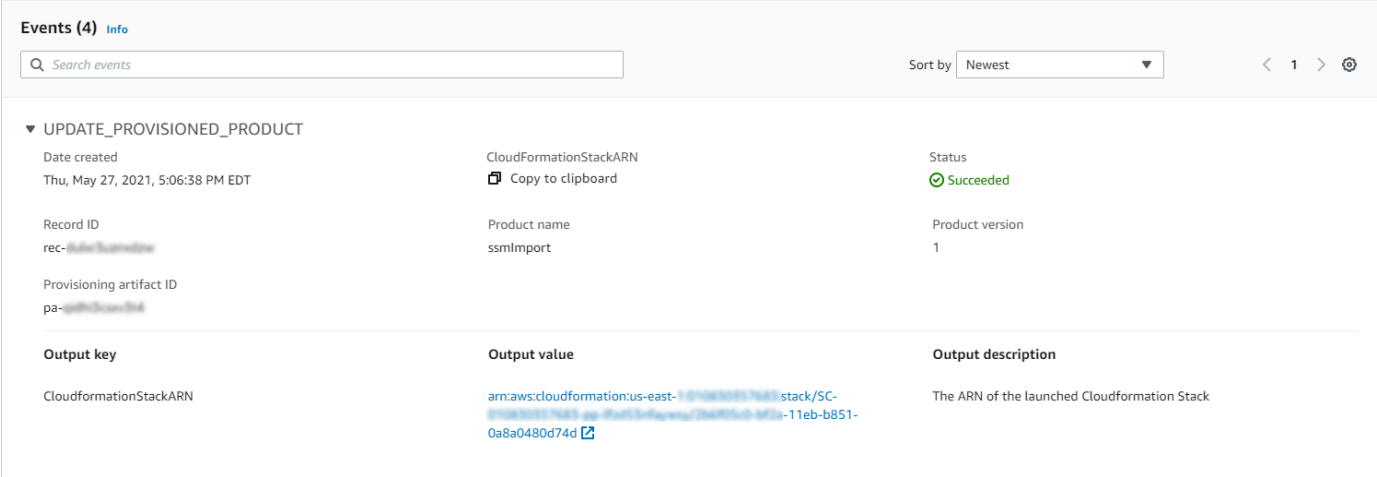
4. Wählen Sie in der Kontoansicht ein bereitgestelltes Produkt aus und öffnen Sie es, um dessen Details anzuzeigen.



Sie können die Details des bereitgestellten Produkts anzeigen.



5. Scrollen Sie nach unten, um den Abschnitt Ereignisse zu erweitern. Notieren Sie sich die `CloudformationStack`ARN Werte `Provisioned product ID` und .



6. Verwenden Sie die bereitgestellte Produkt-ID, um den AWS CloudTrail Datensatz zu identifizieren, der diesem Start entspricht, und identifizieren Sie den anfordernden Benutzer (in der Regel geben Sie während des Verbunds eine E-Mail-Adresse ein). In unserem Beispiel lautet diese "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. Verwenden Sie den `CloudformationStackARN` Wert , um AWS CloudFormation Ereignisse zu identifizieren, um Informationen zu den erstellten Ressourcen zu finden. Sie können diese

Informationen auch über die AWS CloudFormation-API abrufen. Weitere Informationen finden Sie unter AWS CloudFormation-API-Referenz.

Sie können die Schritte 1 bis 4 mit der AWS Service Catalog-API oder der ausführenAWS CLI. Weitere Informationen finden Sie im -AWS Service CatalogEntwicklerhandbuch. und in der -AWS Service CatalogBefehlszeilenreferenz.

Verwalten von Terraform-Open-Source-Produktstatusfehlern

Terraform-Open-Source-`ProvisionProduct`Fehler werden in den `TAINTED` Status weitergeleitet, sodass jedes bereitgestellte Produkt mit fortfahren kann`UpdateProvisionedProduct`. Wenn dies der Fall ist:

- `UpdateProvisionedProduct` versucht nicht, Tags zu aktualisieren oder zu korrigieren oder eine Ressourcengruppe zu erstellen oder zu ändern.
- `UpdateProvisionedProduct` berücksichtigt bei der Entscheidung, ob das bereitgestellte Produkt auf `AVAILABLE` oder festgelegt werden soll, keine Fehler aus früheren Bereitstellungsvorgängen`TAINTED`.

AWS Service Catalog wendet nur Tags während an`ProvisionProduct`. Alle fehlgeschlagenen Markierungen, die auf einen Fehler des `ProvisionProduct` Vorgangs zurückzuführen sind, werden nicht automatisch behoben.

Beispiele für Statusfehler

Beispiel 1: erstellt AWS Service Catalog keine Ressourcengruppe während `ProvisionProduct`

Im folgenden Szenario haben Sie ein bereitgestelltes Produkt im `AVAILABLE` Status , auch wenn es keine unterstützende Ressourcengruppe gibt und keine Tags auf die Ressourcen angewendet werden.

1. Ihre Aktion initiiert `ProvisionProduct`.
2. Die Terraform-Bereitstellungs-Engine reagiert auf `ProvisionProduct` mit einem Workflow-Fehler und stellt keine bereit`ResourceIdentifier`.
3. Der `ProvisionProduct` Workflow erstellt keine Ressourcengruppe und legt dann den Status des bereitgestellten Produkts auf fest`ERROR`.
4. Anschließend starten Sie den `Updateprovisionedproduct` Vorgang.

5. Die Terraform-Bereitstellungs-Engine reagiert auf „Erfolg“.
6. Daher setzt der `UpdateprovisionedProduct` Workflow den Status des bereitgestellten Produkts auf `AVAILABLE`, erstellt aber keine Ressourcengruppe und versucht auch nicht, Tags anzuwenden.

Beispiel 2: AWS Service Catalog erstellt neue Ressourcen während `UpdateProvisionedProduct`

Im folgenden Szenario haben Sie ein bereitgestelltes Produkt im `AVAILABLE` Status , auch wenn neue Ressourcen keine Tags angewendet haben.

1. Ihre Aktion initiiert `ProvisionProduct`.
2. Die Terraform-Bereitstellungs-Engine reagiert auf „Erfolg“ und stellt eine bereit`ResourceIdentifier`.
3. Der `ProvisionProduct` Workflow erstellt eine Ressourcengruppe und wendet Tags auf alle identifizierten Ressourcen an.
4. Sie initiieren `UpdateProvisionedProduct` für ein neues Artefakt, das neue Ressourcen erstellt.
5. Die Terraform-Bereitstellungs-Engine reagiert auf „Erfolg“.
6. Der `UpdateProvisionedProduct` Workflow setzt den Status des bereitgestellten Produkts auf , versucht `AVAILABLE` jedoch nicht, zusätzliche Tags auf die neuen Ressourcen anzuwenden.

Statusfehlerlösung

AWS Service Catalog stellt sicher, dass eine Ressourcengruppe für alle bereitgestellten Produkte erstellt wird, die auf `TAINTED` von festgelegt sind`ProvisionProduct`. Wenn die Terraform-Bereitstellungs-Engine kein zurückgibt `ResourceIdentifier`oder keine Ressourcengruppe erstellen AWS Service Catalog kann, wird das bereitgestellte Produkt auf den `ERR0R` Status gesetzt, sodass Sie es beenden müssen.

Verwalten der Terraform-Open-Source-Produktstatusdatei

Jedes von Terraform Open Source bereitgestellte Produkt verfügt über eine Datei mit einem einzigen Zustand. Es besteht eine 1:1-Beziehung zwischen dem bereitgestellten Produkt und seiner Zustandsdatei. Die Dateien werden in einem Amazon S3-Bucket mit dem Namen gespeichert`sc-`

`terraform-engine-state-${AWS::AccountId}-${AWS::Region}`. Die Statusdatei wird unter dem `ProvisionedProductID` Objektschlüssel `AccountID` oder gespeichert.

Der Zugriff auf Statusdateien ist auf die Startvorlagen `GetStateFile` AWS Lambda und Amazon EC2 beschränkt. -AWS Service CatalogAdministratoren haben keinen direkten Zugriff auf die Statusdateien in Amazon S3. Administratoren müssen mit Amazon EC2 auf die Dateien zugreifen. Standardmäßig können AWS Service Catalog Administratoren die Liste der Statusdateien sehen, aber den Dateiinhalt nicht lesen oder schreiben. Nur die Terraform-Bereitstellungs-Engine kann den Dateiinhalt lesen oder schreiben.

Verwalten von Tags in AWS Service Catalog

AWS Service Catalog stellt Tags bereit, damit Sie Ihre Ressourcen kategorisieren können. Es gibt zwei Arten von Tags: AutoTags und TagOptions.

AutoTags sind Tags, die Informationen über den Ursprung einer bereitgestellten Ressource in identifizieren AWS Service Catalog und automatisch von AWS Service Catalog auf bereitgestellte Ressourcen angewendet werden.

TagOptions sind Schlüssel-Wert-PaareAWS Service Catalog, die in verwaltet werden und als Vorlagen für die Erstellung AWS von Tags dienen.

Themen

- AWS Service Catalog AutoTags
- AWS Service Catalog TagOption Bibliothek

AWS Service Catalog AutoTags

> **Note**
>
> AWS Service Catalog unterstützt nicht AutoTags für Terraform-Open-Source-Produkte.

AutoTags sind Tags, die Informationen über den Ursprung einer bereitgestellten Ressource in identifizieren AWS Service Catalog und automatisch von AWS Service Catalog auf bereitgestellte Ressourcen angewendet werden.

AutoTags enthalten Tags für die eindeutigen Kennungen für Portfolio, Produkt, Benutzer, Produktversion und bereitgestelltes Produkt. Dadurch wird eine Reihe von Tags bereitgestellt, die die AWS Service Catalog-Struktur widerspiegeln, die Kunden im Katalog konfiguriert haben. AutoTags wird nicht auf das 50-Tag-Limit des Kunden angerechnet.

> **Note**
>
> AWS Service Catalog unterstützt nicht AutoTags für Terraform-Open-Source-Produkte.

AWS Service Catalog AutoTags kann dazu beitragen, eine konsistente Markierung für Ihre Ressourcen bereitzustellen, was bei der Festlegung von Budgets für ein Portfolio, ein Produkt oder einen Benutzer nützlich ist. Sie können auch die verwenden AutoTags , um Ressourcen für Vorgänge nach dem Start zu identifizieren, z. B. das Festlegen von AWS Config Regeln. AutoTags Für Ihre bereitgestellten Ressourcen können Sie im Abschnitt Tags der nachgelagerten Services, die für die Bereitstellung verwendet werden, wie AWS CloudFormation, Amazon EC2 und Amazon S3, einsehen.

> **Note**
>
> AWS Service Catalog aktualisiert nicht, AutoTags nachdem Sie AutoTags sich auf bereitgestellte Ressourcen angewendet haben. Wenn Sie das bereitgestellte Produkt auf ein anderes Produkt, ein anderes bereitgestelltes Artefakt oder einen neuen Startpfad aktualisieren, zeigen die vorhandenen AutoTags immer noch die ursprünglichen Werte an.

AutoTag Details

- aws:servicecatalog:portfolioArn – Der ARN des Portfolios, aus dem das bereitgestellte Produkt gestartet wurde
- aws:servicecatalog:productArn – Der ARN des Produkts, aus dem das bereitgestellte Produkt gestartet wurde
- aws:servicecatalog:provisioningPrincipalArn – Der ARN des Bereitstellungsprinzipals (Benutzers), der das bereitgestellte Produkt erstellt hat.
- aws:servicecatalog:provisionedProductArn – Der bereitgestellte Produkt-ARN.
- aws:servicecatalog:provisioningArtifactIdentifier - Die ID des ursprünglichen Bereitstellungsartefakts (Produktversion).

AWS Service Catalog TagOption Bibliothek

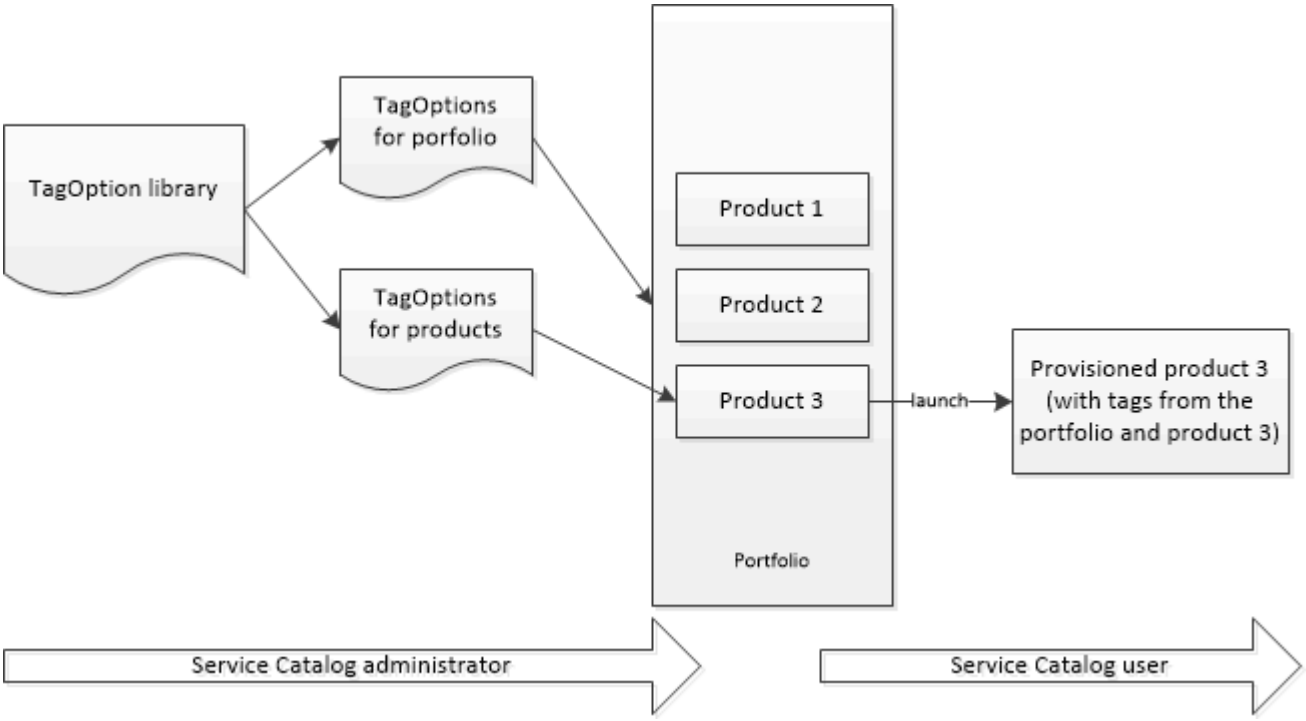
Damit Administratoren Tags für bereitgestellte Produkte einfach verwalten können, AWS Service Catalog stellt eine TagOption Bibliothek bereit. Ein TagOption ist ein Schlüssel-Wert-Paar, das in verwaltet wirdAWS Service Catalog. Es handelt sich nicht um ein -AWSTag, sondern dient als Vorlage zum Erstellen eines -AWSTags basierend auf dem TagOption.

AWS Service Catalog unterstützt nicht TagOptions für Terraform Open Source- oder Terraform Cloud-Produkte.

Die TagOption Bibliothek erleichtert das Erzwingen von Folgendem:

- Eine einheitliche Taxonomie
- Ein ordnungsgemäßes Markieren von AWS Service Catalog-Ressourcen
- Definierte, vom Benutzer auswählbare Optionen für die zulässigen Tags

Administratoren können Portfolios und Produkten TagOptions zuordnen. Während eines Produktstarts (Bereitstellung) AWS Service Catalog aggregiert das zugehörige Portfolio und das Produkt TagOptionsund wendet sie auf das bereitgestellte Produkt an, wie im folgenden Diagramm gezeigt.



Mit der TagOption Bibliothek können Sie ihre Zuordnungen zu Portfolios oder Produkten deaktivieren TagOptions und beibehalten und sie bei Bedarf reaktivieren. Dieser Ansatz trägt nicht nur zur Wahrung der Bibliotheksintegrität bei, sondern ermöglicht Ihnen auch, , TagOptions die möglicherweise zeitweise oder nur unter besonderen Umständen verwendet werden.

Sie verwalten TagOptions mit der AWS Service Catalog Konsole oder der TagOption Bibliotheks-API. Weitere Informationen finden Sie unter Service-Catalog-API-Referenz.

Inhalt

- Starten eines Produkts mit TagOptions
- Verwalten von TagOptions

- Verwenden von TagOptions mit AWS Organizations Tag-Richtlinien

Starten eines Produkts mit TagOptions

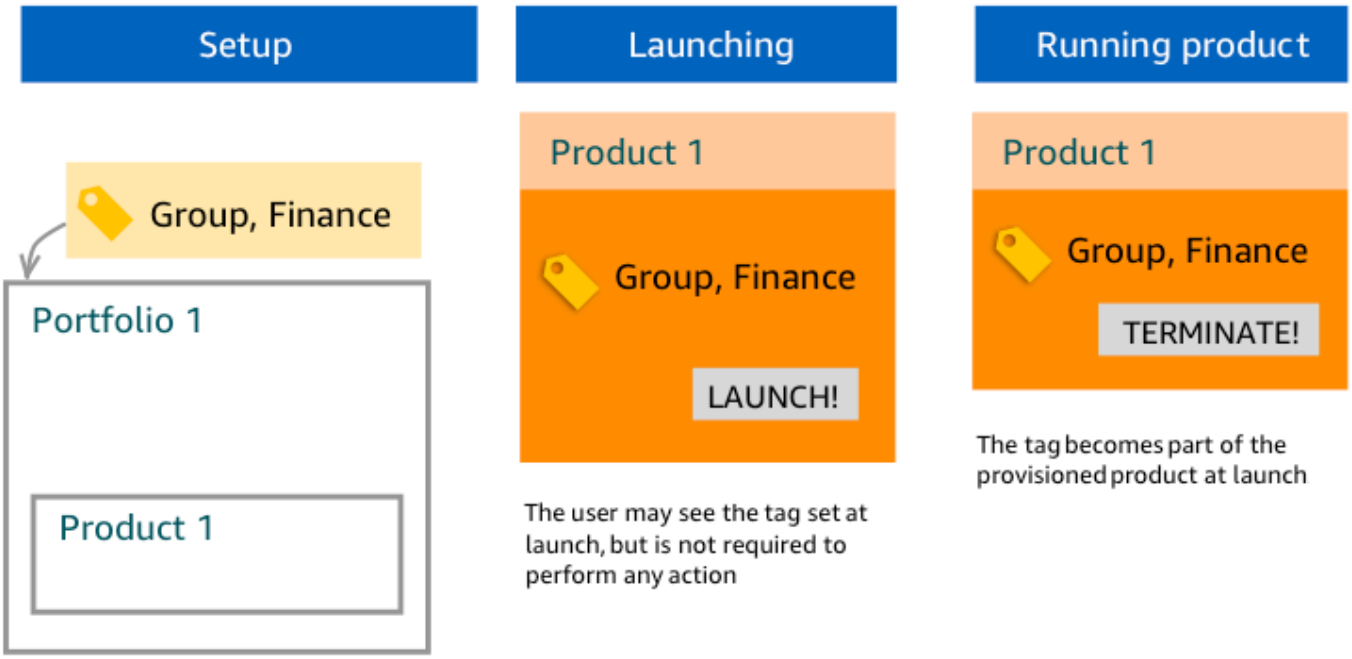
Wenn ein Benutzer ein Produkt startet, das hat TagOptions, AWS Service Catalog führt die folgenden Aktionen in Ihrem Namen durch:

- Sammelt alle TagOptions für das Produkt und das Launching-Portfolio.
- Stellt sicher, dass nur TagOptions mit eindeutigen Schlüsseln in einem Tag auf dem bereitgestellten Produkt verwendet werden. Benutzer erhalten Listen zur Auswahl mehrerer Werte für einen Schlüssel. Nachdem der Benutzer einen Wert ausgewählt hat, wird dieser als Tag in dem bereitgestellten Produkt verwendet.
- Ermöglicht Benutzern, dem Produkt während der Bereitstellung nicht in Konflikt stehende Tags hinzuzufügen.

Die folgenden Anwendungsfälle zeigen, wie beim Start TagOptions funktioniert.

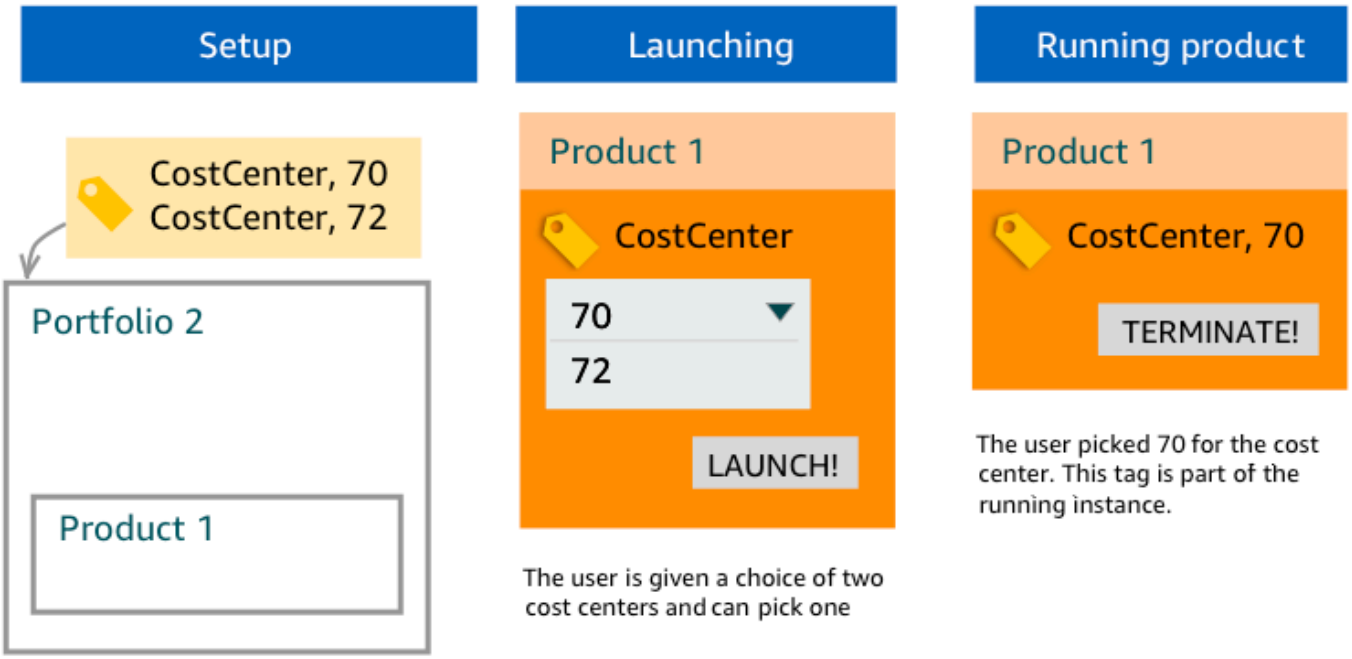
Beispiel 1: Ein eindeutiger TagOption Schlüssel

Ein Administrator erstellt TagOption[Group=Finance] und ordnet es Portfolio1 zu, das Product1 ohne enthält TagOptions. Wenn ein Benutzer das bereitgestellte Produkt startet, TagOption wird das einzelne wie folgt zu Tag[Group=Finance]:



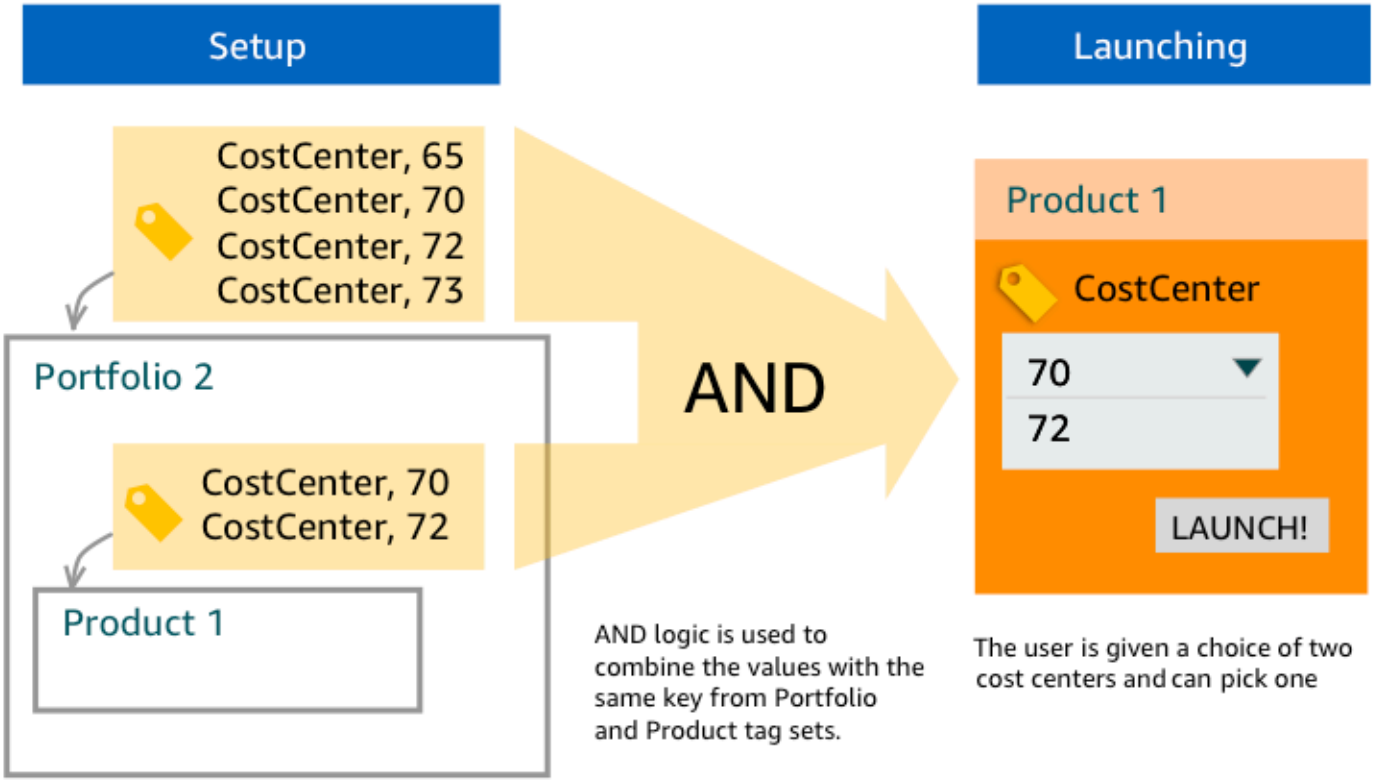
Beispiel 2: Ein Satz von TagOptions mit demselben Schlüssel für ein Portfolio

Ein Administrator hat zwei TagOptions mit demselben Schlüssel in einem Portfolio platziert, und es gibt keine TagOptions mit demselben Schlüssel für Produkte innerhalb dieses Portfolios. Während des Starts muss der Benutzer einen der beiden Werte auswählen, die dem Schlüssel zugeordnet sind. Das bereitgestellte Produkt wird dann mit dem Schlüssel und dem vom Benutzer ausgewählten Wert markiert.



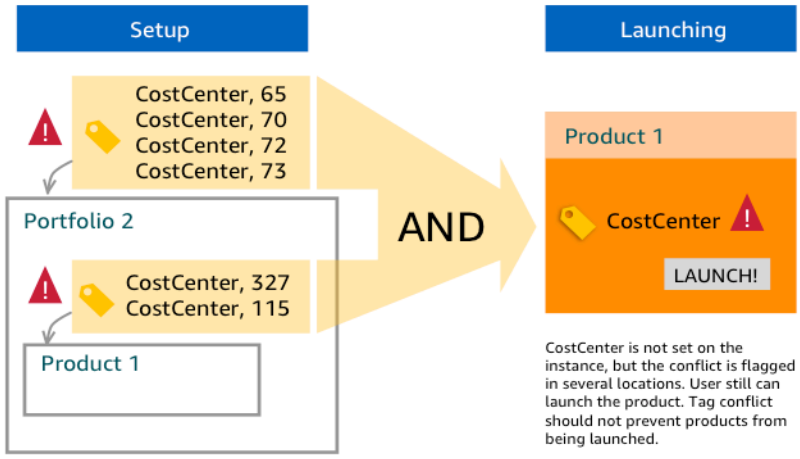
Beispiel 3: Ein Satz von TagOptions mit demselben Schlüssel sowohl für das Portfolio als auch für ein Produkt in diesem Portfolio

Ein Administrator hat mehrere TagOptions mit demselben Schlüssel in einem Portfolio platziert, und es gibt auch mehrere TagOptions mit demselben Schlüssel für das Produkt innerhalb dieses Portfolios. AWS Service Catalog erstellt einen Satz von Werten aus der Aggregation (logische AND-Operation) des TagOptions. Wenn der Benutzer das Produkt startet, sieht er diesen Satz von Werten und wählt einen Wert aus. Das bereitgestellte Produkt wird mit dem Schlüssel und dem vom Benutzer ausgewählten Wert markiert.



Beispiel 4: Mehrere TagOptions mit demselben Schlüssel und widersprüchlichen Werten

Ein Administrator hat mehrere TagOptions mit demselben Schlüssel in einem Portfolio platziert, und es gibt auch mehrere TagOptions mit demselben Schlüssel für das Produkt in diesem Portfolio. AWS Service Catalog erstellt einen Satz von Werten aus der Aggregation (logische AND-Operation) des TagOptions. Wenn die Aggregation keine Werte für diesen Schlüssel findet, erstellt AWS Service Catalog ein Tag mit demselben Schlüssel und dem Wert `sc-tagconflict-`*`portfolioid`*`-`*`productid`*, wobei *`portfolioid`* und *`productid`* die ARNs des Portfolios und des Produkts sind. Auf diese Weise wird sichergestellt, dass das bereitgestellte Produkt mit dem richtigen Schlüssel und mit einem Wert markiert wird, den der Administrator finden und korrigieren kann.



Verwalten von TagOptions

Als Administrator können Sie die folgenden Aktionen ausführen, um TagOptions in der TagOptions Bibliothek zu verwalten:

- Erstellen und Löschen
- Aktivieren oder Deaktivieren von
- Zuordnen oder Aufheben der Zuordnung
- Edit (Bearbeiten)

So erstellen Sie TagOptions in der Konsole

1. Öffnen Sie die Service-Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie im linken Navigationsmenü TagOptions Bibliothek aus.
3. Geben Sie unter Neu erstellen TagOption einen Schlüssel und einen Wert ein und wählen Sie dann Hinzufügen aus.

   Nachdem das neue erstellt TagOption wurde, wird es nach Schlüssel-Wert-Paaren gruppiert und alphabetisch in der TagOptions Liste sortiert.

   Informationen zum Erstellen eines TagOption mithilfe der AWS Service Catalog API finden Sie unter CreateTagOption.

So löschen Sie TagOptions in der Konsole

1. Öffnen Sie die Service-Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie im linken Navigationsmenü TagOptions Bibliothek und dann Aktionen aus.
3. Wählen Sie Löschen und bestätigen Sie den Löschvorgang.

So aktivieren oder deaktivieren Sie eine oder mehrere TagOptions in der Konsole

1. Öffnen Sie die Service-Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie im linken Navigationsmenü TagOptions Bibliothek und dann Aktionen aus.
3. Wählen Sie zum Aktivieren die gewünschte Inaktivität aus TagOption . Wählen Sie dann Aktionen und dann Aktivieren aus dem Dropdown-Menü aus und bestätigen Sie Ihre Auswahl.

   Wählen Sie zum Deaktivieren die TagOption gewünschte aktive aus. Wählen Sie dann Aktionen und dann Deaktivieren aus dem Dropdown-Menü aus und bestätigen Sie Ihre Auswahl.

So ordnen Sie einem Portfolio in der Konsole ein oder mehrere Portfolios TagOptions zu oder trennen sie

1. Öffnen Sie die Service-Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie im linken Navigationsmenü Portfolios aus und öffnen Sie dann das Portfolio, das Sie zuordnen oder die Zuordnung aufheben möchten.
3. Wählen Sie die TagOptions Registerkarte und eine oder mehrere aus TagOptions , die dem Portfolio zugeordnet oder getrennt werden sollen.
4. Wählen Sie Aktionen. Wählen Sie dann Zuordnen oder Zuordnung aufheben und bestätigen Sie Ihre Auswahl.

So verknüpfen Sie ein oder mehrere TagOptions mit einem Produkt in der Konsole oder heben die Zuordnung auf

1. Öffnen Sie die -AWS Service CatalogKonsole unter: https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie im linken Navigationsmenü unter Administration die Option Produkte aus. Öffnen Sie dann das Produkt, das Sie zuordnen oder die Zuordnung aufheben möchten.

3. Wählen Sie die TagOptions Registerkarte und eine oder mehrere aus TagOptions , die dem Portfolio zugeordnet oder getrennt werden sollen.
4. Wählen Sie Aktionen. Wählen Sie dann Zuordnen oder Zuordnung aufheben und bestätigen Sie Ihre Auswahl.

> **Note**
>
> Informationen zum Zuordnen TagOptions zu einem Portfolio oder Produkt mithilfe der AWS Service Catalog API finden Sie unter AssociateTagOptionWithResource.
> Informationen zum Entfernen (Trennen der Zuordnung) TagOptions mithilfe der AWS Service Catalog-API finden Sie unter DisassociateTagOptionFromResource.

So bearbeiten Sie Werte für TagOptions in der Konsole

1. Öffnen Sie die Service-Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie im linken Navigationsmenü TagOptions Bibliothek aus.
3. Wählen Sie einen aus TagOption und öffnen Sie den Wert. (Der Wert ist mit einem Hyperlink versehen.) Wählen Sie dann Bearbeiten aus.
4. Bearbeiten Sie im Feld Wert den Wert und wählen Sie Änderungen speichern aus.

Verwenden von TagOptions mit AWS Organizations Tag-Richtlinien

Dieses Thema bietet einen kurzen Überblick über Tag-Richtlinien für AWS Organizations und TagOptions für AWS Service Catalog. Es schlägt auch vor, wie Tagging-Konflikte verhindert werden können, wenn beide Funktionen gleichzeitig verwendet werden.

TagOptions für AWS Service Catalog gilt für bereitgestellte Produkte (CloudFormationStacks), während Tag-Richtlinien für für AWS Konten und Organisationseinheiten (OU) oder einen Organisationsstamm AWS Organizations gelten. Wenn Sie beispielsweise eine Tag-Richtlinie an eine Organisationseinheit anfügen, gilt dieselbe Tag-Richtlinie für alle Konten in dieser Organisationseinheit. Wenn Sie beide Tagging-Funktionen gleichzeitig verwenden, sollten Sie sie so konfigurieren, dass sie nicht in Konflikt geraten.

Tag-Richtlinien

Mit Tag-Richtlinien können Sie Regeln für die Verwendung von Tags für AWS Ressourcen in Ihren Konten in definierenAWS Organizations. Sie können Tag-Richtlinien verwenden, um einen konsistenten Ansatz für das Markieren von AWS Ressourcen auf Kontoebene zu erstellen und aufrechtzuerhalten.

Tag-Richtlinien bieten eine einfache Möglichkeit, um sicherzustellen, dass Benutzer konsistente Tags anwenden, markierte Ressourcen prüfen und eine ordnungsgemäße Ressourcenkategorisierung aufrechterhalten. Sie können auch definieren, wie Tag-Schlüssel in Großbuchstaben geschrieben werden sollen und welche Werte Sie zulassen möchten. Sie können beispielsweise verlangen, dass für alle EC2-Instances in einem Konto ein Tag-Schlüssel als **`CostCenter`** und Werte als festgelegt werden muss, damit dieses Tag **`Data Insights`** oder ist**`Marketing`**.

Mit Tag-Richtlinien können Sie Optionen auswählen, um Tagging-Regeln zu erzwingen, nicht konforme Operationen für Tags zu verhindern und die Ressourcentypen anzugeben, für die die Durchsetzung gilt. Wenn Sie keine Durchsetzungsoption wählen, können Sie mit Tag-Richtlinien die nicht konformen Tags erstellen oder mutieren, melden sie jedoch in der AWS Organizations Konsole als nicht konform.

Weitere Informationen zum Einrichten der Tagging-Erzwingung auf Kontoebene finden Sie unter Tag-Richtlinien in AWS Organizations.

TagOptions

TagOptions sind eine Markierungsfunktion, die für bereitgestellte Produkte auf CloudFormation Stack-Ebene AWS Service Catalog gilt, wenn sie auf ein zugeordnetes Produkt angewendet werden. AWS Service Catalog bietet eine TagOptions Bibliothek, in der Sie die Schlüssel-Wert-Paare definieren können, die Sie Ihren AWS Service Catalog Produkten zuordnen möchten. Wenn Sie ein AWS Service Catalog Produkt starten, müssen Sie TagOption Werte für die vorhandenen TagOption Schlüssel auswählen, die diesem Portfolio oder Produkt zugeordnet sind, um dieses Produkt zu starten. Da Sie TagOptions auf Portfolio- oder Produktebene festlegen, können Sie eine konsistente Taxonxie für das Markieren mit Portfolios erzwingen, die über Konten und Regionen hinweg gemeinsam genutzt werden.

Weitere Informationen zur Einrichtung TagOptions von in finden Sie AWS Service Catalogunter Bibliothek AWS Service Catalog TagOption .

Vermeiden von Konflikten zwischen AWS Organizations Tag-Richtlinien und AWS Service Catalog TagOptions

Wenn Sie AWS Organizations Tag-Richtlinien für Konten in Ihrer Organisation konfigurieren, empfehlen wir Folgendes:

- Teilen Sie die Anforderungen für konforme Tags mit Administratoren, die auch für AWS Service Catalog Portfolios und Produkte verwalten TagOptions.
- Teilen Sie die Anforderungen für konforme Tags mit Endbenutzern, die Produkte in starten AWS Service Catalog und ihren Produktstarts optionale Endbenutzer-Tags anfügen können.

Angenommen, Sie möchten ein Produkt in startenAWS Service Catalog, das den TagOption Schlüssel verwendet`city`, und Sie haben eine Tag-Richtlinie, die erfordert, dass Tag-Schlüssel mit Tag-Werte von US-Städten `city` haben, z. B. **`Atlanta`**, oder **`Austin`**. erlaubt AWS Service Catalog es Ihnen nicht, ein Produkt zu starten**`San Francisco`**, ohne TagOption Werte für die erforderlichen TagOption Schlüssel für ein Produkt ausgewählt zu haben.

Wenn Sie in diesem Fall TagOption Werte für den TagOption Schlüssel haben, `city` die Südamerika-Städten enthalten, wie z. B. **`Rio de Janeiro`** oder **`Buenos Aires`**, AWS Service Catalog wird das Produkt nicht starten. Stattdessen müssen Sie beim Start einen TagOption Wert auswählen, der eine US-Stadt enthält, um die Tag-Richtlinie zu erfüllen.

Die folgende Tabelle enthält Szenarien, in denen beschrieben wird, wie Sie die Probleme bei der Markierung von Konflikten beheben können, die bei der Verwendung von Tag-Richtlinien und TagOptions gleichzeitig auftreten können.

Szenario	Grund	Lösung
Das Produkt kann aufgrund nicht konformer Tags nicht gestartet werden, wenn die Tag-Erzwingung in der Tag-Richtlinie überprüft ist.	Angabe TagOptions mit Schlüsseln und Werten, die Sie nicht zur zulässigen Liste der konformen Tags in Ihrer Tag-Richtlinie hinzugefügt haben. Hinzufügen optionaler benutzerdefinierter Tags,	Wenn Sie ein bestimmtes Groß-/Kleinschreibungsschema in der Durchsetzung von Tag-Schlüsseln konfigurieren, stellen Sie sicher, dass Ihre TagOptions Tag-Schlüssel und optionalen benutzerdefinierten Tag-Schlüssel mit dem übereinstimmen, was

Szenario	Grund	Lösung
	die nicht Ihrer Tag-Richtlinie entsprechen.	Sie in Ihrer Tag-Richtlinie angegeben haben. Beachten Sie, dass, wenn das Feld für die Groß-/Kle inschreibung von Tag-Schlü sseln in Ihrer Tag-Richtlinie nicht aktiviert ist, alle Tag-Schlüssel in Kleinbuchstaben konform sind und sicherste llen, dass Ihre TagOptions Tag-Schlüssel und optionalen benutzerdefinierten Tag-Schlü ssel mit dem übereinstimmen, was Sie in Ihrer Tag-Richtlinie benötigt haben.

Szenario	Grund	Lösung
Das Produkt kann aufgrund einer nicht konformen Tag-Schlüsselüberschreibung nicht gestartet werden.	Angeben der Groß-/Kle inschreibung in den TagOption s Schlüsseln, die mit den Regeln zur Durchsetzung von Tag-Richtlinienbuchstaben nicht übereinstimmen.	Konfigurieren Sie Ihre Tag-Richtlinien korrekt. Wenn Sie die Einhaltung der Tag-Schlüsselüberschreibung nicht angeben, wird die Standard-Tag-Schlüsselüberschreibung vollständig in Kleinbuchstaben geschrieben. Wenn Sie in Ihrer Tag-Richt linie die Einhaltung der Tag-SchlüsselGroß-/Kleinsch reibung nicht angeben, stellen Sie außerdem sicher, dass Ihre TagOptions Tag-Schlüssel in alle Kleinbuch staben AWS Service Catalog enthalten, um die Durchsetz ungsregeln einzuhalten. Wenn Sie eine Tag-Richtlinie verwenden, für die die Groß-/Kleinschreibungs-Compliance nicht aktiviert ist, betrachtet diese Tag-Richtlinie nur alle Kleinbuchstaben-Tag-Schlüss el als konform.
Das Produkt kann aufgrund inkompatibler Tag-Werte nicht gestartet werden.	Auswählen eines TagOptions Tag-Werts für einen Produktst art, der sich nicht in Ihrer Tag-Richtlinie Zulässige Liste Tag-Wert-Compliance befindet.	Ordnen Sie Ihren Produkten und Portfolios TagOptions zu, die mit den in der Listen-Tag-Richtlinie Tag Value Compliance zulässigen Tag-Werten übereinstimmen.

Externe Motoren für AWS Service Catalog

In AWS Service Catalog werden externe Engines durch einen EXTERNAL Produkttyp repräsentiert. Der EXTERNAL Produkttyp ermöglicht die Integration von Provisioning-Engines von Drittanbietern wie Terraform. Sie können externe Engines verwenden, um die Funktionen von Service Catalog über die nativen AWS CloudFormation Vorlagen hinaus zu erweitern und so die Verwendung anderer Instructure-as-Code-Tools (IaC) zu ermöglichen.

Mit EXTERNAL diesem Produkttyp können Sie Ressourcen über die vertraute Oberfläche von Service Catalog verwalten und bereitstellen und gleichzeitig die spezifischen Funktionen und die Syntax Ihres ausgewählten IaC-Tools nutzen.

Um EXTERNAL Produkttypen im Service Catalog zu aktivieren, müssen Sie eine Reihe von Standardressourcen in Ihrem Konto definieren. Diese Ressourcen werden als Engine bezeichnet. Service Catalog delegiert Aufgaben an bestimmten Punkten der Artefaktanalyse- und Bereitstellungsvorgänge an die Engine.

Ein Bereitstellungsartefakt stellt die spezifische Version eines Produkts in Service Catalog dar, sodass Sie konsistente Ressourcen verwalten und bereitstellen können.

Wenn Sie DescribeProvisioningParametersOperationen DescribeProvisioningArtifactoder Operationen für ein Bereitstellungsartefakt für einen EXTERNAL Produkttyp aufrufen AWS Service Catalog, ruft Service Catalog eine AWS Lambda Funktion in der Engine auf. Dies ist erforderlich, um die Liste der Parameter aus dem bereitgestellten Bereitstellungsartefakt zu extrahieren und an sie zurückzugeben. AWS Service Catalog Diese Parameter werden später als Teil des Bereitstellungsprozesses verwendet.

Wenn Sie ein EXTERNAL Bereitstellungsartefakt per Aufruf bereitstellen ProvisionProduct, führt Service Catalog zunächst einige Aktionen intern aus und sendet dann eine Nachricht an eine Amazon SQS SQS-Warteschlange in der Engine. Als Nächstes übernimmt die Engine die bereitgestellte Startrolle (die IAM-Rolle, die Sie einem Produkt als Startbeschränkung zuweisen), stellt die Ressourcen auf der Grundlage des bereitgestellten Bereitstellungsartefakts bereit und ruft die NotifyProvisionProductEngineWorkflowResultAPI auf, um Erfolg oder Misserfolg zu melden.

Aufrufe an UpdateProvisionedProductund TerminateProvisionedProductwerden auf ähnliche Weise behandelt, wobei jeder über eine eigene Warteschlange und Notify-APIs verfügt:

- NotifyProvisionProductEngineWorkflowResult
- NotifyUpdateProvisionedProductEngineWorkflowResult

- NotifyTerminateProvisionedProductEngineWorkflowResult.

Themen

- Überlegungen
- Parsen von Parametern
- Bereitstellung
- Aktualisieren
- Wird beendet
- Tagging

Überlegungen

Beschränkung auf eine externe Engine pro Hub-Konto

Sie können nur eine `EXTERNAL` Provisioning-Engine pro Service Catalog-Hub-Konto verwenden. Das Service hub-and-spokeCatalog-Modell ermöglicht es dem Hub-Konto, Basisprodukte zu erstellen und das Portfolio gemeinsam zu nutzen, während die Spoke-Konten Portfolios importieren und die Produkte nutzen können.

Dieses Limit ist darauf zurückzuführen, dass nur an eine Engine in einem Konto weitergeleitet werden `EXTERNAL` kann. Wenn ein Administrator mehrere externe Engines haben möchte, muss er die externen Engines (zusammen mit den Portfolios und Produkten) in verschiedenen Hub-Konten einrichten.

Externe Engines unterstützen nur Startrollen mit Startbeschränkungen

`EXTERNAL`Bereitstellungsartefakte unterstützen nur die Bereitstellung mit Startrollen, die mithilfe von Startbeschränkungen angegeben werden. Eine Startbeschränkung gibt die IAM-Rolle an, die Service Catalog annimmt, wenn ein Endbenutzer ein Produkt startet, aktualisiert oder beendet. Weitere Informationen zu Startbeschränkungen finden Sie unter AWS Service Catalog Startbeschränkungen.

Parsen von Parametern

`EXTERNAL`Bereitstellungsartefakte können ein beliebiges Format haben. Das bedeutet, dass die Engine bei der Erstellung eines `EXTERNAL` Produkttyps die Parameterliste aus dem bereitgestellten Bereitstellungsartefakt extrahieren und an Service Catalog zurückgeben muss. Dazu erstellen

Sie in Ihrem Konto eine Lambda-Funktion, die das folgende Anforderungsformat akzeptiert, das Bereitstellungsartefakt verarbeitet und das folgende Antwortformat zurückgibt.

> **Important**
>
> Die Lambda-Funktion muss benannt `ServiceCatalogExternalParameterParser` werden.

Anforderungssyntax:

```
{
    "artifact": {
        "path": "string",
        "type": "string"
    },
    "launchRoleArn": "string"
}
```

Feld	Typ	Erforderlich	Beschreibung
Artefakt	object	Ja	Details für das zu analysierende Artefakt.
Artefakt//Pfad	Zeichenfolge	Ja	Ort, von dem der Parser das Artefakt herunterlädt. Dies ist `AWS_S3` beispielsweise der Amazon S3 S3-URI.
Artefakt//Typ	Zeichenfolge	Ja	Art des Artefakts . Zulässiger Wert:`AWS_S3`.
LaunchRole	Zeichenfolge	Nein	Der Amazon-Ressourcenname (ARN) der Startroll

Feld	Typ	Erforderlich	Beschreibung
			e, die beim Herunterl aden des Artefakts übernommen werden soll. Wenn keine Startrolle angegeben ist, wird die Ausführun gsrolle von Lambda verwendet.

Antwortsyntax:

```
{
    "parameters": [
        {
            "key": "string"
            "defaultValue": "string",
            "type": "string",
            "description": "string",
            "isNoEcho": boolean
        },
    ]
}
```

Feld	Typ	Erforderlich	Beschreibung
Parameter	auflisten	Ja	Die Liste der Parameter, zu deren Angabe Service Catalog den Endbenutzer aufforder t, wenn er ein Produkt bereitstellt oder ein bereitgestelltes Produkt aktualisiert. Wenn im Artefakt keine Parameter

Feld	Typ	Erforderlich	Beschreibung
			definiert sind, wird eine leere Liste zurückgegeben.
Schlüssel	Zeichenfolge	Ja	Der Parameter schlüssel.
defaultValue	Zeichenfolge	Nein	Der Standardwert des Parameters, wenn der Endbenutzer keinen Wert angibt.
Typ	Zeichenfolge	Ja	Der erwartete Typ des Parameter werts für die Engine. Zum Beispiel eine Zeichenfolge, ein boolescher Wert oder eine Map. Die zulässigen Werte sind für jede Engine spezifisch. Service Catalog übergibt jeden Parameterwert als Zeichenfolge an die Engine.
description	Zeichenfolge	Nein	Beschreibung für den Parameter. Es wird empfohlen, dass dies benutzerfreundlich ist.

Feld	Typ	Erforderlich	Beschreibung
isNoEcho	boolesch	Nein	Ermittelt, ob der Parameterwert nicht in Protokollen wiedergegeben wird. Der Standardwert ist falsch (Parameterwerte werden als Echo wiedergegeben).

Bereitstellung

Für den ProvisionProductVorgang delegiert Service Catalog die tatsächliche Bereitstellung von Ressourcen an die Engine. Die Engine ist für die Schnittstelle mit der IaC-Lösung Ihrer Wahl (z. B. Terraform) verantwortlich, um Ressourcen gemäß der Definition im Artefakt bereitzustellen. Die Engine ist auch dafür verantwortlich, Service Catalog über das Ergebnis zu informieren.

Service Catalog sendet alle Bereitstellungsanfragen an eine Amazon SQS SQS-Warteschlange in Ihrem Konto mit dem Namen`ServiceCatalogExternalProvisionOperationQueue`.

Anforderungssyntax:

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

Feld	Typ	Erforderlich	Beschreibung
Token	Zeichenfolge	Ja	Das Token, das diesen Vorgang identifiziert. Das Token muss an Service Catalog zurückgegeben werden, um über die Ausführungsergebnisse zu informieren.
Operation	Zeichenfolge	Ja	Dieses Feld muss `PROVISION_PRODUCT` für diesen Vorgang verwendet werden.
provisionedProductId	Zeichenfolge	Ja	ID des bereitgestellten Produkts.

Feld	Typ	Erforderlich	Beschreibung
provisionedProductName	Zeichenfolge	Ja	Name des bereitgestellten Produkts.
Produkt-ID	Zeichenfolge	Ja	ID des Produkts.
provisioningArtifactId	Zeichenfolge	Ja	ID des Bereitstellungsartefakts.
recordId	Zeichenfolge	Ja	ID des Servicekatalog-Datensatzes für diesen Vorgang.
launchRoleArn	Zeichenfolge	Ja	Amazon-Ressourcenname (ARN) für die IAM-Rolle, die für die Bereitstellung von Ressourcen verwendet werden soll.
Artefakt	object	Ja	Details für das Artefakt, das definiert, wie die Ressourcen bereitgestellt werden.
Artefakt//Pfad	Zeichenfolge	Ja	Ort, von dem die Engine das Artefakt herunterlädt. Dies ist `AWS_S3` beispielsweise der Amazon S3 S3-URI.
Artefakt//Typ	Zeichenfolge	Ja	Art des Artefakts. Zulässiger Wert:`AWS_S3`.

Feld	Typ	Erforderlich	Beschreibung
Identitäts	Zeichenfolge	Nein	Das Feld wird derzeit nicht verwendet.
Parameter	auflisten	Ja	Liste der Parameter -Schlüssel-Wert-Pa are, die der Benutzer als Eingaben für diesen Vorgang in Service Catalog eingegeben hat.
tags	auflisten	Ja	Liste der Benutzer, key-value-pairs die in Service Catalog als Tags eingegebe n wurden, um sie auf die bereitges tellten Ressourcen anzuwenden.

Benachrichtigung über das Workflow-Ergebnis:

Rufen Sie die NotifyProvisionProductEngineWorkflowResult API mit dem Antwortobjekt auf, das auf der API-Detailseite angegeben ist.

Aktualisieren

Für den UpdateProvisionedProductVorgang delegiert Service Catalog die tatsächliche Aktualisierung der Ressourcen an die Engine. Die Engine ist für die Schnittstelle mit der IaC-Lösung Ihrer Wahl (z. B. Terraform) verantwortlich, um die im Artefakt definierten Ressourcen zu aktualisieren. Die Engine ist auch dafür verantwortlich, Service Catalog über das Ergebnis zu informieren.

Service Catalog sendet alle Aktualisierungsanfragen an eine Amazon SQS SQS-Warteschlange in Ihrem Konto mit dem Namen`ServiceCatalogExternalUpdateOperationQueue`.

Anforderungssyntax:

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

Feld	Typ	Erforderlich	Beschreibung
Token	Zeichenfolge	Ja	Das Token, das diesen Vorgang identifiziert. Das Token muss an Service Catalog zurückgegeben werden, um über die

Feld	Typ	Erforderlich	Beschreibung
			Ausführungsergebnisse zu informieren.
Operation	Zeichenfolge	Ja	Dieses Feld muss `UPDATE_PROVISION_PRODUCT` für diesen Vorgang verwendet werden.
provisionedProductId	Zeichenfolge	Ja	ID des bereitgestellten Produkts.
provisionedProductName	Zeichenfolge	Ja	Name des bereitgestellten Produkts.
Produkt-ID	Zeichenfolge	Ja	ID des Produkts.
provisioningArtifactId	Zeichenfolge	Ja	ID des Bereitstellungsartefakts.
recordId	Zeichenfolge	Ja	ID des Servicekatalog-Datensatzes für diesen Vorgang.
launchRoleArn	Zeichenfolge	Ja	Amazon-Ressourcenname (ARN) für die IAM-Rolle, die für die Bereitstellung von Ressourcen verwendet werden soll.
Artefakt	object	Ja	Details für das Artefakt, das definiert, wie die Ressourcen bereitgestellt werden.

Feld	Typ	Erforderlich	Beschreibung
Artefakt//Pfad	Zeichenfolge	Ja	Ort, von dem die Engine das Artefakt herunterlädt. Dies ist `AWS_S3` beispiels weise der Amazon S3 S3-URI.
Artefakt//Typ	Zeichenfolge	Ja	Art des Artefakts . Zulässiger Wert:`AWS_S3`.
Identitäts	Zeichenfolge	Nein	Das Feld wird derzeit nicht verwendet.
Parameter	auflisten	Ja	Liste der Parameter -Schlüssel-Wert-Pa are, die der Benutzer als Eingaben für diesen Vorgang in Service Catalog eingegeben hat.
tags	auflisten	Ja	Liste der Benutzer, key-value-pairs die in Service Catalog als Tags eingegebe n wurden, um sie auf die bereitges tellten Ressourcen anzuwenden.

Benachrichtigung über das Workflow-Ergebnis:

Rufen Sie die NotifyUpdateProvisionedProductEngineWorkflowResultAPI mit dem Antwortobjekt auf, das auf der API-Detailseite angegeben ist.

Wird beendet

Für den TerminateProvisionedProductVorgang delegiert Service Catalog das tatsächliche Beenden von Ressourcen an die Engine. Die Engine ist dafür verantwortlich, eine Schnittstelle mit der IaC-Lösung Ihrer Wahl (wie Terraform) herzustellen, um Ressourcen, wie im Artefakt definiert, zu terminieren. Die Engine ist auch dafür verantwortlich, Service Catalog über das Ergebnis zu informieren.

Service Catalog sendet alle Terminierungsanfragen an eine Amazon SQS SQS-Warteschlange in Ihrem Konto mit dem Namen`ServiceCatalogExternalTerminateOperationQueue`.

Anforderungssyntax:

```
{
    "token": "string",
    "operation": "string",
    "provisionedProductId": "string",
    "provisionedProductName": "string",
    "recordId": "string",
    "launchRoleArn": "string",
    "identity": {
        "principal": "string",
        "awsAccountId": "string",
        "organizationId": "string"
    }
}
```

Feld	Typ	Erforderlich	Beschreibung
Token	Zeichenfolge	Ja	Das Token, das diesen Vorgang identifiziert. Das Token muss an Service Catalog zurückgegeben werden, um über die Ausführungsergebnisse zu informieren.

Feld	Typ	Erforderlich	Beschreibung
Operation	Zeichenfolge	Ja	Dieses Feld muss `TERMINATE_PROVISIONED_PRODUCT` für diesen Vorgang verwendet werden.
provisionedProductId	Zeichenfolge	Ja	ID des bereitgestellten Produkts.
provisionedProductName	Zeichenfolge	Ja	Name des bereitgestellten Produkts.
recordId	Zeichenfolge	Ja	ID des Servicekatalog-Datensatzes für diesen Vorgang.
launchRoleArn	Zeichenfolge	Ja	Amazon-Ressourcenname (ARN) für die IAM-Rolle, die für die Bereitstellung von Ressourcen verwendet werden soll.
Identitäts	Zeichenfolge	Nein	Das Feld wird derzeit nicht verwendet.

Benachrichtigung über das Workflow-Ergebnis:

Rufen Sie die NotifyTerminateProvisionedProductEngineWorkflowResultAPI mit dem Antwortobjekt auf, das auf der API-Detailseite angegeben ist.

Tagging

Für die Verwaltung von Tags über Resource Groups benötigt Ihre Launch-Rolle die folgenden zusätzlichen Berechtigungsanweisungen:

```
{
    "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**
>
> Die Startrolle benötigt außerdem Tagging-Berechtigungen für die spezifischen Ressourcen im Artefakt, z. B. `ec2:CreateTags`

Überwachen in AWS Service Catalog

Sie können Ihre Ressourcen AWS Service Catalog mit Amazon überwachen CloudWatch, das Rohdaten von sammelt und AWS Service Catalog zu lesbaren Metriken verarbeitet. Diese Statistiken werden für einen Zeitraum von zwei Wochen aufgezeichnet, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihr Service ausgeführt wird. AWS Service Catalog-Metrikdaten werden in Abständen von 1 Minute automatisch an CloudWatch gesendet. Weitere Informationen zu CloudWatchfinden Sie im Amazon CloudWatch - Benutzerhandbuch.

Eine Liste verfügbarer Metriken und Maße finden Sie unter AWS Service Catalog CloudWatch Metriken.

Die Überwachung ist ein wichtiger Teil der Wahrung von Zuverlässigkeit, Verfügbarkeit und Performance von AWS Service Catalog und Ihren AWS-Lösungen. Sie sollten von allen Teilen Ihrer AWS-Lösung Überwachungsdaten sammeln, damit Sie Ausfälle, die sich über mehrere Punkte erstrecken, leichter debuggen können. Bevor Sie mit der Überwachung von AWS Service Catalog beginnen, sollten Sie einen Überwachungsplan mit Antworten auf die folgenden Fragen erstellen:

- Was sind Ihre Ziele bei der Überwachung?
- Welche Ressourcen werden überwacht?
- Wie oft werden diese Ressourcen überwacht?
- Welche Überwachungstools werden verwendet?
- Wer soll die Überwachungsaufgaben ausführen?
- Wer soll benachrichtigt werden, wenn Fehler auftreten?

Überwachungstools

AWS bietet verschiedene Tools, mit deren Hilfe Sie AWS Service Catalog überwachen können. Sie können einige dieser Tools so konfigurieren, dass diese die Überwachung für Sie übernehmen, während bei anderen Tools ein manuelles Eingreifen nötig ist. Wir empfehlen, dass Sie die Überwachungsaufgaben möglichst automatisieren.

Automatisierte Überwachungstools

Sie können Amazon- CloudWatch Alarme verwenden, um Unterbrechungen zu überwachen AWS Service Catalog und zu melden.

CloudWatch Alarme überwachen eine einzelne Metrik über einen von Ihnen angegebenen Zeitraum und führen eine oder mehrere Aktionen aus, die auf dem Wert der Metrik im Verhältnis zu einem bestimmten Schwellenwert über eine Reihe von Zeiträumen basieren. Die Aktion ist eine Benachrichtigung, die an ein Amazon Simple Notification Service (Amazon SNS)-Thema oder eine Amazon EC2 Auto Scaling-Richtlinie gesendet wird. - CloudWatch Alarme rufen keine Aktionen auf, nur weil sie sich in einem bestimmten Status befinden. Der Status muss geändert und für eine bestimmte Anzahl von Zeiträumen beibehalten worden sein. Informationen zum Erstellen eines Alarms finden Sie unter Erstellen von Amazon- CloudWatch Alarmen. Weitere Informationen zur Verwendung von Amazon CloudWatch-Metriken mit finden Sie AWS Service Catalogunter AWS Service Catalog CloudWatch Metriken.

AWS Service Catalog CloudWatch Metriken

Sie können Ihre Ressourcen AWS Service Catalog mit Amazon überwachen CloudWatch, das Rohdaten von sammelt und AWS Service Catalog zu lesbaren Metriken verarbeitet. Diese Statistiken werden für einen Zeitraum von zwei Wochen aufgezeichnet, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihr Service ausgeführt wird. AWS Service Catalog-Metrikdaten werden in Abständen von 1 Minute automatisch an CloudWatch gesendet. Weitere Informationen zu CloudWatchfinden Sie im Amazon- CloudWatch Benutzerhandbuch.

Themen

- Aktivieren von CloudWatch Metriken
- Verfügbare Metriken und Dimensionen
- Anzeigen von AWS Service Catalog-Metriken

Aktivieren von CloudWatch Metriken

Amazon- CloudWatch Metriken sind standardmäßig aktiviert.

Verfügbare Metriken und Dimensionen

Die Metriken und Dimensionen, die an Amazon AWS Service Catalog sendet, CloudWatch sind unten aufgeführt.

AWS Service Catalog-Metriken

Der `AWS/ServiceCatalog`-Namespace enthält die folgenden Metriken.

Metrik	Beschreibung
`ProvisionedProductLaunch`	Die Anzahl der bereitgestellten Produkte, die für ein bestimmtes Produkt und ein bestimmtes Bereitstellungsartefakt in einem bestimmten Zeitraum ausgeführt werden. Einheiten: Anzahl Gültige Statistiken: Minimum, Maximum, Summe, Durchschnitt

Dimensionen für AWS Service Catalog-Metriken

AWS Service Catalog sendet die folgenden Dimensionen an Amazon CloudWatch.

Dimension	Beschreibung
`State`	Diese Dimension filtert die angeforderten Daten für alle bereitgestellten Produkte, die mit diesem angegebenen Zustand ausgeführt werden. So können Sie Ihre Daten nach dem Ausführungszustand kategorisieren. Gültiger Zustand: ERFOLGREICH, FEHLGESCHLAGEN
`ProductId`	Diese Dimension filtert die angeforderten Daten nur für die identifizierte Produkt-ID. So können Sie genau das Produkt bestimmen, von dem aus der Start erfolgen soll.

Dimension	Beschreibung
`ProvisioningArtifactId`	Diese Dimension filtert die angeforderten Daten nur für die identifizierte Bereitstellungsartefakt-ID. So können Sie genau die Version von Produkten bestimmen, von der aus der Start erfolgen soll.

Anzeigen von AWS Service Catalog-Metriken

Sie können Amazon- CloudWatch Metriken in der Amazon- CloudWatch Konsole anzeigen, die eine detaillierte und anpassbare Anzeige Ihrer Ressourcen sowie die Anzahl der laufenden Aufgaben in einem Service bietet.

Themen

- Anzeigen von AWS Service Catalog Metriken in der Amazon CloudWatch -Konsole

Anzeigen von AWS Service Catalog Metriken in der Amazon CloudWatch -Konsole

Sie können AWS Service Catalog Metriken in der Amazon- CloudWatch Konsole anzeigen. Die Amazon- CloudWatch Konsole bietet eine detaillierte Ansicht der AWS Service Catalog Metriken, und Sie können die Ansichten an Ihre Bedürfnisse anpassen. Weitere Informationen zu Amazon CloudWatchfinden Sie im Amazon- CloudWatch Benutzerhandbuch.

So zeigen Sie Metriken in der Amazon- CloudWatch Konsole an

1. Öffnen Sie die Amazon- CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Abschnitt Metrics (Metriken) im linken Navigationsbereich Service Catalog aus.
3. Wählen Sie die Metriken, die angezeigt werden sollen.

Protokollieren von AWS Service Catalog-API-Aufrufen mithilfe von AWS CloudTrail

AWS Service Catalog ist in integriert, einem ServiceAWS CloudTrail, der die Aktionen eines Benutzers, einer Rolle oder eines -AWSServices in aufzeichnetAWS Service Catalog. CloudTrail

erfasst alle API-Aufrufe für AWS Service Catalog als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS Service Catalog-Konsole und Code-Aufrufe der AWS Service Catalog-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3-Bucket aktivieren, einschließlich Ereignissen für AWS Service Catalog. Wenn Sie keinen Trail konfigurieren, können Sie trotzdem die neuesten Ereignisse in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von CloudTrailgesammelten Informationen können Sie die an gestellte AnfrageAWS Service Catalog, die IP-Adresse, von der die Anfrage gestellt wurde, den Initiator der Anfrage, den Zeitpunkt der Anfrage und zusätzliche Details bestimmen.

Weitere Informationen zu CloudTrailfinden Sie im AWS CloudTrail-Benutzerhandbuch.

AWS Service Catalog -Informationen in CloudTrail

CloudTrail wird bei der Erstellung in Ihrem AWS Konto aktiviert. Wenn eine Aktivität in auftrittAWS Service Catalog, wird diese Aktivität in einem - CloudTrail Ereignis zusammen mit anderen -AWSServiceereignissen im Ereignisverlauf aufgezeichnet. Sie können die neusten Ereignisse in Ihr AWS-Konto herunterladen und dort suchen und anzeigen. Weitere Informationen finden Sie unter Anzeigen von Ereignissen mit dem CloudTrail Ereignisverlauf .

Zur kontinuierlichen Aufzeichnung von Ereignissen in Ihrem AWS-Konto, einschließlich Ereignissen für AWS Service Catalog, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Bereitstellung von Protokolldateien an einen Amazon S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS-Partition und stellt die Protokolldateien in dem von Ihnen angegebenen Amazon-S3-Bucket bereit. Darüber hinaus können Sie andere -AWSServices konfigurieren, um die in den CloudTrail Protokollen erfassten Ereignisdaten weiter zu analysieren und entsprechend zu agieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- In AWS CloudTrail unterstützte Services und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für AWS CloudTrail
- Empfangen von AWS CloudTrail-Protokolldateien aus mehreren Regionen und Empfangen von AWS CloudTrail-Protokolldateien aus mehreren Konten

CloudTrail protokolliert alle AWS Service Catalog Aktionen. Aufrufe der `UpdateProvisionedProduct` Aktionen `CreatePortfolio`, `CreateProduct` und erzeugen beispielsweise Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Stammbenutzer- oder AWS Identity and Access Management (IAM)-Benutzeranmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer ausgeführt wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

Grundlagen zu AWS Service Catalog-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Bereitstellung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge. Das folgende Beispiel zeigt einen - CloudTrail Protokolleintrag, der die `CreateApplication`-API demonstriert.


```
{
    "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"
}
```

Konsolen-Branding-Einstellungen

AWS Service Catalog ermöglicht es Administratoren, Konsolen-Branding-Einstellungen für Konten anzugeben. Administratoren können mithilfe des Konsolen-Brandings einen Unternehmensnamen, ein Logobild sowie eine primäre und sekundäre (akzentuelle) Farbe für eine Vielzahl von Website-Komponenten angeben. Diese Branding-Einstellungen sind sowohl für Administratoren als auch für Endbenutzer sichtbar, wenn sie die Konsole verwenden.

Einstellungen für das Konsolen-Branding verbessern das Erscheinungsbild eines Kontos und führen Folgendes aus:

- Erstellt einen nahtlosen visuellen Übergang zwischen der Konsole und internen Anwendungen
- Unterscheidung von Konten, die von verschiedenen internen Teams innerhalb desselben Unternehmens verwendet werden
- Differenziert Konten in mehreren Umgebungen, z. B. Entwicklung, Staging oder Produktion

> **Note**
>
> Administratoren geben die Branding-Einstellungen der Konsole auf Kontoebene an.

So geben Sie die Branding-Einstellungen der Konsole an

1. Wählen Sie im linken Navigationsmenü Einstellungen aus.
2. Wählen Sie Bearbeiten aus, um entweder die Branding-Einstellungen im Light-Modus oder im Dark-Modus zu verwenden.
3. Laden Sie ein Logo hoch, geben Sie einen Markennamen ein und wählen Sie dann die Primärfarbe und die Sekundärfarbe aus.
4. Wählen Sie Speichern.

Eine Liste der Regionen, in denen das Branding der Konsole AWS Service Catalog unterstützt, finden Sie unter AWS-Region Support für das Branding der Konsole.

AWS-Region -Unterstützung für Konsolen-Branding-Einstellungen

AWS Service Catalog unterstützt Konsolen-Branding-Einstellungen in den , die in der folgenden Tabelle AWS-Regionen aufgeführt sind.

AWS-Region-Name	AWS-Region-Identität
USA Ost (Nord-Virginia)	us-east-1
USA Ost (Ohio)	us-east-2
USA West (Nordkalifornien)	us-west-1
US West (Oregon)	us-west-2
Afrika (Kapstadt)	af-south-1
Asien-Pazifik (Hongkong)	ap-east-1
Asien-Pazifik (Jakarta)	ap-southeast-3
Asien-Pazifik (Mumbai)	ap-south-1
Asien-Pazifik (Osaka)	ap-northeast-3
Asien-Pazifik (Seoul)	ap-northeast-2
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Canada (Central)	ca-central-1
Europa (Frankfurt)	eu-central-1
Europe (Ireland)	eu-west-1
Europe (London)	eu-west-2

AWS-Region-Name	AWS-Region-Identität	
Europa (Mailand)	eu-south-1	
Europa (Paris)	eu-west-3	
Europe (Stockholm)	eu-north-1	
Naher Osten (Bahrain)	me-south-1	
South America (São Paulo)	sa-east-1	
AWS GovCloud (USA-Ost)	us-gov-east-1	
AWS GovCloud (USA-West)	us-gov-west-1	

Dokumentverlauf

In der folgenden Tabelle werden die wichtigen Änderungen an der Dokumentation für beschrieben AWS Service Catalog. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

- API-Version: 2014-11-12
- Letzte Aktualisierung der Dokumentation: 16. Mai 2024

Änderung	Beschreibung	Datum
Externe Motoren für AWS Service Catalog	AWS Service Catalog fügt neue Dokumentation für externe Engines hinzu. Externe Engines werden durch einen `EXTERNAL` Produkttyp repräsentiert. Der `EXTERNAL` Produkttyp ermöglicht die Integration von Provisioning-Engines von Drittanbietern wie Terraform. Sie können externe Engines verwenden, um die Funktionen von Service Catalog über die nativen AWS CloudFormation Vorlagen hinaus zu erweitern und so die Verwendung anderer Instructu re-as-Code-Tools (IaC) zu ermöglichen. Weitere Informati onen finden Sie unter Externe Engines für. AWS Service Catalog	16. Mai 2024
Sicherheits-IAM-Update	AWS Service Catalog aktualisiert die `AWSServic eCatalogSyncServic`	7. Mai 2024

	`eRolePolicy` Richtlinie, um sie `codestar-connections` zu änder`codeconnections` . Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien für AWS Service Catalog AppRegistry.	

Frühere Aktualisierungen

In der folgenden Tabelle wird der Versionsverlauf der Dokumentation AWS Service Catalog vor dem 25. April 2024 beschrieben.

Funktion	Beschreibung	Datum der Veröffentlichung
AWS Service Catalog	Weitere Informationen zu den Änderungen von Hashicorp an der Terraform-Lizenzierung und der Aktualisierung auf den Produkttyp External finden Sie unter. Aktualisieren vorhandener Open-Source-Produkte von Terraform und bereitgestellter Produkte auf den externen Produkttyp	20. Oktober 2023
AWS Service Catalog	Weitere Informationen zum Teilen eines Portfolios mit AWS Organizations und zum Zulassen der Synchronisierung finden Sie unter AWS Service Catalog Richtlinie und Rolle im AWS Organizations Zusammenhang mit dem AWSServic	14. April 2023

Funktion	Beschreibung	Datum der Veröffentlichung
	eCatalogOrgsDataSyncServiceRolePolicyDienst. AWSServiceRoleForServiceCatalogOrgsDataSync	
AWS Service Catalog	Informationen zur Verwaltung von Produkten, die mit Git verbunden sind, und AWS Service Catalog zur Möglichkeit, Vorlagen in einem externen Repository mit Ihren AWS Service Catalog Produkten zu synchronisieren, finden Sie unter AWSServiceCatalogSyncServiceRolePolicyRichtlinie und AWSServiceRoleForServiceCatalogSyncRolle im Zusammenhang mit Diensten.	18. November 2022
AWS Service Catalog AppRegistry	Informationen darüber, wie AppRegistry Sie Ihre AWS Anwendungen, die zugehörigen Ressourcensammlungen und Anwendungsattributgruppen speichern können, finden Sie unter. AWS Service Catalog AppRegistry	15. Juni 2022
AWS Service Management Connector	Weitere Informationen zu Konnektoren für Jira Service Management und ServiceNow finden Sie unter AWS Service Management Connector.	9. Juni 2022

Funktion	Beschreibung	Datum der Veröffentlichung
Konnektor für Jira Service Management	Informationen zu den Updates des Connectors für Jira Service Management finden Sie unter AWS Service Management Connector für Jira Service Management.	25. Mai 2021
Konnektor für ServiceNow	Weitere Informationen zu den Updates für den Connector für ServiceNow finden Sie unter AWS Service Management Connector für ServiceNow.	7. April 2021
Konnektor für ServiceNow	Weitere Informationen zu den Updates für den Connector für ServiceNow finden Sie unter AWS Service Management Connector für ServiceNow.	24. September 2020
AWS Service Quotas	Informationen zur AWS Service Catalog Funktions weise von AWS Service Quotas finden Sie unter AWS Service Catalog Standard-Servicekontingenten.	24. März 2020
Bibliothek „Erste Schritte“	Weitere Informationen zu der von angebotenen Bibliothek mit gut gestalteten Produktvo rlagen finden Sie unter AWS Service CatalogBibliothek „Erste Schritte“	10. März 2020

Funktion	Beschreibung	Datum der Veröffentlichung
Versionshinweise	Weitere Informationen zur Produktversionsanleitung finden Sie unter Versionshinweise.	17. Dezember 2019
Konnektor für Jira Service Desk	Informationen zur Verwendung des Connectors für Jira Service Desk finden Sie unter AWS Service Management Connector für Jira Service Desk.	21. November 2019
Konnektor für ServiceNow	Weitere Informationen zu den Updates für den Connector für ServiceNow finden Sie unter AWS Service Management Connector für ServiceNow.	18. November 2019
Neues Kapitel bezüglich der Sicherheit	Weitere Informationen zur Sicherheit in AWS Service Catalog finden Sie unter Sicherheit in AWS Service Catalog.	31. Oktober 2019
Den Besitzer des bereitgestellten Produkts ändern	Informationen zum Ändern des Besitzers bereitgestellter Produkte finden Sie unter Ändern des Besitzers des bereitgestellten Produkts.	31. Oktober 2019

Funktion	Beschreibung	Datum der Veröffentlichung
Neue Einschränkung beim Aktualisieren von Ressourcen	Informationen zur Verwendung der RESOURCE_UPDATE-Beschränkung zur Aktualisierung von Tags in bereitgestellten Produkten finden AWS Service Catalog Sie unter Einschränkungen für Tag-Updates.	17. April 2019
Konnektor für ServiceNow	Informationen zur Verwendung des Connectors für ServiceNow finden Sie unter AWS Service Management Connector für ServiceNow.	19. März 2019
Support für AWS CloudFormation StackSets	Um mit der Verwendung zu beginnen AWS CloudFormation StackSets, siehe Verwenden AWS CloudFormation StackSets.	14. November 2018
Self-Service-Aktionen	Informationen zum Einstieg in die Nutzung von Self-Service-Aktionen finden Sie unter AWS CloudFormation Serviceaktionen.	17. Oktober 2018
CloudWatch Amazon-Metriken	Weitere Informationen zu CloudWatch Amazon-Metriken finden Sie unter AWS Service CatalogAmazon CloudWatch.	26. September 2018

Funktion	Beschreibung	Datum der Veröffentlichung
Support für TagOptions	Informationen zur Verwaltung von Stichwörtern finden Sie unter AWS Service Catalog TagOptionBibliothek.	28. Juni 2017
Importieren eines Portfolios	Informationen zum Importieren eines Portfolios, das von einem anderen AWS Konto gemeinsam genutzt wird, finden Sie unter Portfolio importieren.	16. Februar 2016
Updates der Informationen zu Berechtigungen	Informationen zum Gewähren des Zugriffs auf die Konsolenansicht für Endbenutzer finden Sie unter Konsolenzugriff für Endbenutzer.	16. Februar 2016
Erstversion	Dies ist die erste Version des AWS Service Catalog Administratorhandbuchs.	9. Juli 2015

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.