Benutzerhandbuch

# AWS Service Catalog

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# AWS Service Catalog: Benutzerhandbuch

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

# Table of Contents

Was ist Service Catalog? ... 1
Video: Introduction to 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 ... 6
Kontingente für Einschränkungen ... 7
Portfoliokontingente ... 7
Produktkontingente ... 7
Kontingente für bereitgestellte Produkte ... 7
Regionale Kontingente ... 7
Kontingente für Service-Aktionen ... 7
TagOptions Kontingente ... 8
Einrichten ... 9
... 9
Melden Sie sich an für eine AWS-Konto ... 9
Erstellen eines Benutzers mit Administratorzugriff ... 9
Gewähren Sie Administratoren Berechtigungen ... 11
Erteilen Sie Endbenutzern Berechtigungen ... 14
Installieren und konfigurieren Sie die Terraform Provisioning Engine ... 15
Bestimmung der Warteschlange ... 15
Confused Deputy zu Ihrer Terraform-Provisioning-Engine hinzufügen ... 16
Erste Schritte ... 20
Bibliothek „Erste Schritte“ ... 20
Voraussetzungen ... 21

Weitere Informationen ... 21
Erste Schritte mit einem AWS CloudFormation Produkt ... 21
Schritt 1: Laden Sie die Vorlage herunter ... 22
Schritt 2: Erstellen eines Schlüsselpaares ... 27
Schritt 3: Erstellen Sie ein Portfolio ... 28
Schritt 4: Erstellen Sie ein neues Produkt im Portfolio ... 28
Schritt 5: Fügen Sie eine Vorlagenbeschränkung hinzu ... 29
Schritt 6: Fügen Sie eine Startbeschränkung hinzu ... 30
Schritt 7: Gewähren Sie Endbenutzern Zugriff auf das Portfolio ... 33
Schritt 8: Testen Sie die Endbenutzererfahrung ... 34
Erste Schritte mit einem Terraform-Produkt ... 35
Aktualisierung auf den externen Produkttyp ... 37
Voraussetzung: Konfigurieren Sie Ihre Terraform-Provisioning-Engine ... 38
Schritt 1: Herunterladen der Terraform-Konfigurationsdatei ... 39
Schritt 2: Erstellen Sie ein Terraform-Produkt ... 41
Schritt 3: Erstellen Sie ein Portfolio ... 42
Schritt 4: Produkt zum Portfolio hinzufügen ... 42
Schritt 5: Startrollen erstellen ... 43
Schritt 6: Fügen Sie eine Startbeschränkung hinzu ... 47
Schritt 7: Endbenutzerzugriff gewähren ... 48
Schritt 8: Portfolio mit Endbenutzern teilen ... 49
Schritt 9: Testen Sie die Endbenutzererfahrung ... 50
Schritt 10: Überwachung der Terraform-Bereitstellungsvorgänge ... 51
Sicherheit ... 53
Datenschutz ... 54
Datenschutz durch Verschlüsselung ... 55
Identitäts- und Zugriffsverwaltung ... 55
Zielgruppe ... 56
Beispiele für identitätsbasierte Richtlinien für AWS Service Catalog ... 56
AWS verwaltete Richtlinien ... 62
Verwenden von serviceverknüpften Rollen ... 73
Problembehandlung bei AWS Service Catalog Identität und Zugriff ... 78
Zugriffssteuerung ... 80
Protokollieren und Überwachen ... 81
Compliance-Validierung ... 81
Ausfallsicherheit ... 82

Sicherheit der Infrastruktur ... 83
Bewährte Methoden für die Sicherheit ... 84
Verwalten von Katalogen ... 85
Verwalten von Portfolios ... 85
Erstellen, Anzeigen und Löschen von Portfolios ... 86
Anzeigen von Portfoliodetails ... 86
Erstellen und Löschen von Portfolios ... 86
Produkte hinzufügen ... 87
Hinzufügen von Einschränkungen ... 90
Gewähren des Zugriffs für Benutzer ... 91
Freigeben eines Portfolios ... 92
Portfolios teilen und importieren ... 100
Verwalten von Produkten ... 106
Anzeigen der Produktseite ... 106
Erstellen von Produkten ... 106
Produkte zu Portfolios hinzufügen ... 110
Produkte aktualisieren ... 110
Produkte mit Vorlagendateien aus externen Repositorys synchronisieren ... 112
Produkte löschen ... 121
Verwalten von Versionen ... 130
Verwenden von Einschränkungen ... 131
Starteinschränkungen ... 131
Benachrichtigungseinschränkungen ... 137
Einschränkungen für die Tag-Aktualisierung ... 139
Stack-Set-Einschränkungen ... 139
Vorlageneinschränkungen ... 140
Verwenden von Service-Aktionen ... 145
Voraussetzungen ... 146
Schritt 1: Konfigurieren von Berechtigungen für Endbenutzer ... 146
Schritt 2: Erstellen einer Service-Aktion ... 148
Schritt 3: Verknüpfen der Service-Aktion mit einer Produktversion ... 148
Schritt 4: Testen der Endbenutzerumgebung ... 149
Schritt 5: Verwaltung von Serviceaktionen mit AWS CloudFormation ... 149
Schritt 6: Problembehandlung ... 150
AWS Marketplace Produkte zu Ihrem Portfolio hinzufügen ... 152
AWS Marketplace Produkte verwalten mit AWS Service Catalog ... 153

Manuelles Verwalten und Hinzufügen von AWS Marketplace Produkten ..... 153
Benutzen AWS CloudFormation StackSets ..... 158
Stack-Sets und Stack-Instances ..... 159
Stack-Set-Einschränkungen ..... 159
Verwalten von Budgets ..... 159
Voraussetzungen ..... 160
Erstellen eines Budgets ..... 161
Ein Budget zuordnen ..... 162
Ein Budget anzeigen ..... 163
Die Zuordnung eines Budgets aufheben ..... 164
Verwalten von bereitgestellten Produkten ..... 165
Verwaltung der bereitgestellten Produkte als Administrator ..... 165
Ändern des Besitzers des bereitgestellten Produkts ..... 166
Weitere Informationen finden Sie unter: ..... 167
Vorlagen für bereitgestellte Produkte aktualisieren ..... 167
Tutorial: Identifizieren der Benutzerressourcenzuordnung ..... 168
Verwaltung von Fehlern im Terraform Open Source-Produktstatus ..... 172
Beispiele für Statusfehler ..... 173
Verwaltung der Terraform Open Source-Produktstatusdatei ..... 174
Verwalten von Tags ..... 175
AutoTags ..... 175
TagOption Bücherei ..... 176
Ein Produkt auf den Markt bringen mit TagOptions ..... 178
Verwaltung TagOptions ..... 182
Verwendung TagOptions mit AWS Organizations Tag-Richtlinien ..... 184
Externe Motoren ..... 190
Überlegungen ..... 191
Parsen von Parametern ..... 191
Bereitstellung ..... 195
Aktualisieren ..... 198
Wird beendet ..... 202
Tagging ..... 204
Überwachen ..... 205
Überwachungstools ..... 205
Automatisierte Tools ..... 206
CloudWatch Metriken ..... 206

CloudWatch Metriken aktivieren ..... 206
Verfügbare Metriken und Dimensionen ..... 207
Anzeigen von AWS Service Catalog -Metriken ..... 208
CloudTrail protokolliert ..... 209
AWS Service Catalog Informationen in CloudTrail ..... 209
AWS Service Catalog Logdateieinträge verstehen ..... 211
Branding der Konsole ..... 213
AWS-Region Unterstützung für das Konsolen-Branding ..... 214
Dokumentverlauf ..... 216
Frühere Aktualisierungen ..... 217
..... ccxxiii

# Was ist Service Catalog?

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

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

Der 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 Produktportfolios 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 Service Catalog -Detailseite von.

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

# Video: Introduction to AWS Service Catalog

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

Einführung in AWS Service Catalog

# Service Catalog

Bei den ersten Schritten mit Service Catalog ist es hilfreich, die Komponenten und die ersten Workflows für Administratoren und Endbenutzer zu kennen.

## Benutzer

Service Catalog unterstützt die folgenden Benutzertypen:

- Katalogadministratoren (Administratoren) — Verwalten Sie einen Produktkatalog (Anwendungen und Dienste), organisieren Sie diese 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 zu ermöglichen.
- Endbenutzer — Sie erhalten AWS Anmeldeinformationen von ihrer IT-Abteilung oder ihrem Manager und verwenden sie AWS Management Console , um Produkte zu starten, für die ihnen Zugriff gewährt wurde. 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 zur Bereitstellung bereitstellen möchten AWS. Ein Produkt besteht aus einer oder mehreren AWS Ressourcen, z. B. EC2 Instanzen, Speichervolumes, Datenbanken, Überwachungskonfigurationen und Netzwerkkomponenten oder AWS Marketplace Produktpaketen. Ein Produkt kann eine einzelne Recheninstanz sein, auf der AWS Linux ausgeführt wird, eine vollständig konfigurierte mehrstufige Webanwendung, die in einer eigenen Umgebung läuft, oder etwas dazwischen.

Sie erstellen ein Produkt, indem Sie eine AWS CloudFormation Vorlage importieren. AWS CloudFormation Vorlagen definieren die für das Produkt erforderlichen AWS Ressourcen, die Beziehungen zwischen Ressourcen und die Parameter, die Endbenutzer eingeben können, wenn sie das Produkt starten, um Sicherheitsgruppen zu konfigurieren, Schlüsselpaare zu erstellen und andere Anpassungen vorzunehmen.

## HashiCorp Unterstützung für Terraform Open Source und Terraform Cloud

AWS Service Catalog ermöglicht eine schnelle Self-Service-Bereitstellung mit integrierter Steuerung für Ihre HashiCorp Terraform Open Source- und Terraform Cloud-Konfigurationen. AWS Sie können Service Catalog als ein einziges Tool verwenden, um Ihre Terraform-Konfigurationen innerhalb eines großen Maßstabs zu organisieren, zu verwalten und zu verteilen. AWS Sie können auf die wichtigsten Funktionen von Service Catalog zugreifen, darunter die Katalogisierung standardisierter und vorab genehmigter Terraform-Vorlagen, Zugriffskontrolle, Bereitstellung mit geringsten Rechten, Versionierung, Tagging und gemeinsame Nutzung für Tausende von Konten. AWS 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.

Um mehr zu erfahren und ein Terraform-Produkttutorial zu vervollständigen, lesen Sie diesen Artikel. Erste Schritte mit einem Terraform-Produkt

## Bereitgestellte Produkte

AWS CloudFormation Stacks erleichtern die Verwaltung des Lebenszyklus Ihres Produkts, indem Sie es Ihnen ermöglichen, Ihre Produktinstanz als einzelne Einheit bereitzustellen, zu kennzeichnen, zu aktualisieren und zu beenden. Ein AWS CloudFormation Stack umfasst eine AWS CloudFormation Vorlage, die entweder im JSON- oder YAML-Format geschrieben ist, und die zugehörige Sammlung von Ressourcen. Ein bereitgestelltes Produkt ist ein Stack. Wenn ein Endbenutzer ein Produkt startet, ist die Instanz des Produkts, die von Service Catalog bereitgestellt wird, ein Stapel mit den

Ressourcen, die für die Ausführung des Produkts erforderlich sind. Weitere Informationen finden Sie im AWS CloudFormation -Benutzerhandbuch.

## Portfolios

Ein Portfolio ist eine Sammlung von Produkten, die Konfigurationsinformationen enthält. Portfolios erleichtern das Verwalten der zulässigen Benutzer und Nutzungsarten bestimmter Produkte. Mit Service Catalog können Sie ein maßgeschneidertes 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 mit anderen AWS Konten teilen und dem Administrator dieser Konten die Verteilung Ihrer Portfolios mit zusätzlichen Einschränkungen ermöglichen, z. B. einschränken, welche EC2 Instanzen 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. Dieser Ansatz ermöglicht es Ihnen, neue Versionen von Vorlagen und zugehörigen Ressourcen auf der Grundlage von Softwareupdates oder Konfigurationsänderungen hinzuzufügen.

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 kontrollieren, 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 diese Rolle, um die Cloud-Ressourcen des Produkts mithilfe AWS CloudFormation von zu

starten. Indem Sie jedem Produkt eine IAM-Rolle zuweisen, können Sie verhindern, dass Benutzer Berechtigungen für nicht genehmigte Vorgänge erhalten, und es ihnen ermöglichen, Ressourcen mithilfe des Katalogs bereitzustellen.

## Beschränkungen

Einschränkungen regeln die Art und Weise, 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: Einschränkungen bei der Markteinführung, Einschränkungen bei Benachrichtigungen und Einschränkungen bei Vorlagen.

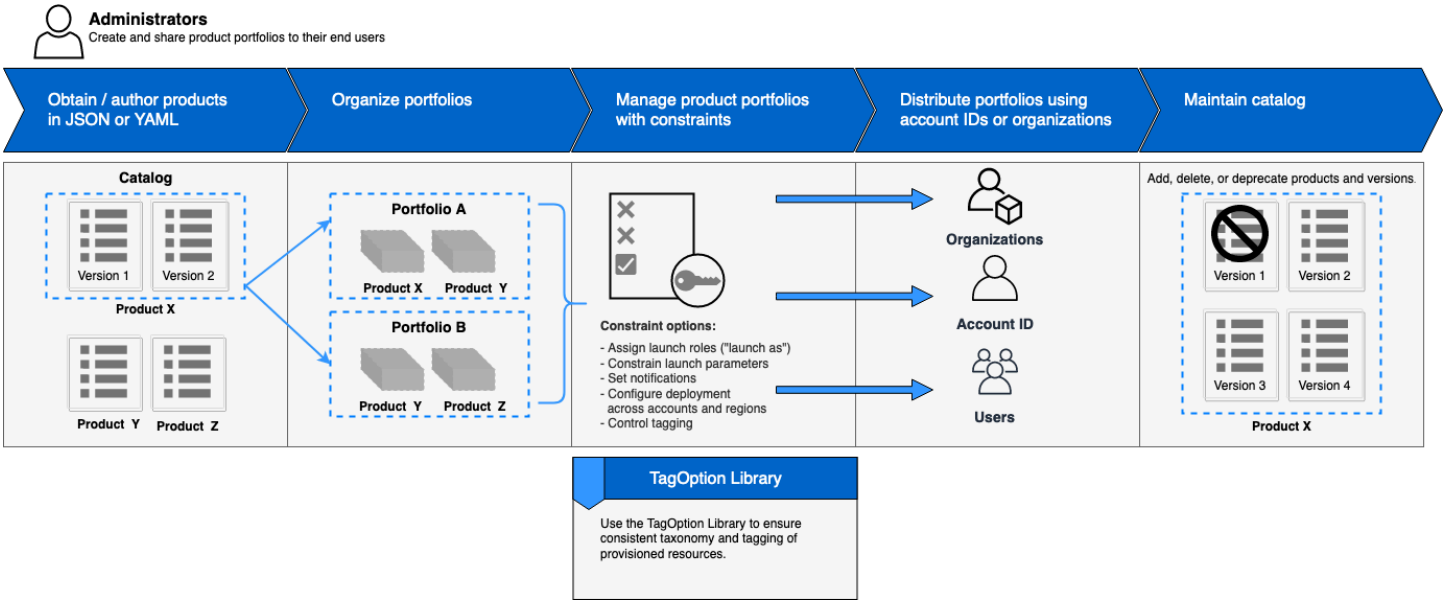
Mit Starteinschränkungen können Sie eine Rolle für ein Produkt im Portfolio festlegen. Verwenden Sie diese Rolle, um die Ressourcen beim Start bereitzustellen, sodass Sie Benutzerberechtigungen einschränken können, ohne die Fähigkeit der Benutzer zu beeinträchtigen, Produkte aus dem Katalog bereitzustellen.

Mit Benachrichtigungsbeschränkungen können Sie mithilfe eines Amazon SNS SNS-Themas Benachrichtigungen über Stack-Ereignisse erhalten.

Template-Einschränkungen schränken die Konfigurationsparameter ein, die dem Benutzer beim Starten des Produkts zur Verfügung stehen (z. B. 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.

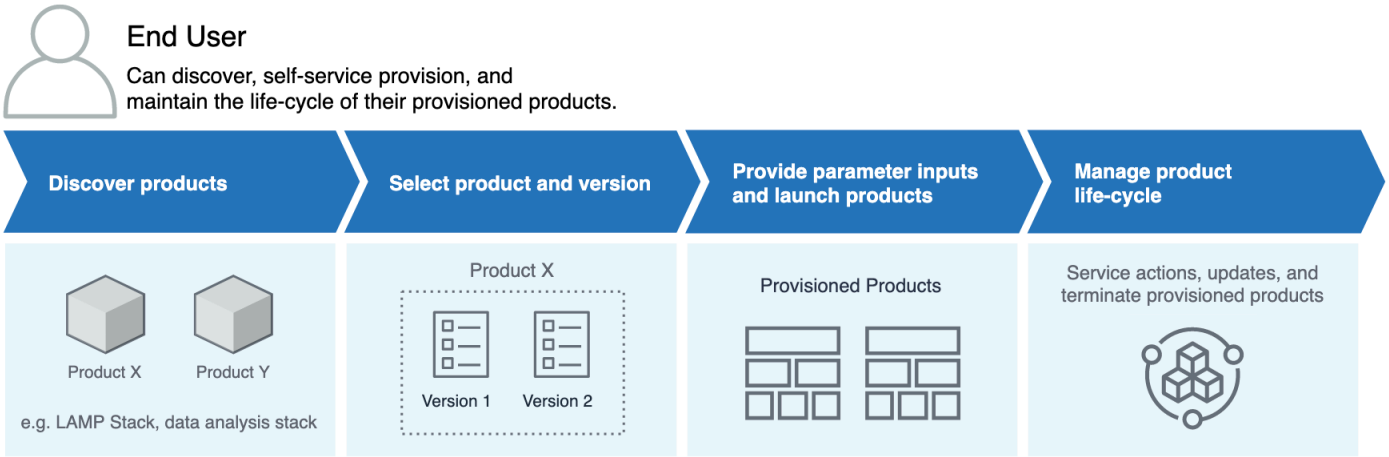
## Anfänglicher Administrator-Workflow

Dieses Diagramm zeigt den anfänglichen Arbeitsablauf eines Administrators zur Erstellung eines Katalogs.




## Anfänglicher Endbenutzer-Workflow

Dieses Diagramm zeigt den anfänglichen Arbeitsablauf für einen Endbenutzer.




# AWS Service Catalog Standard-Servicekontingente

Ihr AWS Konto hat die folgenden Standardkontingente für Einschränkungen AWS Organizations, Portfolio, Produkt, bereitgestelltes Produkt, Region, Serviceaktion und TagOptions.

## 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 eines Benutzers 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/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Ein Teil des Anmeldevorgangs umfasst den Empfang eines Telefonanrufs oder einer Textnachricht und die Eingabe eines Bestätigungscodes auf der Telefontastatur.

   Wenn Sie sich für eine anmelden AWS-Konto, wird eine Root-Benutzer des AWS-Kontoserstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

## Erstellen eines Benutzers 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 eines Benutzers 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 Administratorbenutzer im IAM Identity Center Benutzerzugriff.

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

Anmelden als Administratorbenutzer

- 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 Access-Portal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

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

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

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center Benutzerhandbuch.

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 Anleitung unter Eine Rolle für einen externen Identitätsanbieter (Verbund) erstellen im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Befolgen Sie die Anleitung unter Eine Rolle für einen IAM-Benutzer erstellen 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.

# Gewähren Sie AWS Service Catalog Administratoren Berechtigungen

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 Startbeschränkungen zur Definition der IAM-Rollen, die beim Starten von AWS Service Catalog Produkten durch Endbenutzer übernommen werden
- Gewähren von Zugriff auf Ihre Produkte für Endbenutzer

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

So weisen Sie einem Katalogadministrator Berechtigungen zu

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
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 Beispiel-Richtlinie und fügen Sie sie in das Dokument für die Richtlinie 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: Tags aus.

d. (Optional) Wählen Sie Tag hinzufügen aus, 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. Das erleichtert das Identifizieren und Organisieren von Ressourcen und die Suche danach. Weitere Informationen finden Sie im Allgemeine AWS-Referenz Referenzhandbuch unter AWS Ressourcen taggen.

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 gewähren, die in Amazon S3 AWS Service Catalog gespeichert sind. Weitere Informationen finden Sie unter Beispiele für Benutzerrichtlinien im Amazon Simple Storage Service-Benutzerhandbuch.

   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.

# Erteilen Sie AWS Service Catalog Endbenutzern Berechtigungen

Bevor der Endbenutzer es verwenden kann AWS Service Catalog, müssen Sie Zugriff auf die AWS Service Catalog Endbenutzer-Konsolenansicht 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 einer IAM-Gruppe hinzu.

So erteilen Sie einer Endbenutzer-Gruppe Berechtigungen

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

   a. Geben Sie als Benutzergruppenname den Text ein**`Endusers`**.

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

   c. Wählen Sie das Kontrollkästchen für die **`AWSServiceCatalogEndUserFullAccess`**Richtlinie aus. 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 Sie die Terraform Provisioning Engine

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

## Bestimmung der Warteschlange

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

- Die Provisioning-Engine befindet sich im Konto des Produktbesitzers
- Die Provisioning-Engine befindet sich in derselben Region, in der der Anruf getätigt wurde AWS Service Catalog
- Die Warteschlangen der Provisioning Engine folgen dem unten aufgeführten dokumentierten Benennungsschema

Wenn beispielsweise `us-east-1` vom Konto 1111111111 mit einem Produkt aufgerufen ProvisionProduct wird, das mit dem Konto 0000000000000 erstellt wurde, wird davon ausgegangen, AWS Service Catalog dass es sich um den richtigen SQS-ARN handelt. `arn:aws:sqs:us-east-1:0000000000000:ServiceCatalogTerraformOSProvisionOperationQueue`

Dieselbe Logik gilt für die Lambda-Funktion, die von `DescribeProvisioningParameters` aufgerufen wird.

## Confused Deputy zu Ihrer Terraform-Provisioning-Engine hinzufügen

### Confused Deputy: Kontexttasten auf den Endpunkten, um den Zugriff für Operationen einzuschränken **`lambda:Invoke`**

Die von AWS Service Catalog-bereitgestellten Engines erstellte Lambda-Funktion für den Parameterparser verfügt über eine Zugriffsrichtlinie, die nur dem Dienstprinzipal kontenübergreifende `lambda:Invoke` Berechtigungen gewährt: AWS Service Catalog

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

Dies sollte die einzige Berechtigung sein, die erforderlich ist, damit die Integration mit AWS Service Catalog ordnungsgemäß funktioniert. Sie können dies jedoch mithilfe des Kontextschlüssels `aws:SourceAccount` Confused Deputy weiter einschränken. Wenn Nachrichten AWS Service Catalog an diese Warteschlangen gesendet werden, wird der Schlüssel mit der AWS Service Catalog ID des Bereitstellungskontos aufgefüllt. Dies ist hilfreich, wenn Sie beabsichtigen, Produkte per Portfolio-Sharing zu vertreiben und sicherstellen möchten, dass nur bestimmte Konten Ihre Engine verwenden.

Sie können Ihre Engine beispielsweise so einschränken, dass sie nur Anfragen zulässt, die von 000000000000 und 111111111111 stammen, indem Sie die unten dargestellte 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"]
        }
      }
    }
  ]
}
```

## Confused Deputy-Kontexttasten auf den Endpunkten, um den Zugriff für Operationen einzuschränken `sqs:SendMessage`

Die von AWS Service Catalog-bereitgestellten Engines erstellten Amazon SQS SQS-Warteschlangen für Bereitstellungsvorgänge verfügen über eine Zugriffsrichtlinie, die kontoübergreifende `sqs:SendMessage` (und zugehörige KMS-) Berechtigungen nur dem Service Principal gewährt: AWS Service Catalog

```
{
      "Version": "2008-10-17",
      "Statement": [
        {
          "Sid": "Enable AWS Service Catalog to send messages to the queue",
          "Effect": "Allow",
          "Principal": {
            "Service": "servicecatalog.amazonaws.com"
          },
          "Action": "sqs:SendMessage",
```

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

Dies sollte die einzige Genehmigung sein, die erforderlich ist, damit die Integration ordnungsgemäß funktioniert. AWS Service Catalog Sie können dies jedoch mithilfe des Kontextschlüssels `aws:SourceAccount` Confused Deputy weiter einschränken. Wenn Nachrichten AWS Service Catalog an diese Warteschlangen gesendet werden, AWS Service Catalog füllt die Schlüssel mit der ID des Bereitstellungskontos auf. Dies ist hilfreich, wenn Sie beabsichtigen, Produkte per Portfolio-Sharing zu vertreiben und sicherstellen möchten, dass nur bestimmte Konten Ihre Engine verwenden.

Sie können Ihre Engine beispielsweise so einschränken, dass sie nur Anfragen zulässt, die von 000000000000 und 111111111111 stammen, indem Sie die unten dargestellte 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 damit beginnen, AWS Service Catalog indem Sie eine der gut gestalteten Produktvorlagen in der Bibliothek „Erste Schritte“ verwenden oder die Schritte in einem der Tutorials für die ersten Schritte befolgen.

In diesem Tutorial führen Sie Aufgaben als Katalogadministrator und Endbenutzer aus. Als Katalogadministrator erstellen Sie ein Portfolio und anschließend ein Produkt. Als Endbenutzer stellen Sie sicher, dass Sie auf die Endbenutzerkonsole zugreifen und das Produkt starten können. Bei dem Produkt handelt es sich um eines der folgenden Produkte:

- Eine Cloud-Entwicklungsumgebung, die auf Amazon Linux läuft und auf einer AWS CloudFormation Vorlage basiert, die die AWS Ressourcen definiert, die das Produkt verwenden kann.
- Eine Open-Source-Umgebung, die auf einer Terraform-Provisioning-Engine läuft und auf einer Konfigurationsdatei tar.gz basiert, die die AWS Ressourcen definiert, die das Produkt verwenden kann.

> **Note**
>
> Bevor Sie beginnen, stellen Sie sicher, dass Sie die Aktionspunkte in abgeschlossen haben. Einrichten AWS Service Catalog

Themen


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


## Bibliothek „Erste Schritte“

AWS Service Catalog bietet eine Bibliothek „Erste Schritte“ mit gut gestalteten Produktvorlagen, sodass 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 zur Verwendung AWS CloudFormation von Vorlagen. Weitere Informationen finden Sie unter Steuern des Zugriffs 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 Well-Architected-Framework finden Sie unter AWS Well-Architected.

# Erste Schritte mit einem AWS CloudFormation Produkt

Sie können damit beginnen, AWS Service Catalog indem Sie eine der gut gestalteten Produktvorlagen in der Bibliothek „Erste Schritte“ verwenden oder die Schritte im Tutorial „Erste Schritte“ befolgen.

In diesem Tutorial führen Sie Aufgaben als Katalogadministrator und Endbenutzer aus. Als Katalogadministrator erstellen Sie ein Portfolio und anschließend ein Produkt. Als Endbenutzer stellen Sie sicher, dass Sie auf die Endbenutzerkonsole zugreifen und das Produkt starten können. Das Produkt ist eine Cloud-Entwicklungsumgebung, die auf Amazon Linux läuft und auf einer AWS CloudFormation Vorlage basiert, die die AWS Ressourcen definiert, die das Produkt verwenden kann.

> **Note**
>
> Bevor Sie beginnen, stellen Sie sicher, dass Sie die Aktionspunkte in abgeschlossen habenEinrichten AWS Service Catalog.

Themen

- Schritt 1: Laden Sie die AWS CloudFormation Vorlage herunter

- Schritt 2: Erstellen eines Schlüsselpaares
- Schritt 3: Erstellen Sie ein Portfolio
- Schritt 4: Erstellen Sie ein neues Produkt im Portfolio
- Schritt 5: Fügen Sie eine Vorlagenbeschränkung hinzu, um die Instanzgröße zu begrenzen
- Schritt 6: Fügen Sie eine Startbeschränkung hinzu, um eine IAM-Rolle zuzuweisen
- Schritt 7: Gewähren Sie Endbenutzern Zugriff auf das Portfolio
- Schritt 8: Testen Sie die Endbenutzererfahrung


## Schritt 1: Laden Sie die AWS CloudFormation Vorlage herunter

Sie können AWS CloudFormation Vorlagen 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 zur Verfügung, damit Sie loslegen können. Die Vorlage startet eine einzelne Linux-Instanz, die für den SSH-Zugriff konfiguriert ist.

> **Note**
>
> Für die Verwendung von AWS CloudFormation Vorlagen sind spezielle Berechtigungen erforderlich. Bevor Sie beginnen, stellen Sie sicher, dass Sie über die richtigen Berechtigungen verfügen. Weitere Informationen zu den Voraussetzungen finden Sie unterBibliothek „Erste Schritte“.

### Herunterladen der Vorlage

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

### 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 zur Erstellung dieser Vorlage verwendet wurde. Die neueste Version des Vorlagenformats ist 2010-09-09 und ist derzeit der einzig 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 AWS Service Catalog Einschränkungen verwenden.

  Mit dem `KeyName` Parameter können Sie einen Namen für das Amazon Elastic Compute Cloud (Amazon EC2) -Schlüsselpaar angeben, den Endbenutzer angeben müssen, wenn sie Ihr Produkt AWS Service Catalog auf den Markt bringen. Das Schlüsselpaar erstellen Sie im nächsten Schritt.
- Metadaten (optional) — Objekte, die zusätzliche Informationen zur Vorlage bereitstellen. Der Schlüssel AWS::CloudFormation: :Interface definiert, wie die Endbenutzer-Konsolenansicht

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 einer Nachschlagetabelle. Sie können einen Schlüssel einem entsprechenden Wert zuordnen, indem Sie die systemeigene Funktion Fn::FindInMap in den Abschnitten Ressourcen und Ausgaben verwenden. Die obige Vorlage enthält eine Liste der 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 soll AWS Management Console.
- Ressourcen (erforderlich) — Stack-Ressourcen und ihre Eigenschaften. Sie können in den Abschnitten Ressourcen und Ausgaben der Vorlage auf Ressourcen verweisen. In der obigen Vorlage geben wir eine EC2 Instance an, auf der Amazon Linux ausgeführt wird, und eine Sicherheitsgruppe, die den SSH-Zugriff auf die Instance ermöglicht. Der Abschnitt Eigenschaften der EC2 Instance-Ressource verwendet die Informationen, die der Benutzer eingibt, um den Instance-Typ und einen Schlüsselnamen für den SSH-Zugriff zu konfigurieren.

  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 den Benutzer darüber informiert, wann die Produkteinführung 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 „Aufbau der Vorlage“ 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 EC2 Amazon-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 Key Pairs im  EC2 Amazon-Benutzerhandbuch.

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

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

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 Sie ein Portfolio fortfahren. Führen Sie andernfalls die folgenden Schritte aus.

So erstellen Sie ein Schlüsselpaar

1. Öffnen Sie die EC2 Amazon-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 Sie ein Portfolio

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`**
   - Beschreibung des Portfolios — **`Sample portfolio that contains a single product.`**
   - Besitzer — **`IT (it@example.com)`**
4. Wählen Sie Create (Erstellen) aus.

## Schritt 4: Erstellen Sie ein neues Produkt im Portfolio

Nachdem Sie ein Portfolio erstellt haben, sind Sie bereit, ein Produkt innerhalb des Portfolios zu erstellen. In diesem Tutorial erstellen Sie innerhalb des Engineering Tool-Portfolios ein Produkt namens Linux Desktop, eine Cloud-Entwicklungsumgebung, die auf Amazon Linux läuft.

Um ein Produkt innerhalb eines Portfolios zu erstellen

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

- Product name – **`Linux Desktop`**
- Beschreibung des Produkts — **`Cloud development environment configured for engineering staff. Runs AWS Linux.`**
- Besitzer — **`IT`**
- Vertriebspartner — (leer)

5. Wählen Sie auf der Seite mit den Versionsdetails die Option CloudFormation Vorlage verwenden aus. Wählen Sie dann Spezifizieren Sie eine Amazon S3 S3-Vorlagen-URL und geben Sie Folgendes ein:

   - Select template – **`https://awsdocs.s3.amazonaws.com/servicecatalog/development-environment.template`**
   - Titel der Version — **`v1.0`**
   - Description (Beschreibung) – **`Base Version`**

6. Geben Sie im Abschnitt Support-Details Folgendes ein:

   - E-Mail-Kontakt — **`ITSupport@example.com`**
   - Link zur Support — **`https://wiki.example.com/IT/support`**
   - Beschreibung des Support — **`Contact the IT department for issues deploying or connecting to this product.`**

7. Wählen Sie Produkt erstellen.

## 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 AWS Service Catalog Einschränkungen verwenden.

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 EC2 Amazon-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: Fügen Sie eine Startbeschränkung hinzu, um eine IAM-Rolle zuzuweisen

Eine Startbeschränkung bezeichnet eine IAM-Rolle, die übernommen AWS Service Catalog wird, wenn ein Endbenutzer ein Produkt auf den Markt bringt.

In diesem Schritt fügen Sie dem Linux Desktop-Produkt eine Startbeschränkung hinzu, sodass Sie die IAM-Ressourcen verwenden AWS Service Catalog können, aus denen sich die Produktvorlage zusammensetzt. AWS CloudFormation

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

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

Diese Startbeschränkung 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 eine Startbeschränkung müssen Sie Ihren Endbenutzern zusätzliche IAM-Berechtigungen gewähren, bevor sie das Linux Desktop-Produkt verwenden können. Die `ServiceCatalogEndUserAccess` Richtlinie gewährt beispielsweise die IAM-Mindestberechtigungen, die für den Zugriff auf die Konsolenansicht für AWS Service Catalog Endbenutzer erforderlich sind.

Durch die Verwendung einer Startbeschränkung können Sie sich an die bewährte IAM-Methode halten, die IAM-Berechtigungen für Endbenutzer 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`— Erlaubt AWS Service Catalog volle Berechtigungen zum Erstellen, Lesen, Aktualisieren, Löschen, Auflisten und Markieren von AWS CloudFormation Stacks.
   - `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 ordnet die angegebene verwaltete Richtlinie der angegebenen IAM-Rolle zu.
   - `s3`— Ermöglicht den Zugriff auf Amazon S3 S3-Buckets im Besitz von AWS Service Catalog. Um das Produkt bereitzustellen, ist Zugriff auf Bereitstellungsartefakte AWS Service Catalog erforderlich.

- `servicecatalog`— Erlaubt AWS Service Catalog Berechtigungen zum Auflisten, Lesen, Schreiben, Markieren und Starten von Ressourcen im Namen des Endbenutzers.
- `sns`— Erlaubt AWS Service Catalog Berechtigungen zum Auflisten, Lesen, Schreiben und Markieren von Amazon SNS SNS-Themen für die Startbeschränkung.

> **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“.
5. Geben Sie auf der Seite „Richtlinie überprüfen“ als Namen den Text ein**`linuxDesktopPolicy`**.
6. Wählen Sie Create Policy (Richtlinie erstellen) aus.
7. Wählen Sie im Navigationsbereich Rollen. Wählen Sie dann Rolle erstellen und gehen Sie wie folgt vor:
   a. Wählen Sie für Vertrauenswürdige Entität auswählen die Option AWS Dienst und dann unter Anwendungsfall für andere AWS Dienste die Option Service Catalog aus. Wählen Sie den Anwendungsfall Service Catalog aus und klicken Sie dann auf Weiter.
   b. Suchen Sie nach der linuxDesktopPolicyRichtlinie und aktivieren Sie dann das Kontrollkästchen.
   c. Wählen Sie Weiter.
   d. Geben Sie für Role name (Rollenname) **`linuxDesktopLaunchRole`** ein.
   e. Wählen Sie Rolle erstellen.
8. Öffnen Sie die AWS Service Catalog Konsole unter https://console.aws.amazon.com/servicecatalog.
9. Wählen Sie das Portfolio Engineering Tools aus.
10. Wählen Sie auf der Seite mit den Portfoliodetails die Registerkarte Einschränkungen und dann Einschränkung erstellen aus.
11. Wählen Sie für Produkt die Option Linux Desktop und für Einschränkungstyp die Option Launch aus.
12. Wählen Sie „IAM-Rolle auswählen“. Wählen Sie als Nächstes linuxDesktopLaunchRolle und anschließend Erstellen aus.

## Schritt 7: Gewähren Sie Endbenutzern Zugriff auf das Portfolio

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

Voraussetzungen

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

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.

## Schritt 8: Testen Sie die Endbenutzererfahrung

Um sicherzustellen, dass der Endbenutzer erfolgreich auf die Endbenutzerkonsole zugreifen und Ihr Produkt starten kann, melden Sie sich 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 Portfolio erstellt haben. `Engineering Tools` Wählen Sie für dieses Tutorial die Region us-east-1 aus.
3. Öffnen Sie die AWS Service Catalog Konsole 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.

Um zu überprüfen, ob der Endbenutzer das Linux Desktop-Produkt starten kann

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

1. Wählen Sie im Bereich 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 den **`Linux-Desktop`** 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 zuzulassen, dann Ihre IP-Adresse, gefolgt von, **`/32`** um den Zugriff nur auf Ihre IP-Adresse oder etwas dazwischen zu beschränken.
5. Wählen Sie Produkt starten, um den Stack zu starten. Die Konsole zeigt die Stack-Detailseite für den Linux-Desktop-Stack an. Der ursprüngliche Status des Produkts lautet In Bearbeitung. Die Markteinführung des Produkts dauert mehrere Minuten. AWS Service Catalog Aktualisieren Sie den Browser, um den aktuellen Status anzuzeigen. Nach der Markteinführung lautet der Status A verfügbar.

## Erste Schritte mit einem Terraform-Produkt

AWS Service Catalog ermöglicht eine schnelle Self-Service-Bereitstellung mit integrierter Steuerung Ihrer HashiCorp Terraform-Konfigurationen. AWS Sie können es AWS Service Catalog als ein einziges Tool verwenden, um Ihre Terraform-Konfigurationen nach eigenem Ermessen zu organisieren, zu verwalten und zu verteilen. AWS AWS Service Catalog unterstützt Terraform in mehreren wichtigen Funktionen, darunter die Katalogisierung standardisierter und vorab genehmigter Terraform-Vorlagen, Zugriffskontrolle, Versionierung, Tagging und gemeinsame Nutzung für andere Konten. AWS In sehen Ihre Endbenutzer eine einfache Liste der Produkte und Versionen AWS 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, wurden aufgrund der jüngsten Lizenzänderungen für Terraform alle früheren Verweise von Terraform Open Source auf External AWS Service Catalog geändert. Der Produkttyp External umfasst Unterstützung für die Terraform Community Edition, früher bekannt als Terraform Open Source. Weitere Informationen und Anweisungen zur Migration Ihrer vorhandenen Terraform Open Source-Produkte und bereitgestellten Produkte auf den Produkttyp External finden Sie unter.

Aktualisierung vorhandener Terraform Open Source-Produkte und bereitgestellter Produkte auf den Produkttyp External

Die Schritte im folgenden Tutorial helfen Ihnen bei den ersten Schritten mit einem Terraform-Produkt in. AWS Service Catalog

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

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

- Erstellen Sie ein Terraform-Produkt mit dem Produkttyp Terraform Cloud oder External. Service Catalog verwendet den Produkttyp External zur Unterstützung von Terraform Community Edition-Produkten.
- Ordnen Sie das Produkt einem Portfolio zu
- Erstellen Sie eine Beschränkung für die Markteinführung, damit Ihre Endbenutzer das Produkt bereitstellen können
- Kennzeichnen Sie das Produkt
- Teilen Sie das Portfolio und das Terraform-Produkt mit dem Endbenutzerkonto (Spoke-Konto)

Im Tutorial teilen Sie ein Portfolio mithilfe der Option zum Teilen von Organisationen über das Admin-Hub-Konto, das auch das Verwaltungskonto der Organisation ist. Weitere Informationen zur gemeinsamen Nutzung von Organisationen finden Sie unterFreigeben eines Portfolios.

Die AWS Ressource, die in dem Terraform-Produkt enthalten ist, das Sie im Tutorial erstellen, ist ein einfacher Amazon S3 S3-Bucket.

> **Note**
>
> Bevor Sie beginnen, stellen Sie sicher, dass Sie die Aktionspunkte in abgeschlossen haben. Einrichten AWS Service Catalog

Themen

- Aktualisierung vorhandener Terraform Open Source-Produkte und bereitgestellter Produkte auf den Produkttyp External
- Voraussetzung: Konfigurieren Sie Ihre Terraform-Provisioning-Engine
- Schritt 1: Herunterladen der Terraform-Konfigurationsdatei
- Schritt 2: Erstellen Sie ein Terraform-Produkt
- Schritt 3: Erstellen Sie ein AWS Service Catalog Portfolio
- Schritt 4: Produkt zum Portfolio hinzufügen
- Schritt 5: Startrollen erstellen
- Schritt 6: Fügen Sie Ihrem Terraform-Produkt eine Startbeschränkung hinzu
- Schritt 7: Endbenutzerzugriff gewähren
- Schritt 8: Portfolio mit Endbenutzern teilen
- Schritt 9: Testen Sie die Endbenutzererfahrung
- Schritt 10: Überwachung der Terraform-Bereitstellungsvorgänge


## Aktualisierung vorhandener Terraform Open Source-Produkte und bereitgestellter Produkte auf den Produkttyp External

Um die Unterstützung von HashiCorp Technologien fortzusetzen, wurden aufgrund der jüngsten Lizenzänderungen für Terraform alle früheren Verweise von Terraform Open AWS Service Catalog Source auf External geändert. Der Produkttyp External umfasst Unterstützung für die Terraform Community Edition, früher bekannt als Terraform Open Source. AWS Service Catalog unterstützt Terraform Open Source nicht mehr als gültigen Produkttyp für neue Produkte oder bereitgestellte Produkte. Sie können nur bestehende Terraform Open Source-Ressourcen aktualisieren oder kündigen, einschließlich Produktversionen und bereitgestellter Produkte.

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

1. Aktualisieren Sie Ihre bestehende Terraform Reference Engine, sodass AWS Service Catalog sie sowohl externe als auch Terraform Open Source-Produkttypen unterstützt. Anweisungen zur Aktualisierung Ihrer Terraform Reference Engine finden Sie in unserem Repository. GitHub
2. Erstellen Sie alle vorhandenen Terraform Open Source-Produkte mit dem neuen externen Produkttyp neu.

3. Löschen Sie alle vorhandenen Produkte, die den Terraform Open Source-Produkttyp 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 Konfigurationsdatei tar.gz verwenden.

AWS Service Catalog wird Kunden bei Bedarf bei dieser Änderung unterstützen. Wenn diese Änderungen einen großen Aufwand für Ihr Konto erfordern oder sich auf kritische Produktauslastungen auswirken, wenden Sie sich an Ihren Kundenbetreuer, um Unterstützung zu erhalten.

## Voraussetzung: Konfigurieren Sie Ihre Terraform-Provisioning-Engine

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

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

### Provisioning-Engine für die Terraform Community Edition (externer Produkttyp)

AWS Service Catalog verwendet den Produkttyp External zur Unterstützung von Terraform Community Edition-Produkten. Der Produkttyp External unterstützt je nach Konfiguration der Provisioning-Engine auch andere Provisioning-Tools, darunter Pulumi, Ansible, Chef und mehr.

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

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

- Erforderliche Installationstools
- Den Code erstellen
- Bereitstellung 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 HashiCorp Terraform Cloud verwenden, müssen Sie eine Terraform Provisioning Engine in Ihrem Administratorkonto (Hub-Konto) installieren und konfigurieren. AWS Service Catalog HashiCorp verwaltet diese Engine in einer Remote-Umgebung.

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

- Erforderliche Installationstools
- Den Code erstellen
- Bereitstellung auf einem AWS Konto
- Zusätzliche Informationen zu Bereitstellungsworkflows, Qualitätssicherung und Einschränkungen

## Schritt 1: Herunterladen der Terraform-Konfigurationsdatei

Sie können eine Terraform-Konfigurationsdatei verwenden, um Terraform-Produkte zu erstellen und bereitzustellen. HashiCorp Diese Konfigurationen sind reine Textdateien 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 Datei tar.gz hochladen. In diesem Tutorial finden Sie eine AWS Service Catalog einfache Konfigurationsdatei, mit der Sie loslegen können. Die Konfiguration erstellt einen Amazon S3 S3-Bucket.

## Laden Sie die Konfigurationsdatei herunter

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

## Überblick über die Konfigurationsdatei

Der Text der Beispielkonfigurationsdatei lautet wie 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
}
```

### Ressourcen zur Konfiguration

In der Konfigurationsdatei werden die Ressourcen deklariert, die bei AWS Service Catalog der Bereitstellung des Produkts erstellt werden sollen. 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 Schlüsselwort variable 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 um innerhalb des Moduls auf den Wert der Variablen zu verweisen.
- Anbieter (optional) — Der Cloud-Dienstanbieter für die Bereitstellung von Ressourcen, d. h. `AWS` AWS Service Catalog unterstützt nur `AWS` als Anbieter. Infolgedessen überschreibt die Terraform-Provisioning-Engine alle anderen aufgelisteten Anbieter. `AWS`
- Ressource (erforderlich) — Die AWS Infrastrukturressource für die Bereitstellung. Für dieses Tutorial spezifiziert die Terraform-Konfigurationsdatei Amazon S3.

- Ausgabe (optional) — Die zurückgegebenen Informationen oder der zurückgegebene Wert, ähnlich den zurückgegebenen Werten in einer Programmiersprache. Sie können Ausgabedaten verwenden, um den Infrastruktur-Workflow mit Automatisierungstools zu konfigurieren.

## Schritt 2: Erstellen Sie ein Terraform-Produkt

Nach der Installation der Terraform Provisioning Engine können Sie in ein Terraform-Produkt erstellen. HashiCorp AWS Service Catalog In diesem Tutorial erstellen Sie ein Terraform-Produkt, das einen einfachen Amazon S3 S3-Bucket enthält.

Um ein Terraform-Produkt zu erstellen

1. Öffnen Sie die AWS Service Catalog Konsole unter https://console.aws.amazon.com/servicecatalog/und melden Sie sich als Admin-Benutzer 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 Extern oder Terraform Cloud aus. Service Catalog verwendet den Produkttyp External zur Unterstützung von Terraform Community Edition-Produkten.
5. Geben Sie die folgenden Produktdetails ein:
   - Product name – **`Simple S3 bucket`**
   - Produktbeschreibung — Terraform-Produkt, das einen Amazon S3 S3-Bucket enthält.
   - Besitzer — **`IT`**
   - Vertriebspartner — (leer)
6. Wählen Sie im Bereich Versionsdetails die Option Vorlagendatei hochladen und dann Datei auswählen aus. Wählen Sie die Datei aus, in die Sie heruntergeladen habenSchritt 1: Herunterladen der Terraform-Konfigurationsdatei.
7. Geben Sie Folgendes ein:
   - Versionsname — **`v1.0`**
   - Beschreibung der Version — **`Base Version`**
8. Geben Sie im Abschnitt Support-Details Folgendes ein und wählen Sie dann Produkt erstellen aus.
   - E-Mail-Kontakt — **`ITSupport@example.com`**

- Link zur Support — **`https://wiki.example.com/IT/support`**
- Beschreibung des Support — **`Contact the IT department for issues deploying or connecting to this product.`**

9. Wählen Sie Produkt erstellen.

Nach erfolgreicher Erstellung des Produkts wird auf der Produktseite ein Bestätigungsbanner AWS Service Catalog angezeigt.

## Schritt 3: Erstellen Sie ein AWS Service Catalog Portfolio

Sie können in Ihrem AWS Service Catalog Administratorkonto (Hub-Konto) ein Portfolio erstellen, um die Produktorganisation und Verteilung an Endbenutzerkonten (Spoke-Konten) zu vereinfachen.

So erstellen Sie ein Portfolio

1. Öffnen Sie die AWS Service Catalog Konsole 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`**
   - Beschreibung des Portfolios — **`Sample portfolio for Terraform configurations.`**
   - Besitzer — **`IT (it@example.com)`**
4. Wählen Sie Create (Erstellen) aus.

## Schritt 4: Produkt zum Portfolio hinzufügen

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

Um ein Produkt zu einem Portfolio hinzuzufügen

1. Navigieren Sie zur Seite mit der Produktliste.
2. Wählen Sie das Terraform-Produkt Simple S3 Bucket aus, das Sie in Schritt 2 erstellt haben, und wählen Sie dann Aktionen aus. Wählen Sie im Drop-down-Menü die Option Produkt zum

Portfolio hinzufügen aus. AWS Service Catalog zeigt den Bereich Simple S3-Bucket zum Portfolio hinzufügen an.

3. Wählen Sie das S3-Bucket-Portfolio aus und deaktivieren Sie dann Startbeschränkung erstellen. Sie werden die Startbeschränkung später im Tutorial erstellen.
4. Wählen Sie Produkt zum Portfolio hinzufügen.

Nach dem erfolgreichen Hinzufügen des Produkts zum Portfolio wird auf der Seite mit der Produktliste ein Bestätigungsbanner AWS Service Catalog angezeigt.

## Schritt 5: Startrollen erstellen

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

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

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

Um eine Startrolle im AWS Service Catalog Administratorkonto zu erstellen

1. Während Sie mit dem AWS Service Catalog Administratorkonto angemeldet sind, folgen Sie den Anweisungen zum Erstellen neuer Richtlinien auf der Registerkarte JSON im IAM-Benutzerhandbuch.
2. Erstellen Sie eine Richtlinie für Ihr einfaches Amazon S3 S3-Bucket Terraform-Produkt. Diese Richtlinie muss erstellt werden, bevor Sie die Startrolle erstellen. Sie besteht aus den folgenden Berechtigungen:

- `s3`— Erlaubt AWS Service Catalog volle Rechte zum Auflisten, Lesen, Schreiben, Bereitstellen und Markieren des Amazon S3 S3-Produkts.
- `s3`— Ermöglicht den Zugriff auf Amazon S3 S3-Buckets im Besitz von AWS Service Catalog. Um das Produkt bereitzustellen, ist Zugriff auf Bereitstellungsartefakte AWS Service Catalog erforderlich.
- `resourcegroups`— Ermöglicht AWS Service Catalog das Erstellen, Auflisten, Löschen und Markieren AWS Resource Groups.
- `tag`— Erlaubt 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.
   b. Wählen Sie „Weiter“, „Überprüfen“.
   c. Geben Sie auf der Seite „Richtlinie überprüfen“ als Namen den Text ein**`S3ResourceCreationAndArtifactAccessPolicy`**.
   d. Wählen Sie Create Policy (Richtlinie erstellen) aus.
4. Wählen Sie im Navigationsbereich Rollen und dann Rolle erstellen.
5. Wählen Sie für Vertrauenswürdige Entität auswählen die Option Benutzerdefinierte Vertrauensrichtlinie 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.
7. Wählen Sie in der Liste Richtlinien die, die `S3ResourceCreationAndArtifactAccessPolicy` Sie gerade erstellt haben.
8. Wählen Sie Weiter.
9. Geben Sie für Rollenname den Namen **`SCLaunch-S3product`** ein.

> **Important**
>
> Die Namen der Startrollen müssen mit "SCLaunch" beginnen, gefolgt vom gewünschten Rollennamen.

10. Wählen Sie Rolle erstellen.

> **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 enthalten wie die Rolle im Administratorkonto.

Um eine Startrolle im AWS Service Catalog Endbenutzerkonto zu erstellen

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

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

Nachdem Sie nun sowohl für das Administrator- als auch für das Endbenutzerkonto eine Startrolle erstellt haben, können Sie dem Produkt eine Startbeschränkung hinzufügen.

## Schritt 6: Fügen Sie Ihrem Terraform-Produkt eine Startbeschränkung hinzu

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

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

Diese Startbeschränkung 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 Startbeschränkung können Sie die IAM-Best-Practice-Methode befolgen und die IAM-Berechtigungen für Endbenutzer auf ein Minimum beschränken. Weitere Informationen finden Sie unter Gewähren von geringsten Rechten im IAM-Benutzerhandbuch.

Um dem Produkt eine Startbeschränkung zuzuweisen

1. Öffnen Sie die AWS Service Catalog Konsole 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 Simple S3 Bucket aus. AWS Service Catalog wählt automatisch den Einschränkungstyp Launch aus.
6. Wählen Sie „Rollennamen eingeben“ und anschließend „SCLaunch-S3Product“.
7. Wählen Sie Create.

> **Note**
>
> Der angegebene Rollenname muss in dem Konto vorhanden sein, das die Startbeschränkung erstellt hat, und im Konto des Benutzers, der ein Produkt mit dieser Startbeschränkung auf den Markt bringt.

## Schritt 7: Endbenutzerzugriff gewähren

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

In diesem Tutorial gewähren Sie Endbenutzern Zugriff, indem Sie den Prinzipalnamen teilen. 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 teilen, AWS Service

Catalog wird überprüft, ob diese Prinzipalnamen bereits vorhanden sind. Falls sie existieren, AWS Service Catalog werden die entsprechenden IAM-Prinzipale automatisch dem gemeinsamen Portfolio zugeordnet, um Endbenutzern Zugriff zu gewähren. Weitere Informationen finden Sie unter Ein Portfolio teilen.

Voraussetzungen

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

So erteilen Sie Zugriff auf das Portfolio

1. Navigieren Sie zur Portfolio-Seite 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 Prinzipalnamentyp aus, und geben Sie dann den Prinzipalnamen des gewünschten Endbenutzers im Spoke-Konto ein.
5. Wählen Sie Grant access (Zugriff gewähren).

## Schritt 8: Portfolio mit Endbenutzern teilen

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

Um das Portfolio vom Admin-Hub-Konto aus zu teilen

1. Öffnen Sie die AWS Service Catalog Konsole 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 AWS Organizationsund filtern Sie dann nach Ihrer Organisationsstruktur.
4. Wählen Sie im Bereich AWS Organisation das Endbenutzerkonto (Spoke-Konto) aus.

   Sie können auch einen Stammknoten auswählen, um das Portfolio mit der gesamten Organisation, einer übergeordneten Organisationseinheit (OU) oder einer untergeordneten

Organisationseinheit innerhalb Ihrer Organisation zu teilen, basierend auf Ihrer Organisationsstruktur. Weitere Informationen finden Sie unterFreigeben eines Portfolios.

5. Wählen Sie im Bereich Share-Einstellungen die Option Principal Sharing aus.
6. Wählen Sie Freigeben.

Nachdem das Portfolio erfolgreich für Endbenutzer freigegeben wurde, besteht der nächste Schritt darin, die Endbenutzererfahrung zu überprüfen und das Terraform-Produkt bereitzustellen.

## Schritt 9: Testen Sie die Endbenutzererfahrung

Um sicherzustellen, dass Endbenutzer erfolgreich auf die Endbenutzer-Konsolenansicht zugreifen und Ihr **`Simple S3 bucket`** Produkt starten können, melden Sie sich 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 Catalog Konsole 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.

Um zu überprüfen, ob der Endbenutzer das Terraform-Produkt starten kann

1. Wählen Sie im Bereich Produkte der Konsole Simple S3 Bucket aus.
2. Wählen Sie Produkt starten, um den Assistenten zu starten, der Ihr Produkt konfiguriert.
3. Geben Sie auf der Seite Launch Simple S3 Bucket den **`Amazon S3 product`** Namen des bereitgestellten Produkts 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 S3-Bucket an. Beispiel, **`terraform-s3-product`**.
5. Wählen Sie Produkt starten. Die Konsole zeigt die Stack-Detailseite für den Amazon S3 S3-Produktstart an. Der ursprüngliche Status des Produkts lautet Under Change. Die Markteinführung des Produkts dauert mehrere Minuten. AWS Service Catalog Aktualisieren Sie den Browser, um den aktuellen Status anzuzeigen. Nach einer erfolgreichen Produkteinführung lautet der Status Verfügbar.

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

## Schritt 10: Überwachung der Terraform-Bereitstellungsvorgänge

Wenn Sie die Bereitstellungsvorgänge überwachen möchten, können Sie die CloudWatch Amazon-Protokolle und AWS Step Functions alle Bereitstellungs-Workflows überprüfen.

Es gibt zwei Zustandsmaschinen für den Bereitstellungs-Workflow:

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

Um die Monitoring-State-Machine auszuführen

1. Öffnen Sie die AWS Managementkonsole und melden Sie sich als Administrator in dem Admin-Hub-Konto an, auf dem die Terraform Provisioning Engine installiert ist.
2. Öffnen Sie AWS Step Functions.
3. Wählen Sie im linken Navigationsbereich State Machines aus.
4. Wählen Sie ManageProvisionedProductStateMachine.
5. Geben Sie in der Liste der 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.

Auf der daraufhin angezeigten Seite mit den Ausführungsdetails können Sie alle Schritte des Provisioning-Workflows einsehen. 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).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- 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 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

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 AWS Service Catalog API oder auf andere AWS-Services Weise arbeiten oder diese verwenden. AWS CLI AWS SDKs 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 AWS Service Catalog APIs von Ihrer Amazon Virtual Private Cloud (Amazon VPC) aus 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 Private IPs in Ihrem ermöglicht. VPCs

# Identity and Access Management in AWS Service Catalog

Für den Zugriff auf sind Anmeldeinformationen AWS Service Catalog erforderlich. 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 Einschränkungen beim Start.

> **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 Einschränkungen beim Start.

## 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 *`administrative`* Berechtigungen, die vollen Zugriff auf die Ansicht der Administratorkonsole ermöglichen, und gewährt die Erlaubnis, Produkte und Portfolios zu erstellen und zu verwalten.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `servicecatalog`— Ermöglicht Principals uneingeschränkten Zugriff 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 *`read-only`* Berechtigungen, 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 *`contributor`* Berechtigungen, die vollen Zugriff auf die Konsolenansicht für Endbenutzer ermöglichen, und erteilt 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 Endbenutzerkonsole 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 *`read-only`* Berechtigungen, 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 die AWS Service Catalog Öffentlichkeit APIs.
- `codeconnections`— Erlaubt der Rolle „ AWS Service Catalog Artefaktsynchronisierung“ eingeschränkten öffentlichen ZugriffCodeConnections . APIs
- `cloudformation`— Erlaubt der Rolle „ AWS Service Catalog Artefaktsynchronisierung“ eingeschränkten öffentlichen Zugriff AWS CloudFormation . 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 dienstverknüpften Rollen finden Sie unter Dienstverknüpfte Rollen verwenden (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`— Erlaubt der AWS Service Catalog Datensynchronisierungsrolle eingeschränkten Zugriff auf die AWS Organizations Öffentlichkeit APIs.

Sehen Sie sich die Richtlinie an: AWSServiceCatalogOrgsDataSyncServiceRolePolicy.

Details zur dienstbezogenen Rolle

AWS Service Catalog verwendet die obigen 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 dienstverknüpften Rollen finden Sie unter Dienstverknüpfte Rollen verwenden (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 Organisationseinheit oder dem angegebenen Stammverzeichnis enthalten sind.
- `organizations:ListParents`— Ermöglicht der Rolle AWS Service Catalog Organizations Data Sync, das Stammverzeichnis oder die OUs , die als unmittelbare übergeordnete Einheit der angegebenen untergeordneten Organisationseinheit oder des angegebenen untergeordneten Kontos dienen, aufzulisten.
- `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— AWSServiceCatalogEndUserFullAccessStattdessen verwenden.
- ServiceCatalogEndUserAccess— AWSServiceCatalogEndUserReadOnlyAccessStattdessen verwenden.

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 ermöglich t. AWS Organizations Diese Richtlinie ermöglicht eingeschr änkten Zugriff auf AWS Service Catalog Aktionen (z. B. API-Aufrufe) und auf andere AWS Serviceaktionen, die AWS Service Catalog davon abhängen. | |
| AWSServiceCatalogA dminFullAccess— Verwaltete Richtlinie aktualisieren | AWS Service Catalog Die `AWSServiceCatalogA dminFullAccess` Richtlini e wurde aktualisiert, sodass sie alle Berechtigungen für den AWS Service Catalog Administrator enthält und die Kompatibilität mit gewährlei stet 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 Diensten, die dienstverknüpfte Rollen unterstützen, finden Sie unter AWS Dienste, die mit IAM funktionieren. Suchen Sie in der Spalte Dienstverknüpfte Rollen nach den Diensten, für die Ja steht. 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 dienstgebundene Rolle mit dem Namen verwenden **`AWSServiceRoleForServiceCatalogSync`**— Diese dienstverknüpfte Rolle ist erforderlich, um AWS Service Catalog Bereitstellungsartefakte für ein CodeConnections Produkt AWS Service Catalog zu verwenden 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 Teilen mit 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 dienstbezogene Rolle erneut für Sie erstellt.

## Bearbeiten einer serviceverknüpften Rolle für AWS Service Catalog

AWS Service Catalog erlaubt es 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 Dienstrolle 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. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, 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 zum Beispiel ein Szenario vor, in dem das Produkt den Start aller EC2 Amazon-Instances ermöglicht und das Portfolio zwei Einschränkungen hat: eine, die den Start aller EC2 Nicht-GPU-Instances ermöglicht, und eine, die nur den Start von t1.micro- und EC2 m1.small-Instances erlaubt. 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 Oberfläche 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
- AWS Service Catalog Einschränkungen verwenden
- AWS Service Catalog Serviceaktionen
- AWS Marketplace Produkte zu Ihrem Portfolio hinzufügen
- Benutzen AWS CloudFormation StackSets
- Verwalten von Budgets

# Verwalten von Portfolios

Portfolios werden auf der Portfolio-Seite in der AWS Service Catalog Administratorkonsole erstellt, angezeigt und aktualisiert.

Aufgaben

- Erstellen, Anzeigen und Löschen von Portfolios
- Anzeigen von Portfoliodetails
- Erstellen und Löschen von Portfolios
- Produkte hinzufügen
- Hinzufügen von Einschränkungen

- Gewähren des Zugriffs für Benutzer
- Freigeben eines Portfolios
- Portfolios teilen und importieren

## Erstellen, Anzeigen und Löschen von Portfolios

Auf der Portfolio-Seite 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.

Um die Portfolio-Seite aufzurufen

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 neu bei uns sind AWS Service Catalog, sehen Sie die Startseite. AWS Service Catalog 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 Portfolio-Seite fort.

Während der Nutzung AWS Service Catalog können Sie jederzeit zur Portfolio-Seite zurückkehren. Wählen Sie in der Navigationsleiste Service Catalog und dann Portfolios aus.

## Anzeigen von Portfoliodetails

In der AWS Service Catalog Administratorkonsole werden auf der Portfolio-Detailseite die Einstellungen für ein Portfolio aufgeführt. Verwenden Sie diese Seite, um die Produkte im Portfolio zu verwalten, Benutzern Zugriff auf Produkte zu gewähren 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 Portfolio-Seite, 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.
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 (gemeinsam genutzte) Portfolios entfernen, importierte Portfolios jedoch nicht löschen.

Bevor Sie ein Portfolio löschen können, müssen Sie alle Produkte, Einschränkungen, Gruppen, Rollen, Benutzer, Anteile und entfernen TagOptions. Öffnen Sie dazu ein Portfolio, um die Portfoliodetails anzuzeigen. Wählen Sie dann einen Tab, 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. Sie können nur lokale Portfolios löschen. Wenn Sie versuchen, ein importiertes (geteiltes) Portfolio zu löschen, ist das Aktionsmenü nicht verfügbar.
4. Wählen Sie im Bestätigungsfenster Delete.

## Produkte hinzufügen

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

> **Note**
>
> Wenn Sie ein AWS Service Catalog Produkt erstellen, können Sie eine AWS CloudFormation Vorlage 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 benötigen außerdem die Erlaubnis, Objekte aus zusätzlichen Buckets abzurufen, wenn Sie ein Produkt bereitstellen. Weitere Informationen finden Sie unter Produkte erstellen.

## Ein neues Produkt hinzufügen

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

So fügen Sie ein neues Produkt hinzu

1. Navigieren Sie zur Seite Portfolios und wählen Sie dann den Namen des Portfolios aus, zu dem Sie das Produkt hinzufügen möchten.
2. Erweitern Sie auf der Seite mit den Portfoliodetails den Bereich 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 Produktliste angezeigt, um Ihnen bei der Auswahl des richtigen Produkts zu helfen.
   - Beschreibung — Die vollständige Beschreibung. Diese Beschreibung wird in der Produktliste angezeigt, um Ihnen bei der Auswahl des richtigen Produkts zu helfen.
   - Eigentümer oder Vertriebspartner — Der Name oder die E-Mail-Adresse des Eigentümers. Die Kontaktinformationen für den Händler 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 wählen — Wählen Sie für AWS CloudFormation Produkte Ihre eigene Vorlagendatei, eine AWS CloudFormation Vorlage von einem lokalen Laufwerk oder eine URL, die auf eine in

Amazon S3 gespeicherte Vorlage, eine bestehende AWS CloudFormation Stack-ARN-Vorlage oder eine in einem externen Repository gespeicherte Vorlagendatei verweist.

Wählen Sie für Teraform-Produkte Ihre eigene Vorlagendatei, eine Konfigurationsdatei tar.gz von einem lokalen Laufwerk oder eine URL, die auf eine in Amazon S3 gespeicherte Vorlage verweist, oder eine Konfigurationsdatei tar.gz, 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 dafür verantwortlich, die Richtigkeit und den Zugriff auf die Support-Informationen zu gewährleisten.
   - Support-Beschreibung (optional) — Eine Beschreibung, wie Sie den E-Mail-Kontakt und den Support-Link verwenden sollten.

6. Wählen Sie Produkt erstellen.

## Ein vorhandenes Produkt hinzufügen

Sie können bestehende Produkte an drei Stellen zu einem Portfolio hinzufügen: Portfolioliste, Portfoliodetailseite oder Produktlistenseite.

So fügen Sie einem Portfolio ein vorhandenes Produkt hinzu

1. Navigieren Sie zur Portfolio-Seite.
2. Wählen Sie ein Portfolio aus. Wählen Sie dann Aktionen — Produkt zum Portfolio hinzufügen.
3. Wählen Sie ein Produkt aus und klicken Sie dann auf Produkt zum Portfolio hinzufügen.

## Ein Produkt aus einem Portfolio entfernen

Wenn Sie ein Produkt nicht mehr verwenden möchten, entfernen Sie es aus einem Portfolio. Das Produkt ist weiterhin in Ihrem Katalog auf der Produktseite 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 Bereich Produkte.
3. Wählen Sie ein oder mehrere Produkte aus und klicken Sie dann auf Entfernen.
4. Bestätigen Sie Ihre Auswahl.

# Hinzufügen von Einschränkungen

Sie sollten Einschränkungen hinzufügen, um zu kontrollieren, wie Benutzer mit Produkten umgehen. Weitere Informationen zu den Arten von Einschränkungen, die AWS Service Catalog unterstützt werden, finden Sie unterAWS Service Catalog Einschränkungen verwenden.

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 wählen Sie ein Portfolio aus.
3. Erweitern Sie auf der Seite mit den Portfoliodetails den Abschnitt Beschränkung erstellen und wählen Sie Einschränkungen hinzufügen aus.
4. Wählen Sie unter Produkt das Produkt aus, auf das die Einschränkung angewendet werden soll.
5. Wählen Sie für Einschränkungstyp eine der folgenden Optionen:

   Starten — Ermöglicht es Ihnen, dem Produkt, das für die Bereitstellung der AWS Ressourcen verwendet wird, eine IAM-Rolle zuzuweisen. Weitere Informationen finden Sie unter AWS Service Catalog Einschränkungen beim Start.

Benachrichtigung — Ermöglicht es Ihnen, Produktbenachrichtigungen zu einem Amazon SNS SNS-Thema zu streamen. Weitere Informationen finden Sie unter AWS Service Catalog Einschränkungen bei Benachrichtigungen.

Vorlage — Ermöglicht es Ihnen, die Optionen einzuschränken, die Endbenutzern bei der Produkteinführung zur Verfügung stehen. Eine Vorlage besteht aus einer Textdatei im JSON-Format, die eine oder mehrere Regeln enthält. Regeln werden der vom Produkt verwendeten AWS CloudFormation Vorlage hinzugefügt. Weitere Informationen finden Sie unter Vorlageneinschränkungsregeln.

Stack Set — Ermöglicht die Konfiguration der Produktbereitstellung über Konten und Regionen hinweg mithilfe von AWS CloudFormation StackSets. Weitere Informationen finden Sie unter AWS Service Catalog Einschränkungen für Stapelsätze.

Tag-Update — Ermöglicht es Ihnen, Tags zu aktualisieren, nachdem das Produkt bereitgestellt wurde. Weitere Informationen finden Sie unter Einschränkungen bei der AWS Service Catalog Tag-Aktualisierung.

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 wählen Sie ein Portfolio aus.
3. Erweitern Sie auf der Seite mit den Portfoliodetails den Abschnitt Beschränkung erstellen und wählen Sie die Einschränkung aus, die Sie bearbeiten möchten.
4. Wählen Sie Einschränkungen bearbeiten aus.
5. Bearbeiten Sie die Einschränkung nach Bedarf und wählen Sie Speichern.

## 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 einer IAM-Gruppe zuzuordnen und dieser Gruppe Zugriff 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.

Neben dem 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 Principals mit anderen Konten teilen möchten, können Sie dem Portfolio Principalnamen (Gruppen, Rollen oder Benutzer) zuordnen. Hauptnamen 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, auf 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 mit den Portfoliodetails die Registerkarte Zugriff aus.
5. Wählen Sie unter Portfoliozugriff die Option Zugriff gewähren aus.
6. Wählen Sie als Typ die Option Principal Name und dann den Typ group/, role/ oder user/ aus. Sie können bis zu 9 Prinzipalnamen hinzufügen.
7. Wählen Sie Grant Access, um den Principal dem aktuellen Portfolio zuzuordnen.

So entfernen Sie den Zugriff auf ein Portfolio

1. Wählen Sie auf der Seite mit den Portfoliodetails eine Gruppe, eine Rolle oder einen Benutzernamen aus.
2. Wählen Sie Zugriff entfernen.

## Freigeben eines Portfolios

Um es einem AWS Service Catalog Administrator für ein anderes AWS Konto zu ermöglichen, Ihre Produkte an Endbenutzer zu verteilen, teilen Sie Ihr AWS Service Catalog Portfolio mit ihnen, indem Sie entweder account-to-account Sharing oder verwenden AWS Organizations.

Wenn Sie ein Portfolio über account-to-account Sharing oder Organizations teilen, teilen Sie 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 AWS Identity and Access Management Zugriff für Endbenutzer hinzufügen.

> **Note**
>
> Sie können eine gemeinsam genutzte Ressource nicht gemeinsam nutzen. Dazu gehören Portfolios, die ein freigegebenes Produkt enthalten.

## Account-to-account teilen

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

Um ein Portfolio mit einem AWS Konto zu teilen

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 Aktionsmenü die Option Teilen aus.
3. Geben Sie unter Konto-ID eingeben die Konto-ID des AWS Kontos ein, mit dem Sie Inhalte teilen. (Optional) Wählen Sie TagOption Teilen aus. Wählen Sie dann „Teilen“.
4. Senden Sie die URL an den AWS Service Catalog Administrator des Zielkontos. Die URL öffnet die Seite „Portfolio importieren“, wobei der ARN des gemeinsam genutzten Portfolios automatisch bereitgestellt wird.

### Importieren eines Portfolios

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

Sie müssen kein Portfolio importieren, wenn das Portfolio gemeinsam genutzt wurde AWS Organizations.

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

Um alle importierten Portfolios anzuzeigen, öffnen Sie die AWS Service Catalog Konsole unter https://console.aws.amazon.com/servicecatalog/. Wählen Sie auf der Seite Portfolios die Registerkarte Importiert aus. Sehen Sie sich die Tabelle Importierte Portfolios an.

## Teilen mit AWS Organizations

Sie können AWS Service Catalog Portfolios teilen mit AWS Organizations.

Zunächst müssen Sie entscheiden, ob Sie Inhalte über das Verwaltungskonto oder über ein delegiertes Administratorkonto teilen. Wenn Sie Inhalte nicht von Ihrem Verwaltungskonto aus teilen möchten, registrieren Sie ein delegiertes Administratorkonto, das Sie für die gemeinsame Nutzung 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.)

### Teilen von einem Verwaltungskonto aus

Sie können ein Portfolio mit einer Organisation teilen, wenn Sie Ihre Organisationsstruktur verwenden oder die ID eines Organisationsknotens eingeben.

Um ein Portfolio mithilfe der Organisationsstruktur mit einer Organisation zu teilen

1. Öffnen Sie die AWS Service Catalog Konsole 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 Organizationsund filtern Sie sie.

   Sie können den Stammknoten auswählen, um das Portfolio mit Ihrer gesamten Organisation, einer übergeordneten Organisationseinheit (OU), einer untergeordneten Organisationseinheit oder einem AWS Konto innerhalb Ihrer Organisation zu teilen.

Durch die gemeinsame Nutzung für eine übergeordnete Organisationseinheit wird das Portfolio für alle Konten und untergeordneten Organisationseinheiten innerhalb dieser übergeordneten Organisationseinheit gemeinsam genutzt.

Sie können „Nur AWS Konten anzeigen“ auswählen, um eine Liste aller AWS Konten in Ihrer Organisation zu sehen.

Um ein Portfolio mit einer Organisation zu teilen, geben Sie die ID des Organisationsknotens ein

1. Öffnen Sie die AWS Service Catalog Konsole 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 die Daten mit Ihrer gesamten Organisation, einem AWS Konto innerhalb Ihrer Organisation oder einer Organisationseinheit teilen möchten.

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

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 auf die gleiche Weise gemeinsam nutzen wie ein Verwaltungskonto. Sie sind berechtigt, Portfolios zu erstellen, zu löschen und gemeinsam zu nutzen.

Um einen delegierten Administrator zu registrieren oder abzumelden, müssen Sie die API oder CLI vom Verwaltungskonto aus 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 anrufen. `EnableAWSOrganizationsAccess`

Das Verfahren für die gemeinsame Nutzung eines Portfolios von einem delegierten Administratorkonto aus ist dasselbe wie das Teilen über ein Verwaltungskonto, wie oben unter beschrieben. the section called “Teilen von einem Verwaltungskonto aus”

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

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

> **Note**
>
> Wenn das von einem delegierten Administrator erstellte Portfolio und die Aktien nach der Abmeldung des delegierten Administrators nicht entfernt werden, registrieren Sie den delegierten Administrator erneut und deregistrieren Sie ihn erneut. Durch diese Aktion werden das Portfolio und die von diesem Konto erstellten Aktien entfernt.

Konten innerhalb Ihrer Organisation verschieben

Wenn Sie ein Konto innerhalb Ihrer Organisation verschieben, können sich die AWS Service Catalog Portfolios ändern, die mit dem Konto geteilt werden.

Konten haben nur Zugriff auf Portfolios, die mit ihrer Zielorganisation oder Organisationseinheit geteilt wurden.

## Teilen TagOptions beim Teilen von Portfolios

Als Administrator können Sie eine Freigabe erstellen, die Sie einschließen möchten TagOptions. TagOptions sind Schlüssel-Wert-Paare, die Administratoren Folgendes ermöglichen:

- Definieren und erzwingen Sie die Taxonomie für Tags.
- Definieren Sie Tag-Optionen und ordnen Sie sie Produkten und Portfolios zu.

- Teilen Sie Tag-Optionen für Portfolios und Produkte mit anderen Konten.

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

In Empfängerkonten können Administratoren ihrem importierten Portfolio weitere lokale TagOptions Konten zuordnen, um kontospezifische Tagging-Regeln durchzusetzen.

> **Note**
>
> Um ein Portfolio gemeinsam nutzen zu können, benötigen Sie die AWS Konto-ID des Verbrauchers. Suchen Sie die AWS Konto-ID in der Konsole unter Mein Konto.

> **Note**
>
> Wenn a einen einzigen Wert TagOption hat, AWS wird dieser Wert während des Bereitstellungsprozesses automatisch durchgesetzt.

Zum Teilen TagOptions beim Teilen 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 in der obigen Liste die Option Teilen aus und klicken Sie dann auf die Schaltfläche Teilen.
4. Wählen Sie aus, ob Sie es mit einem anderen AWS Konto oder einer anderen Organisation teilen möchten.
5. Geben Sie die 12-stellige Konto-ID-Nummer ein, wählen Sie Aktivieren und dann Teilen aus.

   Das Konto, das Sie geteilt haben, wird im Abschnitt Geteilte Konten angezeigt. Es gibt an, ob TagOptions sie aktiviert wurden.

Sie können eine Portfolioaktie auch so aktualisieren, dass sie einschließt TagOptions. Alle Produkte TagOptions , die zum Portfolio und Produkt gehören, werden jetzt auf dieses Konto übertragen.

Um eine Portfolioaktie so zu aktualisieren, dass sie Folgendes beinhaltet 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 in der obigen Liste die Option Teilen aus.
4. Wählen Sie unter „Geteilte Konten mit“ eine Konto-ID und dann „Aktionen“ aus.
5. Wähle „Aktualisieren“, „Teilen aufheben“ oder „Teilen aufheben“.

   Wenn Sie Update Unshare auswählen, wählen Sie Aktivieren, um das Teilen zu starten. TagOptions Das Konto, das Sie geteilt haben, wird im Abschnitt Gemeinsam genutzte Konten angezeigt.

   Wenn du Unshare auswählst, bestätige, dass du das Konto nicht mehr teilen möchtest.

## Teilen von Hauptnamen beim Teilen von Portfolios

Als Administrator können Sie eine Portfolio-Freigabe 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 teilen, AWS Service Catalog wird überprüft, ob diese Prinzipalnamen bereits vorhanden sind. Falls sie existieren, AWS Service Catalog werden die entsprechenden IAM-Prinzipale automatisch dem gemeinsamen Portfolio zugeordnet, 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 dennoch die Möglichkeit hat, Prinzipale (Benutzer/Rollen) zu erstellen, könnte dieser Benutzer einen IAM-Prinzipal erstellen, der einer Prinzipalnamenzuordnung für das Portfolio entspricht. Dieser Benutzer weiß zwar möglicherweise nicht, über welche Prinzipalnamen er verknüpft ist AWS Service Catalog, kann jedoch den Benutzer erraten. Wenn dieser potenzielle Eskalationspfad ein Problem darstellt, AWS Service Catalog empfiehlt er die Verwendung von `PrincipalType` as`IAM`. Bei dieser Konfiguration muss das `PrincipalARN` bereits im Empfängerkonto vorhanden sein, bevor es zugeordnet werden kann.

Wenn Sie Principal Names im Hauptkonto hinzufügen oder entfernen, AWS Service Catalog werden diese Änderungen automatisch auf das Empfängerkonto angewendet. Benutzer im Empfängerkonto können dann Aufgaben entsprechend ihrer Rolle ausführen:

- Endbenutzer können das Produkt des Portfolios bereitstellen, aktualisieren und beenden.
- Administratoren können ihrem importierten Portfolio zusätzliche IAM-Principals zuordnen, um kontospezifischen Endbenutzern Zugriff zu gewähren.

> **Note**
>
> Die gemeinsame Nutzung von Principalnamen ist nur für verfügbar. AWS Organizations

Um Principal Names beim Teilen von Portfolios zu teilen

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 AWS Organizations.
5. Wählen Sie den gesamten Organisationsstamm, eine Organisationseinheit (OU) oder ein Organisationsmitglied aus.
6. Aktivieren Sie in den Freigabeeinstellungen die Option Principal Sharing.

Sie können eine Portfoliofreigabe auch so aktualisieren, dass sie die gemeinsame Nutzung des Prinzipalnamens einschließt. Dadurch werden alle Principal Names, die zu diesem Portfolio gehören, mit dem Empfängerkonto geteilt.

Um eine Portfolio-Aktie zu aktualisieren, um Principal Names 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 den Tab Teilen.
4. Wählen Sie den Share aus, den Sie aktualisieren möchten, und klicken Sie dann auf Teilen.

5. Wählen Sie „Freigabe aktualisieren“ und anschließend „Aktivieren“, um die gemeinsame Nutzung von Benutzern zu initiieren. AWS Service Catalog gibt dann die Principal Names in den Empfängerkonten weiter.

Deaktivieren Sie die gemeinsame Nutzung von Prinzipalnamen, wenn Sie die Prinzipalnamen nicht mehr mit Empfängerkonten teilen möchten.

Verwenden von Platzhaltern bei der gemeinsamen Nutzung von Prinzipalnamen

AWS Service Catalog unterstützt die Gewährung von Portfoliozugriff auf IAM-Prinzipalnamen (Benutzer-, Gruppen- oder Rollennamen) mit Platzhaltern wie '*' oder '?'. Durch die Verwendung von Platzhaltermustern können Sie mehrere IAM-Prinzipalnamen gleichzeitig abdecken. Der ARN-Pfad und der Prinzipalname erlauben eine unbegrenzte Anzahl von Platzhalterzeichen.

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`**

Im ARN-Format des IAM-Prinzipals (**`arn:partition:iam:::resource-type/resource-path/resource-name`**) gehören user/, group/ oder role/ zu den gültigen Werten. Das „?“ und „*“ sind nur nach dem Ressourcentyp im Resource-ID-Segment zulässig. Sie können Sonderzeichen an einer beliebigen Stelle innerhalb der Ressourcen-ID verwenden.

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

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

## Portfolios teilen und importieren

Um Ihre AWS Service Catalog Produkte Benutzern zur Verfügung zu stellen, die nicht zu Ihrer gehören AWS-Konten, z. B. Benutzern, die anderen Organisationen oder anderen Organisationen

AWS-Konten in Ihrer Organisation angehören, teilen Sie Ihre Portfolios mit ihnen. Sie können Inhalte auf verschiedene Arten teilen, z. B. durch account-to-account gemeinsame Nutzung, gemeinsame Nutzung durch Organisationen und Bereitstellung von Katalogen mithilfe von Stacksets.

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 teilen möchten (eine importierte Version Ihres Portfolios, die mit dem Original synchron bleibt), können Sie das account-to-account Teilen verwenden oder das Teilen über AWS Organizations.

Informationen zur Verwendung von Stacksets zur Bereitstellung einer Kopie Ihres Katalogs finden Sie unter So richten Sie einen Katalog mit AWS Service Catalog Standardprodukten für Unternehmen mit mehreren Regionen und Konten ein.

Wenn Sie ein Portfolio mithilfe von account-to-account Sharing oder teilen AWS Organizations, ermöglichen 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, also der Administrator, mit dem Sie ein Portfolio teilen, kann die Produkte oder Einschränkungen nicht ändern, kann jedoch den 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 ihrem AWS Konto gehören:

- Durch Hinzufügen von Benutzern, Gruppen und Rollen zum importierten Portfolio.
- Durch Hinzufügen von Produkten aus dem importierten Portfolio zu einem lokalen Portfolio, einem separaten Portfolio, das der Empfängeradministrator erstellt und das zu seinem AWS Konto gehört. Der Empfängeradministrator fügt dann Benutzer, Gruppen und Rollen zu diesem lokalen Portfolio hinzu. Alle Einschränkungen, die ursprünglich für Produkte im gemeinsamen Portfolio galten, gelten auch für das lokale Portfolio. Der Administrator des lokalen Portfolioempfängers kann

zusätzliche Einschränkungen hinzufügen, kann jedoch die Einschränkungen, die ursprünglich aus dem gemeinsamen Portfolio importiert wurden, 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 Launch-Rolle ist eine IAM-Rolle, die zur Bereitstellung von AWS Ressourcen (wie EC2 Amazon-Instances oder Amazon RDS-Datenbanken) AWS Service Catalog verwendet wird, wenn ein Endbenutzer das Produkt startet. Als Administrator können Sie wählen, ob Sie einen bestimmten ARN für die Startrolle oder einen lokalen Rollennamen festlegen möchten. Wenn Sie die Rolle ARN verwenden, wird die Rolle auch dann verwendet, wenn der Endbenutzer einem anderen AWS Konto angehört als dem, 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 Einschränkungen beim Start. Das AWS Konto, dem die Startrolle gehört, stellt die AWS Ressourcen bereit, und für dieses Konto fallen die Nutzungsgebühren für diese Ressourcen an. Weitere Informationen finden Sie unter AWS Service Catalog -Preisgestaltung.

Dieses Video zeigt Ihnen, wie Sie Portfolios für mehrere Konten gemeinsam nutzen können. AWS Service Catalog

Portfolios kontenübergreifend teilen (https://www.youtube.com/embed/BVSohYOppjk% 22% 3EShare) in AWS 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 Konten der Geschäftsleitung und den Konten der Angehörigen erfolgen.

## Beziehung zwischen freigegebenen und importierten Portfolios

In dieser Tabelle werden die Beziehung zwischen einem importierten Portfolio und einem gemeinsam genutzten Portfolio sowie die Aktionen zusammengefasst, die ein Administrator, der ein Portfolio importiert, mit diesem Portfolio und den darin enthaltenen Produkten ergreifen kann und nicht.

| Element des freigegebenen Portfolios | Beziehung zu dem importierten Portfolio | Empfänger-Administrator kann | Empfänger-Administrator kann nicht |
|---|---|---|---|
| Produkte und Produktversionen | Geerbt<br><br>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<br><br>Wenn der Portfolio-Ersteller einem | In einem lokalen Portfolio kann der Administrator Startbeschränkunge | Starteinschränkungen hinzufügen oder aus dem importierten Portfolio entfernen. |

| Element des freigegebenen Portfolios | Beziehung zu dem importierten Portfolio | Empfänger-Administrator kann | Empfänger-Administrator kann nicht |
|---|---|---|---|
| | gemeinsam genutzten Produkt Startbeschränkungen hinzufügt oder diese daraus entfernt, wird die Änderung auf alle importierten Instanzen des Produkts übertragen.<br><br>Wenn der Administrator des Empfängers seinem lokalen Portfolio ein importiertes Produkt hinzufügt, wird diese importierte Startbeschränkung nicht auf das gemeinsam genutzte Portfolio übertragen. | n anwenden, die sich auf die lokale Markteinführung des Produkts auswirken. | |

| Element des freigegebenen Portfolios | Beziehung zu dem importierten Portfolio | Empfänger-Administrator kann | Empfänger-Administrator kann nicht |
|---|---|---|---|
| Vorlageneinschränkungen | Geerbt<br><br>Wenn der Ersteller des Portfolios eine Vorlageneinschränkung hinzufügt oder aus einem freigegebenen Produkt entfernt, wird die Änderung auf alle importierten Instances des Produkts verteilt.<br><br>Wenn der Empfängeradministrator ein importiertes Produkt zu einem lokalen Portfolio hinzufügt, werden die Beschränkungen für importierte Vorlagen nicht auf das lokale Portfolio übertragen. | In einem lokalen Portfolio kann der Administrator Vorlageneinschränkungen hinzufügen, die das lokale Produkt einschränken. | Die importierten Vorlageneinschränkungen entfernen. |
| 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 auf der Grundlage einer aktualisierten Vorlage erstellen, und Produkte in Portfolios zusammenfassen, 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 bereits bereitgestellte Produkte aktualisieren.

Aufgaben

- Anzeigen der Produktseite
- Erstellen von Produkten
- Produkte zu Portfolios hinzufügen
- Produkte aktualisieren
- Produkte mit Vorlagendateien von GitHub GitHub Enterprise oder Bitbucket synchronisieren
- Produkte löschen
- Verwalten von Versionen

## Anzeigen der Produktseite

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

Um die Seite mit der Produktliste aufzurufen

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 Produktseite in der AWS Service Catalog Administratorkonsole.

> **Note**
>
> Die Erstellung von Terraform-Produkten erfordert eine zusätzliche Konfiguration, einschließlich einer Terraform-Provisioning-Engine und einer Startrolle. Weitere Informationen finden Sie unter. Erste Schritte mit einem Terraform-Produkt

Um ein neues AWS Service Catalog Produkt zu erstellen

1. Navigieren Sie zur Seite mit der Produktliste.
2. Wählen Sie Produkt erstellen und anschließend Produkt erstellen aus.
3. Produktdetails — Ermöglicht es Ihnen, den Produkttyp auszuwählen, den Sie erstellen möchten. AWS Service Catalog unterstützt die AWS CloudFormation Produkttypen Terraform Cloud und External (unterstützt 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.
   - Eigentümer — Die Person oder Organisation, die dieses Produkt veröffentlicht. Der Besitzer kann der Name Ihrer IT-Organisation oder ein Administrator sein.
   - Vertriebspartner (optional) — Der Name des Herausgebers der Anwendung. In diesem Feld können Sie die Produktliste sortieren, um das Auffinden von Produkten zu erleichtern.
4. Mit den Versionsdetails können Sie Ihre Vorlagendatei hinzufügen und Ihr Produkt erstellen. Geben Sie Folgendes ein:
   - Methode wählen — Es gibt vier Möglichkeiten, eine Vorlagendatei hinzuzufügen.
     - Verwenden Sie eine lokale Vorlagendatei — Laden Sie eine AWS CloudFormation Vorlage oder eine Terraform tar.gz -Konfigurationsdatei von einem lokalen Laufwerk hoch.
     - Eine Amazon S3-URL verwenden — Geben Sie eine URL an, die auf eine AWS CloudFormation Vorlage oder eine Terraform-Konfigurationsdatei tar.gz verweist, die in Amazon S3 gespeichert ist. Wenn Sie eine Amazon S3 S3-URL angeben, muss diese mit beginnen`https://`.
     - Verwenden Sie ein externes Repository — Geben Sie Ihr Code-Repository GitHub, Ihr GitHub Enterprise- oder Bitbucket-Code-Repository an. AWS Service Catalog ermöglicht

es dir, Produkte mit Vorlagendateien zu synchronisieren. Für Terraform-Produkte muss das Vorlagendateiformat eine einzelne Datei sein, die in Tar archiviert und in Gzip komprimiert ist.

- Einen vorhandenen CloudFormation Stack verwenden — Geben Sie den ARN für einen vorhandenen CloudFormation Stack ein. Diese Methode unterstützt weder Terraform Cloud noch externe 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 — Wird auf der Registerkarte „Versionen“ auf einer Produktdetailseite verwaltet. Wenn eine Produktversion erstellt wird — während des Workflows zur Produkterstellung — wird die Anleitung für diese Version auf die Standardeinstellung gesetzt. Weitere Informationen zur Anleitung finden Sie unter Versionen verwalten.

5. Die Support-Details identifizieren die Organisation in Ihrem Unternehmen und bieten eine Kontaktstelle für 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 finden oder Tickets einreichen können. Die URL muss mit `http://` oder `https://` beginnen. Administratoren sind dafür verantwortlich, die Richtigkeit und den Zugriff auf die Support-Informationen zu gewährleisten.
   - Support-Beschreibung (optional) — Eine Beschreibung, wie Sie den E-Mail-Kontakt und den Support-Link verwenden sollten.
6. Tags verwalten (optional) — Neben der Verwendung von Tags zur Kategorisierung Ihrer Ressourcen können Sie sie auch verwenden, um Ihre Berechtigungen zum Erstellen dieser Ressource zu authentifizieren.
7. Produkt erstellen — Wenn Sie das Formular ausgefüllt haben, wählen Sie Produkt erstellen aus. Nach einigen Sekunden erscheint das Produkt auf der Seite mit der Produktliste. Möglicherweise müssen Sie Ihren Browser aktualisieren, um das Produkt zu sehen.

Sie können es auch verwenden CodePipeline , um eine Pipeline zu erstellen und zu konfigurieren, um Ihre Produktvorlage in Ihrem Quell-Repository bereitzustellen AWS Service Catalog und die Änderungen, die Sie in diesem vorgenommen haben, zu übermitteln. Weitere Informationen finden Sie unter Tutorial: Eine Pipeline erstellen, die für bereitgestellt wird. AWS Service Catalog

Sie können Parametereigenschaften in Ihrer AWS CloudFormation oder Terraform-Vorlage definieren und diese Regeln bei der Bereitstellung durchsetzen. Diese Eigenschaften können die Mindest- und Höchstlänge, Mindest- und Höchstwerte, 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 im AWS CloudFormation Benutzerhandbuch unter Parameter.

## Fehlerbehebung

Sie benötigen die Berechtigung, Objekte aus Amazon S3 S3-Buckets abzurufen. 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 berechtigt sind, Objekte aus den folgenden Buckets abzurufen:

- Der Bucket, in dem die Vorlage für das Bereitstellungsartefakt gespeichert ist.
- Der Bucket, der mit "cf-templates-*" beginnt und in dem AWS Service Catalog die Vorlage für das Bereitstellungsartefakt gespeichert wird.
- Der interne Bucket, der mit "sc-*" beginnt und in dem Metadaten gespeichert werden. AWS Service Catalog Sie können diesen Bucket von Ihrem Konto aus 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-*/*"
          ]
      }
```

## Produkte zu Portfolios hinzufügen

Sie können Produkte zu einer beliebigen Anzahl von Portfolios hinzufügen. Wenn ein Produkt aktualisiert wird, erhalten alle Portfolios (einschließlich gemeinsam genutzter 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 mit der Produktliste.
2. Wählen Sie ein Produkt aus und klicken Sie dann auf Aktionen. Wählen Sie im Drop-down-Menü die Option Produkt zum Portfolio hinzufügen aus. Sie werden zur Seite „Zum Portfolio ***name-of-product*** hinzufügen“ weitergeleitet.
3. Wählen Sie ein Portfolio aus und klicken Sie dann auf Produkt zum Portfolio hinzufügen.

Wenn Sie einem Portfolio ein Terraform-Produkt hinzufügen, ist für das Produkt eine Beschränkung bei der Markteinführung erforderlich. 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 Startbeschränkung verwendet, verwendet das Konto diesen Namen für die IAM-Rolle. Auf diese Weise können die Einschränkungen für die Startrolle kontounabhängig sein, sodass Sie weniger Ressourcen pro gemeinsam genutztem Konto erstellen können. Einzelheiten und Anweisungen finden Sie unter Schritt 6: Fügen Sie Ihrem Terraform-Produkt eine Startbeschränkung hinzu

Ein Portfolio kann zahlreiche Produkte enthalten, bei denen es sich um eine Mischung aus AWS CloudFormation und Terraform-Produkttypen handelt.

## Produkte aktualisieren

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-Konfigurationsdatei tar.gz ersetzen. Sie müssen die

vorhandene AWS CloudFormation Vorlagendatei durch eine neue 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 Seite mit den bereitgestellten Produkten oder den Detailseiten für bereitgestellte Produkte verwenden.

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

Erstellen einer neuen Produktversion

1. Navigieren Sie zur Seite mit der Produktliste.
2. Wählen Sie das Produktprodukt aus, das Sie aktualisieren möchten. Sie werden zur Seite mit den Produktdetails weitergeleitet.
3. Erweitern Sie auf der Seite mit den Produktdetails den Tab Versionen und wählen Sie dann Neue Version erstellen aus.
4. Gehen Sie unter Versionsdetails wie folgt vor:

   - Vorlage wählen — Es gibt vier Möglichkeiten, eine Vorlagendatei hinzuzufügen.

     Verwenden Sie eine lokale Vorlagendatei — Laden Sie eine AWS CloudFormation Vorlage oder eine Terraform tar.gz -Konfigurationsdatei von einem lokalen Laufwerk hoch.

     Eine Amazon S3-URL verwenden — Geben Sie eine URL an, die auf eine AWS CloudFormation Vorlage oder eine Terraform-Konfigurationsdatei tar.gz verweist, die in Amazon S3 gespeichert ist. Wenn Sie eine Amazon S3 S3-URL angeben, muss diese mit https://beginnen.

     Verwenden Sie ein externes Repository — Geben Sie Ihr Code-Repository GitHub, Ihr GitHub Enterprise- oder Bitbucket-Code-Repository an. AWS Service Catalog ermöglicht es dir, Produkte mit Vorlagendateien zu synchronisieren. Für Terraform-Produkte muss das Vorlagendateiformat eine einzelne Datei sein, die in Tar archiviert und in Gzip komprimiert ist.

Einen vorhandenen CloudFormation Stack verwenden — Geben Sie den ARN für einen vorhandenen CloudFormation Stack ein. Diese Methode unterstützt weder Terraform Cloud noch externe 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 Vorgängerversion.

5. Wählen Sie Produktversion erstellen aus.

Sie können CodePipeline damit auch eine Pipeline erstellen und konfigurieren AWS Service Catalog, in der Sie Ihre Produktvorlage bereitstellen und Ihre Änderungen in Ihrem Quell-Repository bereitstellen. Weitere Informationen finden Sie unter Tutorial: Eine Pipeline erstellen, die bereitgestellt wird für 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 mit der AWS Service Catalog Konsole, der CodeConnections Konsole AWS Command Line Interface (CLI) oder herstellen CodeConnections APIs.

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 in großen Mengen 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.
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 der letzten Synchronisierung abrufen.

> **Note**
>
> Sie können Repository-Informationen und den Status der letzten Synchronisierung auf Produktebene einsehen. Benutzer müssen über IAM-Berechtigungen für verfügen, um Repository-Details einsehen CodeConnections APIs 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.

> **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 die Option AWS CLI to verwenden

- 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.

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 |

| AWS-Region Name | AWS-Region Identität | Support für GIT-synchronisierte Produkte |
|---|---|---|
| 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 |
| Naher Osten (Bahrain) | me-south-1 | Nein |
| Südamerika (São Paulo) | sa-east-1 | Ja |

| AWS-Region Name | AWS-Region Identität | Support für GIT-synchronisierte Produkte |
|---|---|---|
| AWS GovCloud (US-Ost) | us-gov-east-1 | Nein |
| AWS GovCloud (US-West) | us-gov-west-1 | Nein |

## Produkte löschen

Wenn Sie ein Produkt löschen, AWS Service Catalog werden alle Produktversionen aus allen Portfolios entfernt, die das Produkt enthalten.

AWS Service Catalog ermöglicht es Ihnen, ein Produkt über die AWS Service Catalog Konsole zu löschen oder AWS CLI. Um ein Produkt erfolgreich zu löschen, müssen Sie zuerst die Zuordnung aller Ressourcen aufheben, die dem Produkt zugeordnet sind. Zu den Zuordnungen von Produktressourcen gehören beispielsweise Portfoliozuordnungen TagOptions, Budgets und Serviceaktionen.

> **Important**
>
> Sie können ein gelöschtes Produkt nicht wiederherstellen.

Um ein Produkt mit der AWS Service Catalog Konsole zu löschen

1. Navigieren Sie zur Portfolio-Seite 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 bei Produkten, denen keine Ressourcen zugeordnet sind, das Produkt, das Sie löschen möchten, indem Sie Löschen in das Textfeld eingeben, und wählen Sie dann Löschen aus.

   Fahren Sie bei Produkten mit zugehörigen Ressourcen mit Schritt 4 fort.
4. Sehen Sie sich im Fenster Produkt löschen die Tabelle Zuordnungen an, in der alle dem Produkt zugewiesenen Ressourcen angezeigt werden. AWS Service Catalog versucht, die Zuordnung dieser Ressourcen aufzuheben, wenn Sie das Produkt löschen.

5. Bestätigen Sie, dass Sie das Produkt und alle zugehörigen Ressourcen löschen möchten, indem Sie Löschen in das Textfeld eingeben.
6. Wählen Sie „Trennen und löschen“.

Wenn AWS Service Catalog die Zuordnung aller Ressourcen des Produkts nicht aufgehoben werden kann, wird das Produkt nicht gelöscht. Im Fenster Produkt löschen werden die Anzahl der fehlgeschlagenen Trennungen sowie eine Beschreibung für jeden Fehler angezeigt. Weitere Informationen zur Behebung fehlgeschlagener Ressourcenzuordnungen beim Löschen eines Produkts finden Sie weiter unten unter Beheben fehlgeschlagener Ressourcenzuordnungen beim Löschen eines Produkts.

Themen


- Löschen von Produkten mit dem AWS CLI
- Behebung fehlgeschlagener Ressourcenzuordnungen beim Löschen eines Produkts


## Löschen von Produkten mit dem AWS CLI

AWS Service Catalog ermöglicht es Ihnen, das AWS Command Line Interface(AWS CLI) zu verwenden, um Produkte aus Ihrem Portfolio zu löschen. Das AWS CLI ist ein Open-Source-Tool, mit dem Sie mithilfe von Befehlen in Ihrer Befehlszeilen-Shell mit AWS Diensten interagieren können. AWS Service Catalog Für die Funktion Force-Delete ist ein AWS CLI Alias erforderlich. Dabei handelt es sich um eine Abkürzung, die Sie in der erstellen können AWS CLI , um häufig verwendete Befehle oder Skripts zu kürzen.

Voraussetzungen

- Installieren und Konfigurieren der AWS CLI. Weitere Informationen finden Sie unter Installation oder Aktualisierung der neuesten Version von AWS CLI und Grundlagen der Konfiguration. Verwenden Sie eine AWS CLI Mindestversion von 1.11.24 oder 2.0.0.
- Der CLI-Alias Delete Product erfordert ein Bash-kompatibles Terminal und den JQ-Befehlszeilen-JSON-Prozessor. Weitere Informationen zur Installation des Befehlszeilen-JSON-Prozessors finden Sie unter Laden Sie jq herunter.
- Erstellen Sie einen AWS CLI Alias für `Disassociation` Batch-API-Aufrufe, sodass Sie ein Produkt mit einem einzigen Befehl löschen können.

Um ein Produkt erfolgreich zu löschen, müssen Sie zuerst die Zuordnung aller Ressourcen aufheben, die dem Produkt zugeordnet sind. Zu den Zuordnungen von Produktressourcen gehören beispielsweise Portfoliozuordnungen, Budgets, Tag-Optionen und Serviceaktionen. Wenn Sie die CLI zum Löschen eines Produkts verwenden, können Sie mit `force-delete-product` dem CLI-Alias die `Disassociate` API aufrufen, um alle Ressourcen zu trennen, die die `DeleteProduct` API verhindern würden. Dadurch wird ein separater Aufruf für einzelne Trennungen vermieden.

> **Note**
>
> Die in den folgenden Verfahren aufgeführten Dateipfade können je nachdem, welches Betriebssystem Sie für diese Aktionen verwenden, variieren.

Einen AWS CLI Alias zum Löschen von AWS Service Catalog Produkten erstellen

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

Erstellen Sie eine **`alias`** Datei in Ihrem AWS CLI Konfigurationsordner

1. Navigieren Sie in der AWS CLI Konsole zum Konfigurationsordner. Standardmäßig ist der Pfad des Konfigurationsordners `~/.aws/` unter Linux und macOS oder `%USERPROFILE%\.aws\` unter Windows.
2. Erstellen Sie `cli` mithilfe der 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 der ersten Zeile ein.
5. Speichern Sie die Datei.

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

Fügen Sie den force-delete-product Alias manuell zu Ihrer **`alias`** Datei hinzu

1. Navigieren Sie in der AWS CLI Konsole 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 Alias-Skript in das Terminalfenster ein, und drücken Sie dann STRG+D, um den `cat` Befehl zu beenden.

Rufen Sie den Alias auf force-delete-product

1. Führen Sie in Ihrem Terminalfenster den folgenden Befehl aus, um den Delete Product-Alias aufzurufen

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

   Das folgende Beispiel zeigt den `force-delete-product` Alias-Befehl 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 dem erfolgreichen 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 AWS CLI zur Verwendung von Aliasnamen und zum Löschen von AWS Service Catalog Produkten finden Sie in den folgenden Ressourcen:

- Erstellen und Verwenden von AWS CLI Aliasen im AWS Command Line Interface (CLI) - Benutzerhandbuch.
- AWS CLI Alias-Repository, Git-Repository.
- AWS Service Catalog Produkte werden gelöscht.
- AWS re:Invent 2016: Der effektive AWS CLI Nutzer auf. YouTube

## Behebung fehlgeschlagener Ressourcenzuordnungen beim Löschen eines Produkts

Wenn Ihr früherer Versuch, ein Produkt zu löschen, aufgrund von Ausnahmen bei der Trennung von Ressourcen fehlgeschlagen ist, sehen Sie sich die Liste der Ausnahmen und deren Lösungen unten an.

> **Note**
>
> Wenn Sie das Fenster Produkte löschen geschlossen haben, bevor Sie die Meldung zur fehlgeschlagenen Trennung von Ressourcen 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 Trennung von Ressourcen

Prüfen Sie im Fenster Produkt löschen die Statusspalte in der Tabelle Zuordnungen. Identifizieren Sie die fehlgeschlagene Ausnahme zur Trennung der Ressourcenzuweisung und die vorgeschlagenen Lösungen:

| Art der Status-Ausnahme | Ursache | Auflösung |
| --- | --- | --- |
| Produktprodukt-**** | AWS Service Catalog konnte das Produkt nicht löschen TagOptions, weil dem Produkt noch Budgets zugeordnet sind, mindestens eines `ProvisioningArtifact` mit zugehörigen Aktionen, das Produkt immer noch einem Portfolio zugewiesen ist, dem Produkt Benutzer zugewiesen sind oder das Produkt Einschränkungen aufweist. | Versuchen Sie erneut, das Produkt zu löschen. |
| Benutzer: `username` ist nicht berechtigt, 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 Trennen der Zuordnung von Produktressourcen zu erhalten, für die Sie derzeit nicht berechtigt sind. |

# Verwalten von Versionen

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

Versionen haben 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 gibt es für Produktversionen keine Anleitung. 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 gestartetes Produkt, das mit p bereitgestellt wurde, eine inzwischen 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 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.

# AWS Service Catalog Einschränkungen verwenden

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 Einschränkungen beim Start
- AWS Service Catalog Einschränkungen bei Benachrichtigungen
- AWS Service Catalog Einschränkungen beim Tag-Update
- AWS Service Catalog Einschränkungen für Stapelsätze
- AWS Service Catalog Einschränkungen für Vorlagen

## AWS Service Catalog Einschränkungen beim Start

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

- AWS CloudFormation Produkttyp: Schritt 6: Fügen Sie eine Startbeschränkung hinzu, um eine IAM-Rolle zuzuweisen

- Produkttyp Terraform Open Source oder Terraform Cloud: Schritt 5: Startrollen erstellen

Einschränkungen bei der Markteinführung gelten für Produkte im Portfolio (Zuordnung zum Produktportfolio). Markteinführungsbeschränkungen 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 Einschränkungen bei der Markteinführung müssen Endbenutzer Produkte mit ihren eigenen IAM-Anmeldeinformationen starten und verwalten. Dazu benötigen sie Berechtigungen für die AWS Dienste AWS CloudFormation, die die Produkte verwenden, und AWS Service Catalog. Durch die Verwendung einer Startrolle können Sie stattdessen die Berechtigungen der Endbenutzer auf das Minimum beschränken, das sie für das jeweilige 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 Startbeschränkung zuweisen, muss über die folgenden Berechtigungen verfügen:

Für Cloudformation-Produkte

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

Für Terraform-Produkte

- Services in der Amazon S3 S3-Vorlage für das Produkt
- Lesezugriff auf die Amazon S3 S3-Vorlage in einem serviceeigenen Amazon S3 S3-Bucket.
- `resource-groups:Tag`zum Taggen in einer EC2 Amazon-Instance (wird von der Terraform-Provisioning-Engine bei der Durchführung von Bereitstellungsvorgängen übernommen)
- `resource-groups:CreateGroup`für das Tagging von Ressourcengruppen (vorausgesetzt, um Ressourcengruppen AWS Service Catalog zu erstellen und Tags zuzuweisen)

Die Vertrauensrichtlinie der IAM-Rolle muss es ermöglichen AWS Service Catalog , die Rolle zu übernehmen. Im folgenden Verfahren wird die Vertrauensrichtlinie automatisch festgelegt, wenn Sie den Rollentyp auswählen AWS Service Catalog . Wenn Sie die Konsole nicht verwenden, finden Sie weitere Informationen im Abschnitt Erstellen von Vertrauensrichtlinien für AWS Dienste, 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 AWS Service Catalog Endbenutzern Berechtigungen erteilen beschrieben.

> **Note**
>
> Um bereitgestellte Cloudformation-Produkte und -Ressourcen in der AWS Service Catalog Konsole anzeigen zu können, benötigen AWS CloudFormation Endbenutzer Lesezugriff. Beim Anzeigen der bereitgestellten Produkte und Ressourcen in der Konsole wird die Rolle „Launch“ nicht verwendet.

So erstellen Sie eine Startrolle

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

   Terraform-Produkte erfordern zusätzliche Konfigurationen für die Startrolle. Weitere Informationen finden Sie unter Schritt 5: Startrollen erstellen unter 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 neben AWS Servicerollen 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 Startbeschränkung konfigurieren, müssen Sie diese Zeichenfolge verwenden:`"s3:ExistingObjectTag/servicecatalog:provisioning":"true"`.

5. Fügen Sie der Richtlinie für jeden zusätzlichen Service, den das Produkt nutzt, eine Zeile hinzu. Um beispielsweise Berechtigungen für Amazon Relational Database Service (Amazon RDS) hinzuzufügen, geben Sie am Ende der letzten Zeile in der `Action` Liste ein Komma 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 dem Produkt die Rolle als Startbeschränkung zu. Diese Aktion weist darauf AWS Service Catalog hin, dass er die Rolle übernehmen soll, 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 aus und wählen Sie unter Einschränkungstyp die Option Launch aus. Klicken Sie auf Weiter.
5. Im Abschnitt Launch Constraint 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 Startbeschränkung verwendet, verwendet das Konto diesen Namen für die IAM-Rolle. Bei diesem Ansatz können die Einschränkungen für die Startrolle kontounabhängig sein, sodass Sie weniger Ressourcen pro gemeinsam genutztem Konto erstellen können.

> **Note**
>
> Der angegebene Rollenname muss in dem Konto vorhanden sein, das die Startbeschränkung erstellt hat, und im Konto des Benutzers, der ein Produkt mit dieser Startbeschränkung auf den Markt bringt.

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

## Confused Deputy wird zur Launch Constraint hinzugefügt

AWS Service Catalog unterstützt den Confused Deputy-Schutz für Benutzer APIs , die mit einer „Rolle übernehmen“ -Anforderung ausgeführt werden. Wenn Sie eine Startbeschränkung hinzufügen, können Sie den Zugriff auf die Startrolle einschränken, indem `sourceAccount` Sie die `sourceArn` Bedingungen in der Vertrauensrichtlinie für die Startrolle verwenden. Dadurch wird sichergestellt, 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 für die Startrolle angeben, um die Rolle „Annehmen“ auf das Konto 1111111111 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 über dasselbe (111111111111) verfügen. `AccountId` Andernfalls schlägt der Vorgang mit einem `AccessDenied` Fehler fehl, wodurch ein Missbrauch der Startrolle verhindert wird.

Folgendes AWS Service Catalog APIs ist für den Schutz vor Confused Deputy gesichert:

- `LaunchConstraint`

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

Der `sourceArn` Schutz für unterstützt AWS Service Catalog nur Vorlagen ARNs wie "`arn:<aws-partition>:servicecatalog:<region>:<accountId>:`". Bestimmte Ressourcen ARNs werden nicht unterstützt.

### Überprüfung der Startbeschränkung

Um zu überprüfen, ob die Rolle zum Starten des Produkts AWS Service Catalog verwendet und das Produkt erfolgreich bereitgestellt wird, starten Sie das Produkt von der AWS Service Catalog Konsole aus. 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 Catalog Konsole Service Catalog, Endbenutzer aus.
2. Wählen Sie das Produkt aus, um die Seite mit den Produktdetails zu öffnen. Vergewissern Sie sich, dass in der Tabelle mit den Startoptionen der Amazon-Ressourcenname (ARN) der Rolle angezeigt wird.
3. Wählen Sie Produkt starten.
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 Einschränkungen bei Benachrichtigungen

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

Eine Benachrichtigungsbeschränkung gibt ein Amazon SNS 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 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.

## AWS Service Catalog Einschränkungen beim Tag-Update

> **Note**
>
> AWS Service Catalog unterstützt keine Einschränkungen bei der Tag-Aktualisierung für Terraform Open Source-Produkte.

Mit Einschränkungen bei der Tag-Aktualisierung können AWS Service Catalog Administratoren Endbenutzern erlauben oder verbieten, Tags auf Ressourcen zu aktualisieren, die mit einem bereitgestellten Produkt verknüpft sind. Wenn die Aktualisierung von Tags zulässig ist, werden während eines bereitgestellten Produktupdates neue Tags, die dem Produkt oder Portfolio zugeordnet sind, auf die bereitgestellten 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.
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 Einschränkungen für Stapelsätze

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

Eine Stack-Set-Beschränkung ermöglicht es Ihnen, Produktbereitstellungsoptionen mithilfe von zu konfigurieren AWS CloudFormation StackSets. Sie können mehrere Konten und Regionen für den Produktstart angeben. Endbenutzer können diese Konten verwalten und festlegen, wo Produkte bereitgestellt werden und in welcher Reihenfolge sie bereitgestellt werden.

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 in den Kontoeinstellungen die Konten, für die Sie Produkte erstellen möchten.
   - Wählen Sie in den Regionaleinstellungen 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 StackSet IAM-Administratorrolle aus, um Ihre Zielkonten zu verwalten. Wenn Sie keine Rolle auswählen, StackSets wird der Standard-ARN verwendet. Erfahren Sie mehr über das Einrichten von Stack-Set-Berechtigungen.
6. Wählen Sie Create (Erstellen) aus.

## AWS Service Catalog Einschränkungen für Vorlagen

> **Note**
>
> AWS Service Catalog unterstützt keine Vorlagenbeschränkungen 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 Vorlagenbeschränkungen auf ein Produkt in einem

Portfolio an. AWS Service Catalog 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 einschränken, die in der dem Produkt zugrunde liegenden AWS CloudFormation Vorlage definiert sind. Die Parameter in einer AWS CloudFormation -Vorlage definieren die Menge von Werten, die Benutzer beim Erstellen eines Stacks angeben können. Ein Parameter könnte beispielsweise die verschiedenen Instance-Typen definieren, aus denen Benutzer wählen können, wenn sie einen Stack starten, der EC2 Instances enthält.

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 beispielsweise EC2 Instance-Typen beinhalten, die für Benutzer, die nur kleine Instance-Typen verwenden sollten (wie `t2.micro` oder`t2.small`), zu groß sind, können Sie eine Vorlageneinschränkung hinzufügen, um die Instance-Typen einzuschränken, die Endbenutzer wählen können. Weitere Informationen zu AWS CloudFormation Vorlagenparametern 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 Beschränkungsregeln für Vorlagen, indem Sie einen Regeleditor verwenden oder die Regeln als JSON-Text in der AWS Service Catalog Administratorkonsole schreiben. 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 Vorlagenbeschränkung anwenden möchten.

3. Erweitern Sie den Abschnitt Einschränkungen und wählen Sie Einschränkungen hinzufügen.
4. Wählen Sie im Fenster Produkt und Typ auswählen unter Produkt das Produkt aus, für das Sie die Vorlagenbeschränkungen definieren möchten. Wählen Sie dann für Einschränkungstyp die Option Vorlage aus. Klicken Sie auf Weiter.
5. Bearbeiten Sie auf der Seite Template Constraint Builder die Einschränkungsregeln mithilfe des JSON-Editors oder der Rule Builder-Schnittstelle.

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

     Um die Regeln mithilfe einer Rule Builder-Oberfläche 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 dem Erstellen einer Regel fertig sind, wählen Sie Regel hinzufügen. 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 Constraint Text Editor.
6. Wenn Sie mit der Bearbeitung der Regeln für Ihre Einschränkung fertig sind, wählen Sie „Senden“. Um die Einschränkung zu sehen, gehen Sie zur Seite mit den Portfoliodetails und erweitern Sie die Option Einschränkungen.

## Vorlageneinschränkungsregeln

Die Regeln, die Einschränkungen für Vorlagen 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 zur Erstellung des Produkts verwendet wurde, 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 also eine VPC angibt, AWS CloudFormation wertet er 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, können Sie den AWS CloudFormation Stack nicht sofort erstellen oder aktualisieren. Wenn Benutzer keine VPC angeben, wird der Wert des Subnetzparameters AWS CloudFormation nicht überprüft.

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 systeminternen Funktionen zur Definition von Regelbedingungen und Assertionen finden AWS Sie unter Regelfunktionen im Benutzerhandbuch.AWS CloudFormation

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 Serviceaktionen

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

AWS Service Catalog ermöglicht es Ihnen, den administrativen Wartungsaufwand und die Schulung von Endbenutzern zu reduzieren und gleichzeitig die Compliance- und Sicherheitsmaßnahmen einzuhalten. 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 Stop und Reboot, und Sie können auch benutzerdefinierte Aktionen definieren.

In diesem Tutorial geben Sie Endbenutzern die Möglichkeit, eine EC2 Amazon-Instance 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 vollständige AWS Administratorrechte verfügen AWS Service Catalog, mit denen Sie bereits vertraut sind und dass Sie bereits über eine Reihe von Produkten, Portfolios und Benutzern verfügen. Wenn Sie damit nicht vertraut sind AWS Service Catalog, schließen Sie die Einrichtung und die 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: Verwaltung von Serviceaktionen mit AWS CloudFormation
- Schritt 6: Problembehandlung


## Schritt 1: Konfigurieren von Berechtigungen für Endbenutzer

Endbenutzer müssen über die erforderlichen Berechtigungen verfügen, um bestimmte Serviceaktionen anzeigen und ausführen zu können. In diesem Beispiel benötigt der Endbenutzer die Erlaubnis, auf die AWS Service Catalog Serviceaktionsfunktion zuzugreifen und einen EC2 Amazon-Neustart durchzuführen.

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 nach Benutzergruppen.
3. Wählen Sie die Gruppen aus, die Endbenutzer für den Zugriff auf AWS Service Catalog Ressourcen 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 der vorhandenen Richtlinie Berechtigungen hinzu, indem wir die benutzerdefinierte Richtlinie auswählen, die für die Berechtigungen AWS Service Catalog Bereitstellen und Beenden der Gruppe 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 EC2 Amazon-Neustartaktion in durchzuführen AWS Service Catalog.

## Schritt 2: Erstellen einer Service-Aktion

Als Nächstes erstellen Sie eine Service-Aktion, um EC2 Amazon-Instances neu zu starten.

1. Öffnen Sie die AWS Service Catalog Konsole 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 Dienstaktionen die Option Aktion erstellen aus.
4. Wählen Sie auf der Seite Aktion erstellen ein AWS Systems Manager Dokument aus, um die Serviceaktion zu definieren. Die Aktion Amazon EC2 Instance Restart wird durch ein AWS Systems Manager Dokument definiert, daher behalten wir die Standardoption im Drop-down-Menü, Amazon-Dokumente, bei.
5. Suchen Sie nach der Aktion AWS-Restart EC2 Instance 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 Instanz-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 mit den Dienstaktionen die Option AWS-Restart EC2instance und anschließend 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 bei der AWS Service Catalog Konsole an.
2. Wählen Sie auf dem AWS Service Catalog Dashboard im Navigationsbereich die Option 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 mit den Produktdetails für bereitgestellte Produkte oben rechts die Option Aktionen und dann die Aktion AWS EC2instance-Neustart aus.
5. Bestätigen Sie, dass Sie die benutzerdefinierte Aktion ausführen möchten. Sie erhalten eine Bestätigung über das Senden der Aktion.

## Schritt 5: Verwaltung von Serviceaktionen mit AWS CloudFormation

Sie können Serviceaktionen und deren Verknüpfungen mit AWS CloudFormation Ressourcen erstellen. Weitere Informationen finden Sie in folgenden Themen im AWS CloudFormation - Benutzerhandbuch:

- AWS::ServiceCatalog::CloudFormationProduct ProvisioningArtifactProperties
- AWS::ServiceCatalog::ServiceActionAssoziation

> **Note**
>
> Wenn Sie Serviceaktionsverknüpfungen mit AWS CloudFormation Ressourcen verwalten, fügen oder entfernen Sie keine Dienstaktionen über das AWS Command Line Interface oder AWS Management Console. Wenn Sie ein Stack-Update durchführen, werden alle Änderungen an Serviceaktionen, die außerhalb von AWS CloudFormation vorgenommen wurden, ersetzt.

## Schritt 6: Problembehandlung

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)

AWS Service Catalog es 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 Dienstaktion wurde durch den Back-End-Dienst, z. B. SSM, gedrosselt.

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

AWS Service Catalog konnte die in der Definition der Serviceaktion angegebene Rolle nicht annehmen. Stellen Sie sicher, dass der Principal servicecatalog.amazonaws.com oder ein regionaler Principal wie servicecatalog.us-east-1.amazonaws.com in der Vertrauensrichtlinie der Rolle auf der Zulassungsliste steht.

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

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

Es wurden keine Ressourcen mit dem Typ des bereitgestellten ***TargetType*** Produkts gefunden

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)

AWS Service Catalog ist bei der Übernahme der angegebenen Rolle auf einen unbekannten Fehler gestoßen.

Der Wert "***InvalidValue***" des Parameters wurde nicht gefunden in ***{ValidValue1}, {ValidValue2}***

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

Fehler beim Parametertyp. Der angegebene Wert für ***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 übergeben AWS Service Catalog , der in der Definition der Serviceaktion nicht definiert ist. Sie können nur Parameter verwenden, die in der Service-Aktionsdefinition definiert sind.

Der Schritt schlägt fehl, wenn eine Aktion ausführt/abgebrochen wird. ***Error message.*** Weitere Einzelheiten zur Diagnose finden Sie im Automation Service Troubleshooting Guide.

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

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

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

TargetType für das SSM Automation-Dokument nicht definiert

Für Serviceaktionen muss für SSM-Automatisierungsdokumente ein TargetType definiertes. Überprüfen Sie Ihr SSM-Automatisierungsdokument.

# AWS Marketplace Produkte zu Ihrem Portfolio hinzufügen

Sie können AWS Marketplace Produkte zu Ihren Portfolios hinzufügen, um diese Produkte Ihren AWS Service Catalog Endbenutzern zur Verfügung zu stellen.

AWS Marketplace ist ein Online-Shop, in dem Sie eine große Auswahl an Software und Diensten finden, abonnieren und sofort nutzen können. Zu den angebotenen Produkten AWS Marketplace gehören Datenbanken, Anwendungsserver, Testtools, Überwachungstools, Content-Management-Tools und Business Intelligence-Software. AWS Marketplace ist verfügbar unterhttps://aws.amazon.com/marketplace. Beachten Sie, dass Sie keine Software-as-a-Service (SaaS) -Produkte von AWS Marketplace bis hinzufügen können AWS Service Catalog.

Sie verteilen ein AWS Marketplace Produkt an AWS Service Catalog Endbenutzer AWS Service Catalog, indem Sie das Produkt mit der AWS CloudFormation Vorlage kopieren und es dann einem Portfolio hinzufügen.

> **Note**
>
> AWS Service Catalog unterstützt nicht den Vertrieb 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 oder das Abonnieren und Hinzufügen von Produkten mithilfe der manuellen Option. Wir empfehlen, Produkte mithilfe der Funktionen hinzuzufügen, die speziell dafür entwickelt wurden AWS Service Catalog.

## AWS Marketplace Produkte verwalten mit AWS Service Catalog

Sie können Ihre abonnierten AWS Marketplace Produkte direkt AWS Service Catalog über eine benutzerdefinierte Oberfläche hinzufügen. Wählen Sie unter AWS Marketplace die Option Service Catalog aus. Weitere Informationen finden Sie in der AWS Marketplace Hilfe und AWS Service Catalog in den häufig gestellten Fragen unter Produkte kopieren nach.

## Manuelles Verwalten und Hinzufügen von AWS Marketplace Produkten

Gehen Sie wie folgt vor, um ein AWS Marketplace Produkt zu abonnieren, dieses Produkt in einer AWS CloudFormation Vorlage zu definieren und die Vorlage einem AWS Service Catalog Portfolio hinzuzufügen.

Um ein AWS Marketplace Produkt zu abonnieren

1. Gehe zu AWS Marketplace athttps://aws.amazon.com/marketplace.
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, um die Versandseite aufzurufen, und wählen Sie dann den Tab Manueller Start.

   Die Informationen auf der Versandseite umfassen die unterstützten Amazon Elastic Compute Cloud (Amazon EC2) -Instance-Typen AWS-Regionen, die unterstützten und die Amazon Machine Image (AMI) -ID, die das Produkt für jede AWS Region verwendet. Beachten Sie, dass bei einigen Optionen Kosten anfallen. Sie werden diese Informationen verwenden, um die AWS CloudFormation Vorlage in späteren Schritten anzupassen.

4. Wählen Sie Accept Terms aus, um das Produkt zu abonnieren.

   Nachdem Sie ein Produkt abonniert haben, können Sie jederzeit auf die Informationen auf der Seite zur AWS Marketplace Produktabwicklung zugreifen, indem Sie Ihre Software und dann das Produkt auswählen.

Um Ihr AWS Marketplace Produkt in einer AWS CloudFormation Vorlage zu definieren

Um die folgenden Schritte durchzuführen, verwenden Sie eine der AWS CloudFormation Beispielvorlagen als Ausgangspunkt und passen die Vorlage so an, dass sie Ihr AWS Marketplace Produkt darstellt. Informationen zum Zugriff auf die Beispielvorlagen finden Sie unter Mustervorlagen im AWS CloudFormation -Benutzerhandbuch.

1. Wählen Sie auf der Seite Mustervorlagen im AWS CloudFormation Benutzerhandbuch eine AWS Region 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. Wählen Sie den Link Dienste, um eine Liste mit Mustervorlagen für Dienste anzuzeigen, die für die Region geeignet sind.
3. Sie können ein beliebiges Beispiel, das für Ihre Zwecke geeignet ist, als Ausgangspunkt verwenden. Die Schritte in diesem Verfahren verwenden die EC2 Amazon-Instance in einer Sicherheitsgruppenvorlage. 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 `InstanceType` Parameter so an, dass er nur EC2 Instance-Typen enthält, die von Ihrem Produkt unterstützt werden. Wenn Ihre Vorlage EC2 Instance-Typen enthält, die nicht unterstützt werden, kann das Produkt für Ihre Endbenutzer nicht gestartet werden.

   a. Sehen Sie sich auf der Seite zur AWS Marketplace Produktabwicklung in im Abschnitt Preisdetails die unterstützten EC2 Instanztypen an.

**On-Demand Plans for Amazon EC2**

**Select a region, operating system, instance type, and vCPU to view rates**

Region: US East (N. Virginia)

Operating system: Linux

Instance type: All

vCPU: All

**Viewing 364 of 364 available instances**

1 2 3 4 5 6 7 ... 19

| Instance name | On-Demand hourly rate | vCPU | Memory | Storage | Network performance |
|---|---|---|---|---|---|
| a1.medium | $0.0255 | 1 | 2 GiB | EBS Only | Up to 10 Gigabit |
| a1.large | $0.051 | 2 | 4 GiB | EBS Only | Up to 10 Gigabit |
| a1.xlarge | $0.102 | 4 | 8 GiB | EBS Only | Up to 10 Gigabit |
| a1.2xlarge | $0.204 | 8 | 16 GiB | EBS Only | Up to 10 Gigabit |
| a1.4xlarge | $0.408 | 16 | 32 GiB | EBS Only | Up to 10 Gigabit |
| a1.metal | $0.408 | 16 | 32 GiB | EBS Only | Up to 10 Gigabit |
| t4g.nano | $0.0042 | 2 | 0.5 GiB | EBS Only | Up to 5 Gigabit |

b. Ändern Sie in Ihrer Vorlage den Standard-Instance-Typ in einen unterstützten EC2 Instance-Typ Ihrer Wahl.

c. Bearbeiten Sie die `AllowedValues` Liste so, dass sie nur EC2 Instance-Typen enthält, die von Ihrem Produkt unterstützt werden.

d. Entfernen Sie alle EC2 Instance-Typen, die Ihre Endbenutzer nicht verwenden sollen, wenn sie das Produkt starten, aus der `AllowedValues` Liste.

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 `Mappings` Abschnitt Ihrer Vorlage die `AWSInstanceType2Arch` Zuordnungen so, dass nur unterstützte EC2 Instanztypen und Architekturen enthalten sind.

   a. Bearbeiten Sie die Liste der Zuordnungen, indem Sie alle EC2 Instanztypen entfernen, die nicht in der Liste für den `AllowedValues` Parameter enthalten sind. `InstanceType`

   b. Bearbeiten Sie den `Arch` Wert für jeden EC2 Instanztyp so, dass er dem Architekturtyp entspricht, 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 darüber, welche Architekturen von EC2 Instance-Familien unterstützt werden, finden Sie in der Amazon Linux AMI Instance Type 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. Sehen Sie sich auf der Produktabwicklungsseite in AWS Marketplace die AMI-ID an, 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 Zuordnung für jede Region, um die nicht unterstützten Architekturen (`PV64``HVM64`, oder`HVMG2`) und das zugehörige AMI zu entfernen. IDs

   d. Geben Sie für jede verbleibende AWS Regions- und Architekturzuordnung die entsprechende AMI-ID auf der Produktdetailseite unter an AWS 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.

Um Ihr AWS Marketplace Produkt zu einem AWS Service Catalog Portfolio hinzuzufügen

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 Portfolio-Seite das Portfolio aus, zu 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.
8. Vergewissern Sie sich auf der Seite „Überprüfen“, dass 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.

# Benutzen AWS CloudFormation StackSets

> **Note**
>
> AutoTags werden derzeit nicht unterstützt mit AWS CloudFormation StackSets.

Sie können AWS CloudFormation StackSets es verwenden, um AWS Service Catalog Produkte für mehrere AWS-Regionen Konten auf den Markt zu bringen. Sie können die Reihenfolge angeben, in der Produkte nacheinander bereitgestellt werden. AWS-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 Stapel in AWS Konten in verschiedenen AWS Regionen erstellen.

Eine Stack-Instance bezieht sich auf einen Stack in einem Zielkonto innerhalb einer AWS Region und ist nur einem Stack-Set zugeordnet.

Weitere Informationen finden Sie unter StackSets-Konzepte.

## Stack-Set-Einschränkungen

In können Sie Stack-Set-Einschränkungen verwenden AWS Service Catalog, um Optionen für die Produktbereitstellung zu konfigurieren.

AWS Service Catalog unterstützt Stack-Set-Beschränkungen für Produkte in zwei Kategorien AWS GovCloud (US) Regions: AWS GovCloud (US-West) und AWS GovCloud (US-Ost).

Weitere Informationen finden Sie unter AWS Service Catalog Stack Set Constraints.

# Verwalten von Budgets

Mithilfe von AWS Budgets können Sie Ihre Servicekosten und die damit verbundene Nutzung nachverfolgen AWS Service Catalog. Sie können Budgets AWS Service Catalog Produkten und Portfolios zuordnen.

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

AWS Budgets bietet Ihnen die Möglichkeit, benutzerdefinierte Budgets festzulegen, die Sie benachrichtigen, wenn Ihre Kosten oder Nutzung Ihren budgetierten Betrag überschreiten (oder voraussichtlich überschreiten werden). 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 können, müssen Sie die Tags für die Kostenzuweisung in der AWS Fakturierung und Kostenmanagement Konsole aktivieren. Weitere Informationen finden Sie unter Benutzerdefinierte Kostenzuordnungs-Tags aktivieren im AWS Fakturierung und Kostenmanagement -Benutzerhandbuch.

> **Note**
>
> Die Aktivierung von Tags dauert bis zu 24 Stunden.

Sie müssen außerdem den Benutzerzugriff auf die AWS Fakturierung und Kostenmanagement Konsole für alle Benutzer oder Gruppen aktivieren, die die Budgetfunktion 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 SNS-Benachrichtigungen verwenden möchten, können Sie Benutzern die Möglichkeit geben, Amazon SNS SNS-Benachrichtigungen zu erstellen, wie im folgenden Richtlinienbeispiel gezeigt.

So erstellen Sie die Budgets-Richtlinie

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Policies.
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, sodass Sie entsprechende

Maßnahmen ergreifen können. Um ein Budget zu erstellen, entscheiden Sie zunächst, welchem Produkt oder Portfolio Sie das Budget zuordnen 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.
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 Sie das Portfolio, das Produkt und den Benutzer, der ein Produkt auf den Markt gebracht hat. AWS Service Catalog wendet diese Tags automatisch auf bereitgestellte Ressourcen an. A TagOption ist ein vom Administrator definiertes Schlüssel-Wert-Paar, das in verwaltet wird. AWS 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. AWS Budgets Wählen Sie Erstellen in. Sie werden zur Seite „Budget festlegen“ weitergeleitet. Fahren Sie mit der Einrichtung Ihres Budgets fort, indem Sie die Schritte unter Budget erstellen 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 werden. Jedes Budget kann mehreren Portfolios und Produkten zugeordnet werden.

Wenn Sie einem Portfolio oder Produkt ein Budget zuordnen, können Sie Informationen zum Budget auf der Detailseite dieses Portfolios oder Produkts einsehen. Damit Ausgaben, die für das Portfolio

oder Produkt getätigt werden, im Budget berücksichtigt werden, müssen Sie dem Budget und dem Portfolio oder Produkt dieselben Tags zuordnen.

> **Note**
>
> Wenn Sie ein Budget aus löschen AWS Budgets, bestehen weiterhin Verknüpfungen zu AWS Service Catalog Produkten und Portfolios. AWS Service Catalog kann keine Informationen über das 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.
5. Wählen Sie auf der Seite „Budgetzuordnung“ ein vorhandenes Budget aus und klicken Sie dann auf Weiter.
6. Die Tabelle mit Produkten 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 zum Budget auf den Seiten Produktdetails und Produktliste einsehen. Wenn ein Budget einem Portfolio zugeordnet ist, können Sie Informationen zum Budget auf den Seiten Portfolios und Portfoliodetails einsehen.

Auf den Seiten Portfolios und Produktlisten werden Budgetinformationen für bestehende 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 sich für ein Produkt oder Portfolio entscheiden, werden Sie auf eine Detailseite weitergeleitet. Die Seiten mit den Portfoliodetails und den 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 Verknüpfungen 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 die Option Budget trennen aus. Eine Bestätigungswarnung wird angezeigt.
5. Nachdem Sie bestätigt haben, dass Sie das Budget aus dem Produkt oder Portfolio entfernen möchten, wählen Sie Bestätigen.

# Verwalten von bereitgestellten Produkten

AWS Service Catalog bietet eine Schnittstelle für die Verwaltung bereitgestellter Produkte. 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


- Verwaltung der bereitgestellten Produkte als Administrator
- Ändern des Besitzers des bereitgestellten Produkts
- Vorlagen für bereitgestellte Produkte aktualisieren
- Tutorial: Identifizieren der Benutzerressourcenzuordnung
- Verwaltung von Fehlern im Terraform Open Source-Produktstatus
- Verwaltung der Terraform Open Source-Produktstatusdatei


## Verwaltung der bereitgestellten Produkte als Administrator

Um alle bereitgestellten Produkte für ein Konto zu verwalten, benötigen Sie `AWSServiceCatalogAdminFullAccess` oder eine gleichwertige 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 Vorlage für Produktartefakte auf die Ausgaben der bereitgestellten 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.

So zeigen Sie alle bereitgestellten Produkte an und verwalten sie

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

   Wenn Sie bereits an 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 Ansicht: und wählen Sie die Zugriffsebene aus, die Sie sehen möchten: 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 sie 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 Option Liste der bereitgestellten Produkte aus.
2. Suchen Sie das bereitgestellte Produkt, das Sie aktualisieren möchten, klicken Sie auf die drei Punkte daneben und wählen Sie Eigentümer des bereitgestellten Produkts ändern aus.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

# Vorlagen für bereitgestellte Produkte aktualisieren

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 ändern.

> **Note**
>
> Das Aktualisieren von Vorlagen wird für bereitgestellte Terraform Open Source- oder Terraform Cloud-Produkte nicht unterstützt. Wenn Sie eine andere Vorlage für ein vorhandenes Terraform-Produkt verwenden möchten, müssen Sie das Produkt löschen und dann mit der gewünschten Vorlage ein neues Produkt erstellen.

Um eine Vorlage für ein bereitgestelltes Produkt zu aktualisieren

1. Wählen Sie im linken Navigationsmenü die Option Bereitgestellte Produkte aus.
2. Wählen Sie unter Bereitgestellte Produkte ein bereitgestelltes Produkt aus und wählen Sie Aktionen, Update aus.

   Beachten Sie, dass Sie auf der Seite mit den bereitgestellten Produktdetails auch Aktionen, Update auswählen können.
3. (Optional) Wählen Sie unter Produktdetails die Option Produkt ändern aus.

   Beachten Sie unter Produkt ändern die folgende Warnung:

Wenn Sie das Produkt ändern, wird dieses bereitgestellte Produkt auf eine andere Produktvorlage aktualisiert. Dadurch können Ressourcen beendet und neue Ressourcen erstellt werden.

Sie können ein bereitgestelltes Produkt innerhalb desselben Produkts auf eine andere Version aktualisieren.

4. (Optional) Wählen Sie unter Produkte das Produkt aus, das Sie mit einer anderen Vorlage aktualisieren möchten. Wählen Sie dann Ändern.

   Beachten Sie in den Produktdetails die folgende Warnung:

   [Produktname] wird von [aktueller Vorlagenname] auf [neuer Vorlagenname] aktualisiert. Der Name Ihres bereitgestellten Produkts, [Name des bereitgestellten Produkts], wird sich jedoch nicht ändern.

   Sie können ein bereitgestelltes Produkt innerhalb desselben Produkts auf eine andere Version aktualisieren.

5. Wählen Sie unter Produktversionen die Version des gewünschten Produkts aus.
6. Wählen Sie unter Parameter die entsprechenden Parameter aus.
7. Wählen Sie Aktualisieren.

   In den bereitgestellten Produktdetails finden Sie die Details des Updates. Der Name des bereitgestellten Produkts ändert sich nicht, aber das bereitgestellte Produkt hat jetzt eine andere Vorlage.

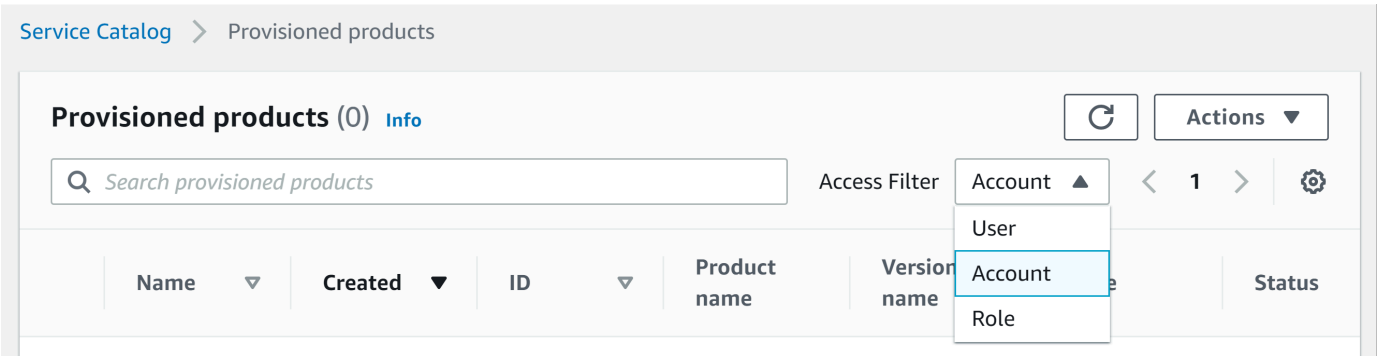
# Tutorial: Identifizieren der Benutzerressourcenzuordnung

Sie können den Benutzer, der ein Produkt bereitgestellt hat, und die mit dem Produkt verknüpften Ressourcen mithilfe der Konsole identifizieren. AWS Service Catalog In diesem Tutorial lernen Sie, wie Sie dieses Beispiel auf Ihre spezifischen bereitgestellten Produkte übertragen.

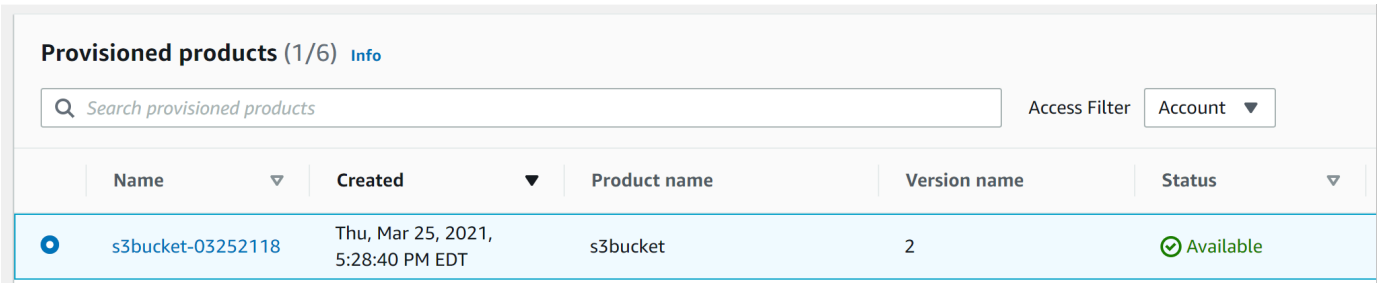
Um alle bereitgestellten Produkte für das Konto zu verwalten, benötigen Sie `AWSServiceCatalogAdminFullAccess`- oder entsprechenden Zugriff auf die Schreibvorgänge des bereitgestellten Produkts. Weitere Informationen finden Sie unter Identity and Access Management im AWS Service Catalog Administratorhandbuch.

So identifizieren Sie den Benutzer, der ein Produkt und die damit verbundenen Ressourcen bereitgestellt hat

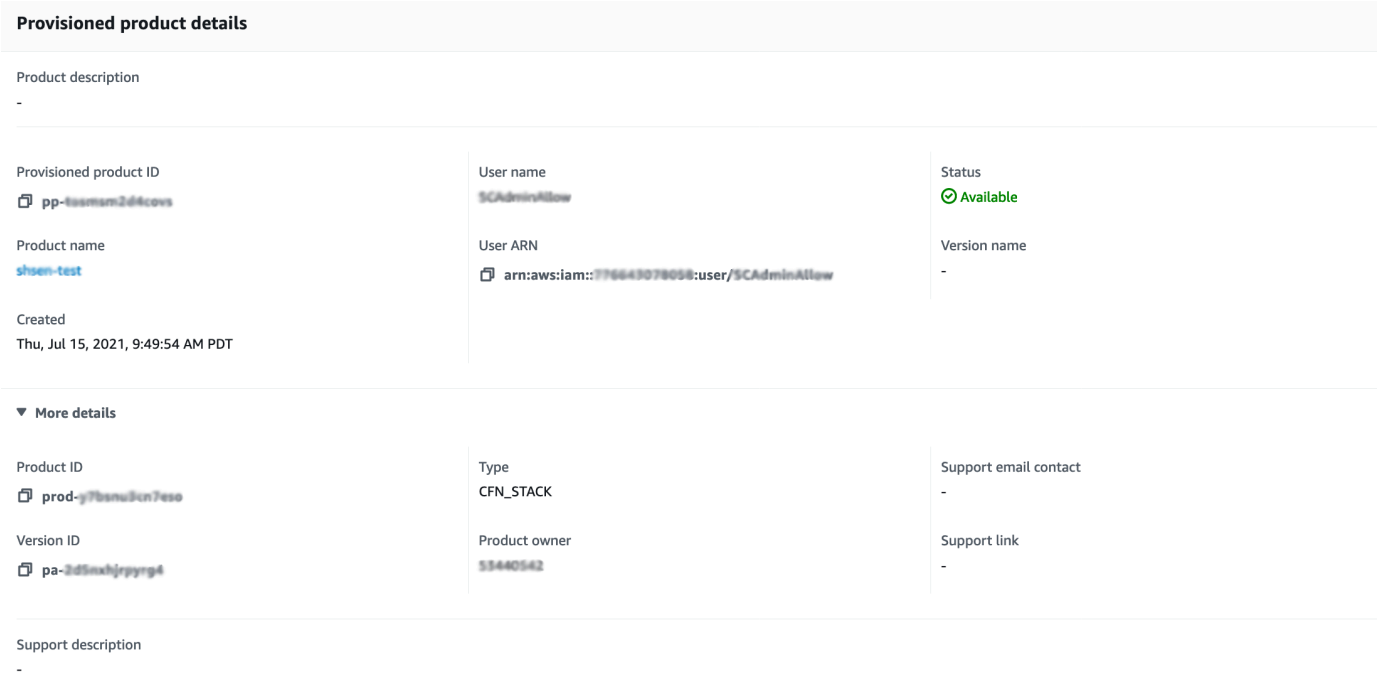
1. Öffnen Sie https://console.aws.amazon.com/servicecatalog.
2. Wählen Sie im linken Navigationsmenü die Option Bereitgestelltes Produkt aus.
3. Wählen Sie im Dropdownmenü Access Filter die Option Account aus.



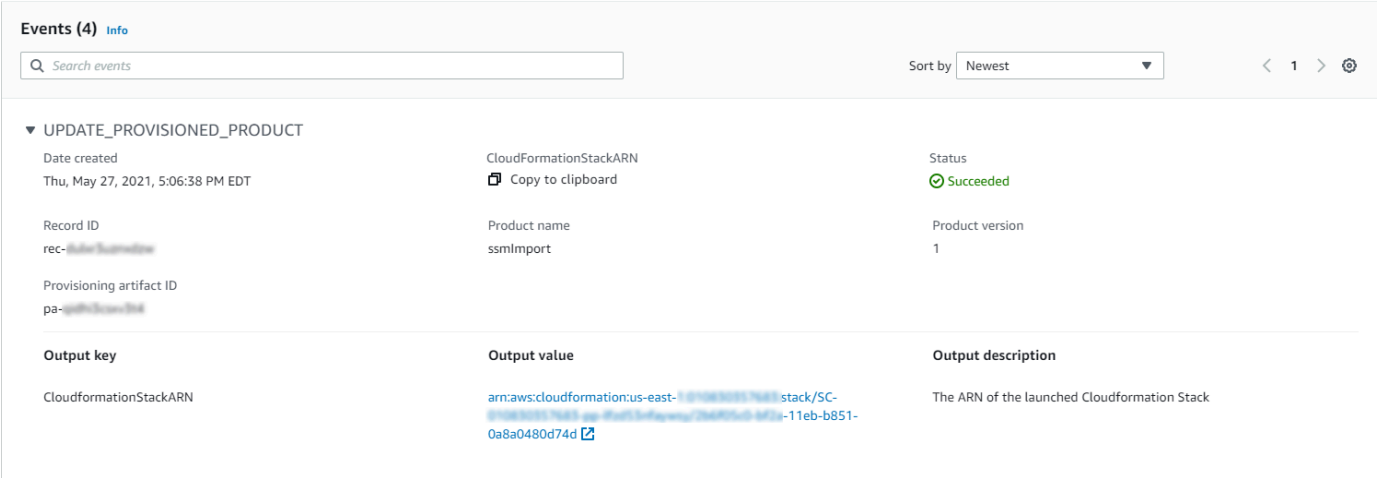

4. Wählen Sie in der Kontoansicht ein bereitgestelltes Produkt aus und öffnen Sie es, um dessen Details anzuzeigen.




Sie können die Details des bereitgestellten Produkts sehen.




5. Scrollen Sie nach unten, um den Abschnitt Ereignisse zu erweitern. Notieren Sie sich die `CloudformationStackARN` Werte `Provisioned product ID` und.




6. Identifizieren Sie anhand der bereitgestellten Produkt-ID den AWS CloudTrail Datensatz, der diesem Launch entspricht, und identifizieren Sie den anfragenden Benutzer (in der Regel geben Sie beim Verbund 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 und 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 mithilfe der AWS Service Catalog API oder der ausführen AWS CLI. Weitere Informationen finden Sie im AWS Service Catalog Entwicklerhandbuch. und AWS Service Catalog Befehlszeilenreferenz.

## Verwaltung von Fehlern im Terraform Open Source-Produktstatus

Terraform Open `ProvisionProduct` Source-Fehler werden an den `TAINTED` Status weitergeleitet, sodass jedes bereitgestellte Produkt weitermachen kann. `UpdateProvisionedProduct` Wenn das passiert:

- `UpdateProvisionedProduct`unternimmt keinen Versuch, Tags zu aktualisieren oder zu korrigieren oder eine Ressourcengruppe zu erstellen oder zu ändern.
- `UpdateProvisionedProduct`berücksichtigt bei der Entscheidung, ob das bereitgestellte Produkt auf oder eingestellt werden soll, Fehler aus früheren Bereitstellungsvorgängen nicht. `AVAILABLE` `TAINTED`

AWS Service Catalog wendet Tags nur währenddessen an. `ProvisionProduct` Jedes fehlgeschlagene Tagging, das auf einen Fehlschlag des `ProvisionProduct` Vorgangs zurückzuführen ist, wird nicht automatisch behoben.

## Beispiele für Statusfehler

### Beispiel 1: erstellt AWS Service Catalog keine Ressourcengruppe während `ProvisionProduct`

Im folgenden Szenario befindet sich ein bereitgestelltes Produkt im `AVAILABLE` Status, auch wenn es keine unterstützende Ressourcengruppe gibt, und es wurden keine Tags auf die Ressourcen angewendet.

1. Ihre Aktion wird eingeleitet`ProvisionProduct`.
2. Die Terraform-Provisioning-Engine reagiert `ProvisionProduct` mit einem Workflow-Fehler und bietet keine. `ResourceIdentifier`
3. Der `ProvisionProduct` Workflow erstellt keine Ressourcengruppe und setzt dann den Status des bereitgestellten Produkts auf. `ERROR`
4. Anschließend initiieren Sie den `UpdateProvisionedproduct` Vorgang.
5. Die Terraform-Provisioning-Engine reagiert mit der Meldung „Erfolg“.
6. Infolgedessen 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 befindet sich ein bereitgestelltes Produkt auch dann im `AVAILABLE` Status, wenn auf neue Ressourcen keine Tags angewendet wurden.

1. Ihre Aktion wird eingeleitet`ProvisionProduct`.
2. Die Terraform-Provisioning-Engine reagiert mit der Meldung „Erfolg“ und bietet eine. `ResourceIdentifier`
3. Der `ProvisionProduct` Workflow erstellt eine Ressourcengruppe und wendet Tags auf alle identifizierten Ressourcen an.
4. Sie `UpdateProvisionedProduct` initiieren ein neues Artefakt, das neue Ressourcen erzeugt.
5. Die Terraform-Provisioning-Engine reagiert mit der Meldung „Erfolg“.
6. Der `UpdateProvisionedProduct` Workflow setzt den Status des bereitgestellten Produkts auf, versucht `AVAILABLE` aber nicht, zusätzliche Tags auf die neuen Ressourcen anzuwenden.

### Lösung für Statusfehler

AWS Service Catalog stellt sicher, dass eine Ressourcengruppe für alle bereitgestellten Produkte mit der Einstellung `TAINTED` von `ProvisionProduct` erstellt wird. Wenn die Terraform-Provisioning-Engine keine Ressourcengruppe zurückgibt oder keine Ressourcengruppe erstellt, wird das bereitgestellte Produkt auf den `ERROR` Status gesetzt und Sie müssen es beenden. `ResourceIdentifier` AWS Service Catalog

## Verwaltung der Terraform Open Source-Produktstatusdatei

Jedes von Terraform Open Source bereitgestellte Produkt verfügt über eine Datei mit einem einzigen Status. Es besteht eine 1:1 -Beziehung zwischen dem bereitgestellten Produkt und seiner Statusdatei. Die Dateien werden in einem Amazon S3 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 die EC2 Amazon-Startvorlagen beschränkt. AWS Service Catalog Administratoren haben keinen direkten Zugriff auf die Statusdateien in Amazon S3. Administratoren müssen über Amazon auf die Dateien zugreifen EC2. Standardmäßig können AWS Service Catalog Administratoren die Liste der Statusdateien sehen, den Dateiinhalt jedoch nicht lesen oder schreiben. Nur die Terraform Provisioning Engine kann den Dateiinhalt lesen oder schreiben.

# Tags verwalten in AWS Service Catalog

AWS Service Catalog stellt Tags bereit, mit denen 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 identifizieren AWS Service Catalog und von diesen automatisch AWS Service Catalog auf bereitgestellte Ressourcen angewendet werden.

TagOptions werden darin verwaltete Schlüssel-Wert-Paare, die als Vorlagen für AWS Service Catalog die Erstellung von Tags dienen. AWS

Themen


- AWS Service Catalog AutoTags
- AWS Service Catalog TagOption Bücherei


## AWS Service Catalog AutoTags

> **Note**
>
> AWS Service Catalog unterstützt AutoTags keine Terraform Open Source-Produkte.

AutoTags sind Tags, die Informationen über den Ursprung einer bereitgestellten Ressource identifizieren AWS Service Catalog und von diesen automatisch auf bereitgestellte Ressourcen angewendet werden AWS Service Catalog .

AutoTags umfassen 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 werden nicht auf das 50-Tag-Limit des Kunden angerechnet.


> **Note**
>
> AWS Service Catalog unterstützt AutoTags keine Terraform Open Source-Produkte.

AWS Service Catalog AutoTags kann Ihnen helfen, Ihre Ressourcen einheitlich zu kennzeichnen. Dies ist hilfreich, wenn Sie Budgets für ein Portfolio, ein Produkt oder einen Benutzer festlegen. Sie können den auch verwenden, um Ressourcen für Operationen AutoTags nach der Markteinführung zu identifizieren, z. B. für die Festlegung AWS Config von Regeln. AutoTags Informationen zu Ihren bereitgestellten Ressourcen finden Sie im Abschnitt Tags der Downstream-Services, die für die Bereitstellung verwendet werden AWS CloudFormation, wie Amazon und Amazon EC2 S3.

> **Note**
>
> AWS Service Catalog wird nicht aktualisiert, AutoTags nachdem Sie sich für bereitgestellte Ressourcen AutoTags angemeldet haben. Wenn Sie das bereitgestellte Produkt auf ein anderes Produkt, ein bereitgestelltes Artefakt oder einen neuen Startpfad aktualisieren, werden für die vorhandenen Produkte AutoTags weiterhin die ursprünglichen Werte angezeigt.

AutoTag Einzelheiten

- 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 Provisioning-Prinzipals (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 Bücherei

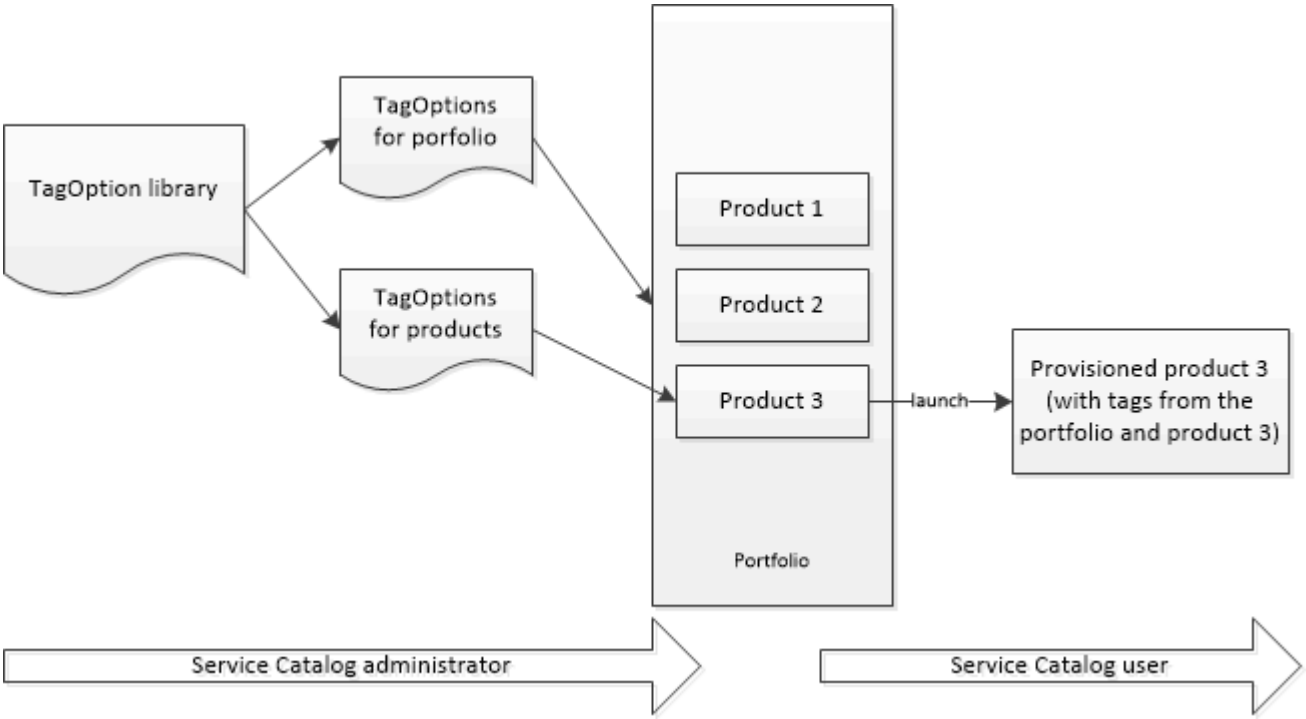
AWS Service Catalog Stellt eine TagOption Bibliothek bereit, um Administratoren die einfache Verwaltung von Tags auf bereitgestellten Produkten zu ermöglichen. A TagOption ist ein Schlüssel-Wert-Paar, das in verwaltet wird. AWS Service Catalog Es ist kein AWS Tag, sondern dient als Vorlage für die Erstellung eines AWS Tags auf der Grundlage von. TagOption

AWS Service Catalog unterstützt TagOptions keine Terraform Open Source- oder Terraform Cloud-Produkte.

Die TagOption Bibliothek macht es einfacher, Folgendes durchzusetzen:

- Eine einheitliche Taxonomie
- Richtiges Markieren von Ressourcen AWS Service Catalog
- Definierte, vom Benutzer auswählbare Optionen für die zulässigen Tags

Administratoren können Portfolios und Produkten zuordnen TagOptions . AWS Service Catalog Aggregiert bei einer Produkteinführung (Bereitstellung) das zugehörige Portfolio und das zugehörige Produkt TagOptions und wendet sie auf das bereitgestellte Produkt an, wie in der folgenden Abbildung dargestellt.




Mit der TagOption Bibliothek können Sie ihre Verknüpfungen zu Portfolios oder Produkten deaktivieren TagOptions und beibehalten und sie bei Bedarf wieder aktivieren. Dieser Ansatz trägt nicht nur dazu bei, die Integrität der Bibliothek zu wahren, sondern ermöglicht Ihnen auch TagOptions die Verwaltung der Dateien, die möglicherweise nur sporadisch 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 Reference.

Inhalt

- Ein Produkt auf den Markt bringen mit TagOptions

- Verwaltung TagOptions
- Verwendung TagOptions mit AWS Organizations Tag-Richtlinien

## Ein Produkt auf den Markt bringen mit TagOptions

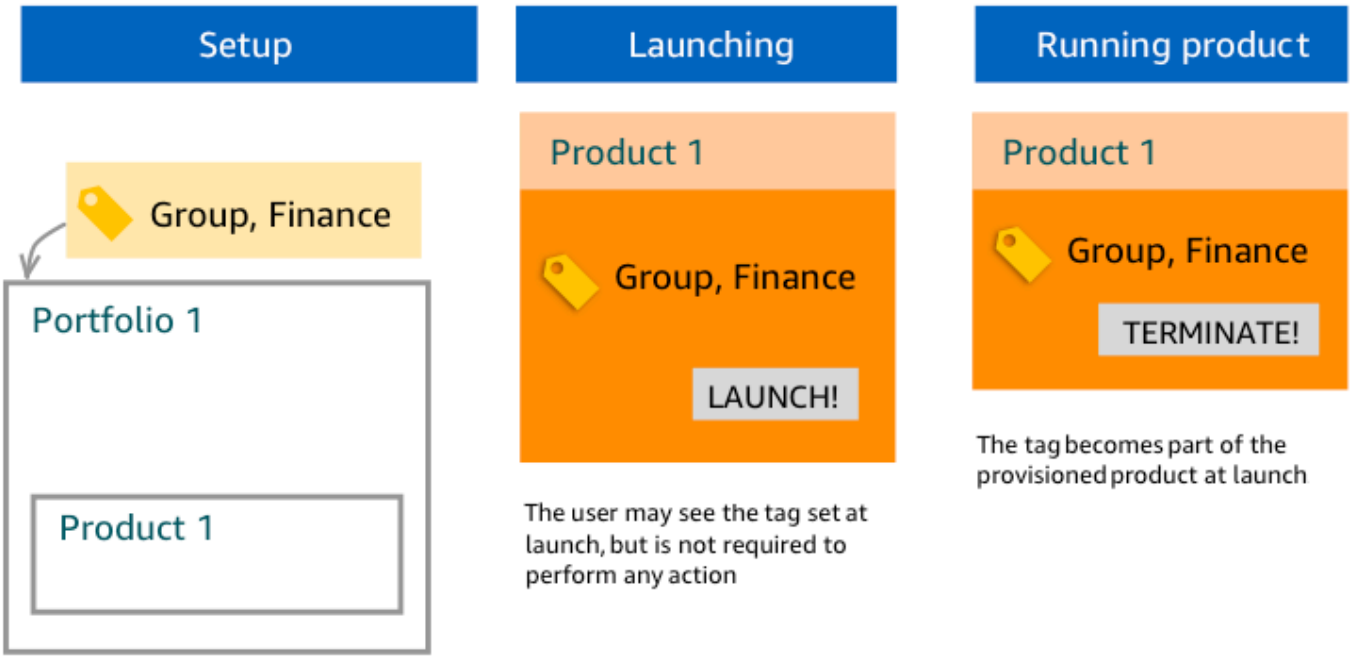
Wenn ein Benutzer ein Produkt auf den Markt bringt TagOptions, AWS Service Catalog führt er in Ihrem Namen die folgenden Aktionen durch:

- Sammelt alles TagOptions für das Produkt und das Einführungsportfolio.
- Stellt sicher, dass nur TagOptions eindeutige Schlüssel 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 das beim Start TagOptions funktioniert.

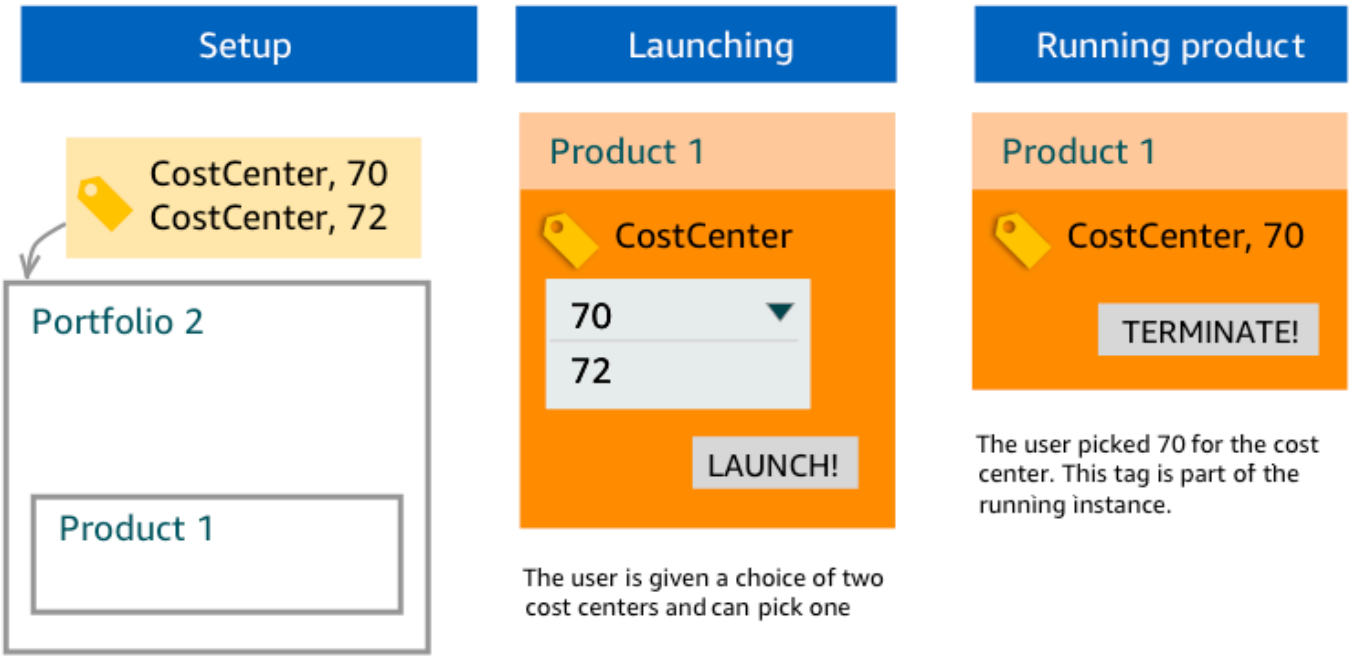
### Beispiel 1: Ein eindeutiger TagOption Schlüssel

Ein Administrator erstellt TagOption[Group=Finance] und ordnet es Portfolio1 zu, bei dem Product1 die Nr. TagOptions Wenn ein Benutzer das bereitgestellte Produkt startet, TagOption wird die Single wie folgt zu Tag [Group=Finance]:



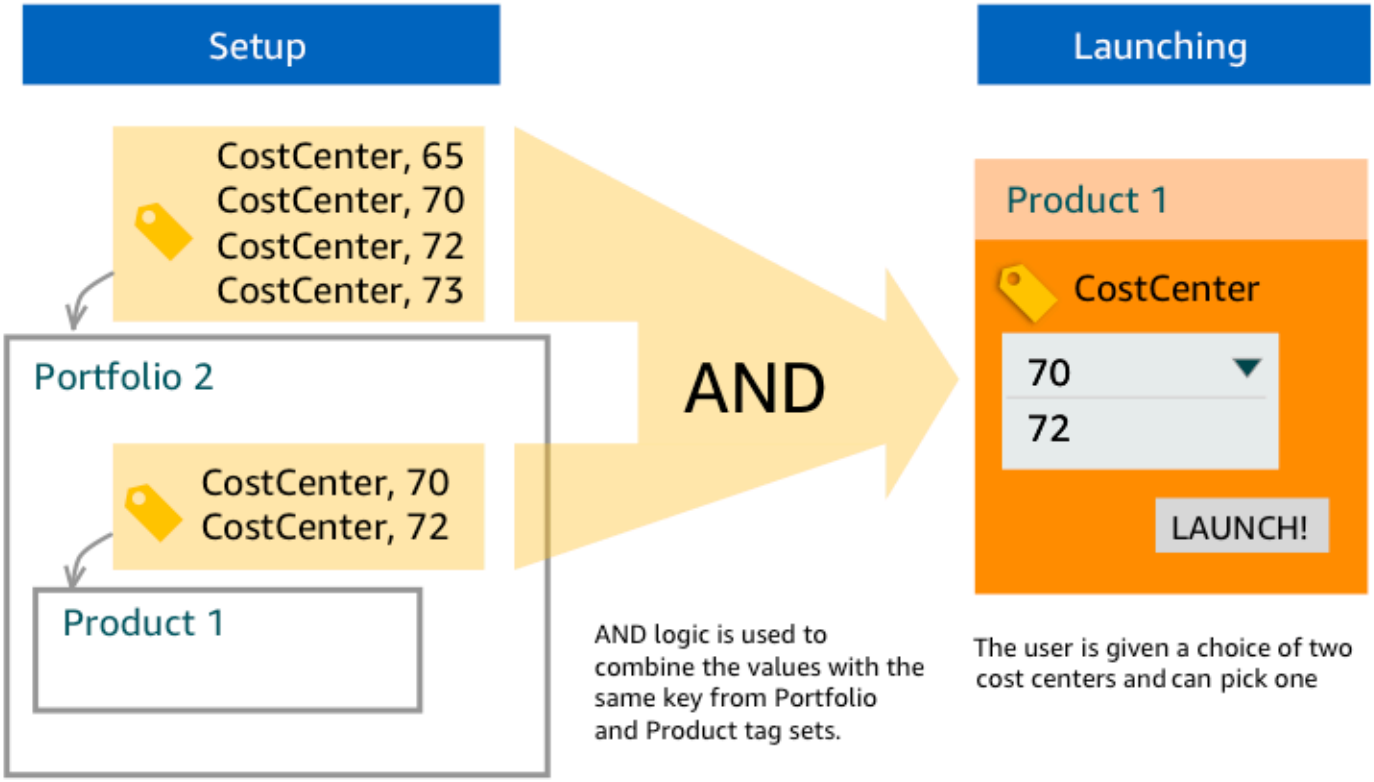

## Beispiel 2: Ein Satz von TagOptions mit demselben Schlüssel in einem Portfolio

Ein Administrator hat zwei TagOptions mit demselben Schlüssel in einem Portfolio platziert, und es gibt keine Produkte TagOptions mit demselben Schlüssel in diesem Portfolio. 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.



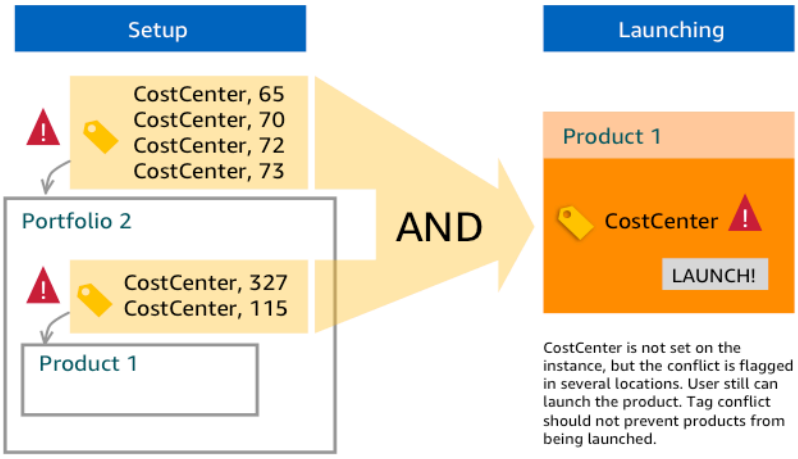

## Beispiel 3: Ein Satz TagOptions mit demselben Schlüssel sowohl für das Portfolio als auch für ein Produkt in diesem Portfolio

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 eine Reihe von Werten aus der Aggregation (logische UND-Verknüpfung) von. 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 auf dem Produkt in diesem Portfolio. AWS Service Catalog erstellt eine Reihe von Werten aus der Aggregation (logische UND-Verknüpfung) von. TagOptions Findet die Aggregation keine Werte für den Schlüssel, AWS Service Catalog wird ein Tag mit demselben Schlüssel und dem Wert`sc-tagconflict-`*`portfolioid`*`-`*`productid`*, where und *`productid`* are the des Portfolios *`portfolioid`* und ARNs des Produkts, erstellt. 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.




## Verwaltung TagOptions

Als Administrator können Sie die folgenden Aktionen zur Verwaltung TagOptions in der TagOptions Bibliothek ausführen:

- Erstellen und löschen
- Aktiviere oder deaktiviere
- Zuordnen oder Zugehörigkeit aufheben
- Edit (Bearbeiten)

Um TagOptions in der Konsole zu erstellen

1. Öffnen Sie die Service Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie im linken Navigationsmenü die Option TagOptionsBibliothek aus.
3. Geben Sie unter Neu TagOption erstellen einen Schlüssel und einen Wert ein und wählen Sie dann Hinzufügen aus.

   Nachdem das neue Objekt erstellt TagOption wurde, wird es nach Schlüssel-Wert-Paaren gruppiert und in der Liste alphabetisch sortiert. TagOptions

   Informationen zum Erstellen eines TagOption mithilfe der AWS Service Catalog API finden Sie unter. CreateTagOption

Um TagOptions in der Konsole zu löschen

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.

Um eine oder mehrere TagOptions in der Konsole zu aktivieren oder zu deaktivieren

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 TagOption gewünschte inaktive Datei aus. Wählen Sie dann Aktionen und dann im Drop-down-Menü die Option Aktivieren aus und bestätigen Sie Ihre Auswahl.

   Wählen Sie zum Deaktivieren das TagOption gewünschte aktive Element aus. Wählen Sie dann Aktionen und dann Deaktivieren aus dem Drop-down-Menü aus und bestätigen Sie Ihre Auswahl.

Um ein oder mehrere Portfolios in der Konsole TagOptions einem Portfolio zuzuordnen oder die Verknüpfung aufzuheben

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 trennen möchten.
3. Wählen Sie die TagOptionsRegisterkarte und wählen Sie eines oder mehrere aus TagOptions , um die Verknüpfung mit dem Portfolio zu verknüpfen oder aufzuheben.
4. Wählen Sie Aktionen. Wählen Sie dann „Zuordnen“ oder „Zuordnung trennen“ und bestätigen Sie Ihre Auswahl.

Um ein oder mehrere Produkte in der Konsole einem oder mehreren TagOptions Produkten zuzuordnen oder zu trennen

1. Öffnen Sie die AWS Service Catalog Konsole 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 trennen möchten.

3. Wählen Sie die TagOptionsRegisterkarte und wählen Sie eine oder mehrere aus TagOptions , um sie dem Portfolio zuzuordnen oder zu trennen.
4. Wählen Sie Aktionen. Wählen Sie dann „Zuordnen“ oder „Zuordnung trennen“ und bestätigen Sie Ihre Auswahl.

> **Note**
>
> Informationen zur Verknüpfung TagOptions mit einem Portfolio oder Produkt mithilfe der AWS Service Catalog API finden Sie unter AssociateTagOptionWithResource.
> Informationen zum Entfernen (Aufheben der Zuordnung) TagOptions mithilfe der AWS Service Catalog API finden Sie unter DisassociateTagOptionFromResource.

Um Werte für TagOptions in der Konsole zu bearbeiten

1. Öffnen Sie die Service Catalog-Konsole unter https://console.aws.amazon.com/servicecatalog/.
2. Wählen Sie im linken Navigationsmenü die Option TagOptionsBibliothek aus.
3. Wählen Sie einen TagOption und öffnen Sie den Wert. (Der Wert ist mit einem Hyperlink verknüpft.) Wählen Sie dann Bearbeiten aus.
4. Bearbeiten Sie den Wert im Feld Wert und wählen Sie Änderungen speichern aus.

## Verwendung TagOptions mit AWS Organizations Tag-Richtlinien

Dieses Thema bietet einen kurzen Überblick über Tag-Richtlinien für AWS Organizations und TagOptions für AWS Service Catalog. Außerdem wird erläutert, wie Tag-Konflikte vermieden werden können, wenn beide Funktionen gleichzeitig verwendet werden.

TagOptions AWS Service Catalog gilt für bereitgestellte Produkte (CloudFormationStacks), während Tag-Richtlinien für für AWS Konten und Organisationseinheiten (OU) oder einen Unternehmensstamm AWS Organizations gelten. Wenn Sie beispielsweise einer Organisationseinheit eine Tag-Richtlinie zuordnen, gilt dieselbe Tag-Richtlinie für alle Konten in dieser Organisationseinheit. Wenn Sie beide Tagging-Funktionen gleichzeitig verwenden, sollten Sie sie so konfigurieren, dass es nicht zu Konflikten kommt.

## Tag-Richtlinien

Mit Tag-Richtlinien können Sie Regeln für die Verwendung von Tags für AWS Ressourcen in Ihren Konten in AWS Organizations definieren. Mithilfe von Tag-Richtlinien können Sie einen konsistenten Ansatz für die Kennzeichnung von AWS Ressourcen auf Kontoebene erstellen und beibehalten.

Tag-Richtlinien bieten eine einfache Möglichkeit, sicherzustellen, dass Benutzer konsistente Tags anwenden, markierte Ressourcen prüfen und die Ressourcen ordnungsgemäß kategorisieren. Sie können auch definieren, wie Tag-Schlüssel groß geschrieben werden sollen und welche Werte Sie zulassen möchten. Sie können beispielsweise vorschreiben, dass für alle EC2 Instanzen in einem Konto ein Tag-Schlüssel als festgelegt **`CostCenter`** und für dieses Tag die Werte **`Data Insights`** oder **`Marketing`** festgelegt werden müssen.

Mithilfe von Tag-Richtlinien können Sie Optionen auswählen, um Tagging-Regeln durchzusetzen, fehlerhafte Operationen mit Tags zu verhindern und die Ressourcentypen festzulegen, für die die Durchsetzung gilt. Wenn Sie keine Durchsetzungsoption wählen, können Sie mit Tag-Richtlinien die nicht konformen Tags erstellen oder ändern, sie werden jedoch in der Konsole als nicht konform gemeldet. AWS Organizations

Weitere Informationen zur Einrichtung der Durchsetzung von Tagging auf Kontoebene finden Sie unter Tag-Richtlinien unter. AWS Organizations

## TagOptions

TagOptions sind eine Tagging-Funktion, die AWS Service Catalog für bereitgestellte Produkte auf CloudFormation Stack-Ebene 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 Ihren Produkten zugeordnet werden sollen. AWS Service Catalog Wenn Sie ein AWS Service Catalog Produkt auf den Markt bringen, müssen Sie TagOption Werte für die vorhandenen TagOption Schlüssel auswählen, die diesem Portfolio oder Produkt zugeordnet sind, um dieses Produkt auf den Markt zu bringen. Da Sie diese Werte TagOptions auf Portfolio- oder Produktebene festlegen, können Sie eine einheitliche Taxonomie für die Kennzeichnung von Portfolios durchsetzen, die über Konten und Regionen hinweg gemeinsam genutzt werden.

Weitere Informationen zur Einrichtung TagOptions in AWS Service Catalog finden Sie unter Bibliothek.AWS Service Catalog TagOption

## Vermeidung 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 Administratoren, die auch AWS Service Catalog Portfolios und Produkte verwalten, die Anforderungen TagOptions für konforme Tags mit.
- Teilen Sie die Anforderungen für konforme Tags mit Endbenutzern, die möglicherweise Produkte auf den Markt bringen, AWS Service Catalog und fügen Sie optionale Endbenutzer-Tags an ihre Produkteinführungen an.

Angenommen, Sie möchten ein Produkt auf den Markt bringen, AWS Service Catalog das den TagOption Schlüssel verwendet`city`, und Sie haben eine Tag-Richtlinie, die vorschreibt, dass Tag-Schlüssel mit `city` Tag-Werten von US-Städten enthalten müssen, z. B.**`Atlanta`**, **`San Francisco`** oder. **`Austin`** AWS Service Catalog erlaubt Ihnen nicht, ein Produkt auf den Markt zu bringen, ohne TagOption Werte für die erforderlichen TagOption Schlüssel für ein Produkt ausgewählt zu haben.

In diesem Fall wird das Produkt nicht auf den Markt gebracht`city`, wenn Sie TagOption Werte für den TagOption Schlüssel haben, die südamerikanische Städte enthalten**`Buenos Aires`**, AWS Service Catalog z. B. **`Rio de Janeiro`** oder. Stattdessen müssen Sie bei der Markteinführung einen TagOption Wert auswählen, der eine Stadt in den USA beinhaltet, um die Tag-Richtlinie einzuhalten.

Die folgende Tabelle enthält Szenarien, in denen beschrieben wird, wie Sie Probleme mit Tag-Konflikten lösen können, die TagOptions bei der gleichzeitigen Verwendung von Tag-Richtlinien auftreten können.

| Szenario | Grund | Lösung |
| --- | --- | --- |
| Das Produkt kann aufgrund nicht kompatibler Tags nicht gestartet werden, wenn die Tag-Durchsetzung in der Tag-Richtlinie aktiviert ist. | Geben Sie TagOptions anhand von Schlüsseln und Werten an, die Sie nicht zur Liste der zulässigen Tags in Ihrer Tag-Richtlinie hinzugefü gt haben. | Wenn Sie in Ihrer Tag-Richt linie ein bestimmtes Schema für die Groß- und Kleinschr eibung von Tag-Schlüsseln konfigurieren, stellen Sie sicher, dass Ihre TagOptions Tag-Schlüssel und optionale |

| Szenario | Grund | Lösung |
| --- | --- | --- |
| | Hinzufügen optionaler benutzerdefinierter Tags, die nicht Ihrer Tag-Richtlinie entsprechen. | n benutzerdefinierten Tag-Schlüssel mit den Angaben in Ihrer Tag-Richtlinie übereinst immen.<br><br>Beachten Sie, dass, wenn das Kontrollkästchen zur Durchsetzung der Groß-/Kle inschreibung von Tags in Ihrer Tag-Richtlinie deaktiviert ist, dies dazu führt, dass alle Tag-Schlüssel in Kleinbuchstaben konform sind und dass Ihre TagOptions Tag-Schlüssel und optionalen benutzerd efinierten Tag-Schlüssel den Anforderungen Ihrer Tag-Richt linie entsprechen (z. B. alle in Kleinbuchstaben). |

| Szenario | Grund | Lösung |
| --- | --- | --- |
| Das Produkt kann aufgrund einer fehlerhaften Groß-/Kleinschreibung von Tag-Schlüsseln nicht gestartet werden. | Die Angabe der Groß-/Kleinschreibung in den TagOptions Schlüsseln entspricht nicht den Regeln zur Durchsetzung der Groß-/Kleinschreibung in der Tag-Richtlinie. | Konfigurieren Sie Ihre Tag-Richtlinien korrekt. Wenn Sie nicht angeben, dass die Einhaltung der Vorschriften für die Groß- und Kleinschreibung von Tagschlüsseln eingehalten wird, ist die Standardeinstellung für die Groß- und Kleinschreibung von Tagschlüsseln.<br><br>Wenn Sie in Ihrer Tag-Richtlinie nicht die Einhaltung der Einhaltung der Regeln für die Groß- und Kleinschreibung von Tagschlüsseln angeben, sollten Sie außerdem sicherstellen, dass Ihre TagOptions Tag-Schlüssel ausschließlich in Kleinbuchstaben geschrieben AWS Service Catalog sind, um den Durchsetzungsregeln zu entsprechen.<br><br>Wenn Sie eine Tag-Richtlinie verwenden, für die die Einhaltung der Groß-/Kleinschreibung nicht aktiviert ist, berücksichtigt diese Tag-Richtlinie nur alle Tag-Schlüssel in Kleinbuchstaben als konform. |

| Szenario | Grund | Lösung |
| --- | --- | --- |
| Das Produkt kann aufgrund inkompatibler Tag-Werte nicht gestartet werden. | Auswahl eines TagOptions Tag-Werts für eine Produktei nführung, der nicht in der Liste der zulässigen Tag-Werte in Ihrer Tag-Richtlinie aufgeführt ist. | Ordnen TagOptions Sie Ihren Produkten und Portfolios, die Ihren Anforderungen in der Liste entsprechen, Tag-Wert-Konformität zulässiger Tag-Werte zu. |

# 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.

Anrufe an UpdateProvisionedProductund TerminateProvisionedProductwerden auf ähnliche Weise behandelt, wobei jeder Anruf über eine eigene Warteschlange und Notify verfügt: APIs

- 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` beispiels weise der Amazon S3 S3-URI. |
| Artefakt//Typ | Zeichenfolge | Ja | Art des Artefakts . Zulässiger Wert:`AWS_S3`. |
| LaunchRole | Zeichenfolge | Nein | Der Amazon-Re ssourcenname (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 (Paramete rwerte werden als Echo wiedergeg eben). |

## 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, wie z. `ec2:CreateTags`

# Überwachung in AWS Service Catalog

Sie können Ihre AWS Service Catalog Ressourcen mithilfe von Amazon überwachen CloudWatch, das Rohdaten sammelt und AWS Service Catalog in lesbare Messwerte umwandelt. Diese Statistiken werden über einen Zeitraum von zwei Wochen aufgezeichnet, sodass Sie auf historische Informationen zugreifen und sich einen besseren Überblick über die Leistung Ihres Services verschaffen können. AWS Service Catalog Metrikdaten werden automatisch CloudWatch in Zeitabständen von 1 Minute an gesendet. Weitere Informationen zu CloudWatch finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Eine Liste verfügbarer Metriken und Maße finden Sie unter AWS Service Catalog CloudWatch Metriken.

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit AWS Service Catalog und Leistung Ihrer AWS Lösungen. Sie sollten Überwachungsdaten aus allen Teilen Ihrer AWS Lösung sammeln, damit Sie einen etwaigen Ausfall an mehreren Stellen leichter debuggen können. Bevor Sie mit der Überwachung beginnen AWS Service Catalog, sollten Sie einen Überwachungsplan erstellen, der Antworten auf die folgenden Fragen enthält:

- 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 stellt verschiedene Tools bereit, die Sie zur Überwachung verwenden können AWS Service Catalog. 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 CloudWatch Amazon-Alarme verwenden, um Störungen zu überwachen AWS Service Catalog und zu melden.

CloudWatch Alarme beobachten 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 mehrere Zeiträume basieren. Die Aktion ist eine Benachrichtigung, die an ein Amazon Simple Notification Service (Amazon SNS) -Thema oder eine Amazon EC2 Auto Scaling Scaling-Richtlinie gesendet wird. CloudWatch Alarme lösen keine Aktionen aus, nur weil sie sich in einem bestimmten Status befinden. Der Status muss sich geändert haben und für eine bestimmte Anzahl von Zeiträumen beibehalten worden sein. Informationen zum Erstellen eines Alarms finden Sie unter CloudWatch Amazon-Alarme erstellen. Weitere Informationen zur Verwendung von CloudWatch Amazon-Metriken mit AWS Service Catalog finden Sie unterAWS Service Catalog CloudWatch Metriken.

# AWS Service Catalog CloudWatch Metriken

Sie können Ihre AWS Service Catalog Ressourcen mithilfe von Amazon überwachen CloudWatch, das Rohdaten sammelt und AWS Service Catalog in lesbare Messwerte umwandelt. Diese Statistiken werden über einen Zeitraum von zwei Wochen aufgezeichnet, sodass Sie auf historische Informationen zugreifen und sich einen besseren Überblick über die Leistung Ihres Services verschaffen können. AWS Service Catalog Metrikdaten werden automatisch CloudWatch in Zeitabständen von 1 Minute an gesendet. Weitere Informationen zu CloudWatch finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Themen


- CloudWatch Metriken aktivieren
- Verfügbare Metriken und Dimensionen
- Anzeigen von AWS Service Catalog -Metriken


## CloudWatch Metriken aktivieren

CloudWatch Amazon-Metriken sind standardmäßig aktiviert.

# Verfügbare Metriken und Dimensionen

Die Metriken und Dimensionen, die AWS Service Catalog an Amazon gesendet werden, 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. Die Dimensionen werden als separate Datensätze in CloudWatch Protokollen veröffentlicht.<br><br>Einheiten: `Count`<br><br>Gültige Statistiken:`Minimum`,`Maximum`,`Sum`, `Average`<br><br>Abmessungen:`State`,`PPState`,`ProductId` , `ProvisioningArtifactId` |
| `ProductProvisioningOperation` | Die Anzahl der mit der Produkt-ID ausgeführten Operationen,`provisioningArtifactId` . Die Dimensionen werden als ein Datensatz in CloudWatch Protokollen veröffentlicht.<br><br>Einheiten: `Count`<br><br>Gültige Statistiken:`Minimum`,`Maximum`,`Sum`, `Average`<br><br>Abmessungen:`State`,`PPState`,`ProductId` , `ProvisioningArtifactId` |

## Dimensionen für AWS Service Catalog -Metriken

AWS Service Catalog sendet die folgenden Abmessungen an Amazon CloudWatch.

| Dimension | Beschreibung |
| --- | --- |
| `PPState` | Diese Dimension filtert die angeforderten Daten für alle bereitgestellten Produkte, die mit diesem angegebenen Zustand ausgeführt werden. So können Sie Ihre Daten nach dem Ausführun gszustand kategorisieren.<br><br>Gültiger Status: VERFÜGBAR, VERDORBEN, FEHLER |
| `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. |
| `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. |
| `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 Ausführun gszustand kategorisieren.<br><br>Gültiger Zustand: ERFOLGREICH, FEHLGESCH LAGEN |

## Anzeigen von AWS Service Catalog -Metriken

Sie können CloudWatch Amazon-Metriken in der CloudWatch Amazon-Konsole anzeigen, die eine detaillierte und anpassbare Anzeige Ihrer Ressourcen sowie der Anzahl der laufenden Aufgaben in einem Service bietet.

Themen

- AWS Service Catalog Metriken in der CloudWatch Amazon-Konsole anzeigen

## AWS Service Catalog Metriken in der CloudWatch Amazon-Konsole anzeigen

Sie können AWS Service Catalog Metriken in der CloudWatch Amazon-Konsole anzeigen. Die CloudWatch Amazon-Konsole bietet eine detaillierte Ansicht der AWS Service Catalog Kennzahlen, und Sie können die Ansichten an Ihre Bedürfnisse anpassen. Weitere Informationen zu Amazon CloudWatch finden Sie im CloudWatch Amazon-Benutzerhandbuch.

So zeigen Sie Metriken in der CloudWatch Amazon-Konsole an

1. Öffnen Sie die CloudWatch Amazon-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 mit AWS CloudTrail

AWS Service Catalog ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in ausgeführt wurden AWS Service Catalog. CloudTrail erfasst alle API-Aufrufe AWS Service Catalog als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der AWS Service Catalog Konsole und Codeaufrufen für die AWS Service Catalog API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für AWS Service Catalog. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von gesammelten Informationen können Sie die Anfrage ermitteln CloudTrail, an die die Anfrage gestellt wurde AWS Service Catalog, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

## AWS Service Catalog Informationen in CloudTrail

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie es erstellen. Wenn eine Aktivität in stattfindet AWS Service Catalog, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der

CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS Konto ansehen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit dem CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich der Ereignisse für AWS Service Catalog, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- AWS CloudTrail unterstützte Dienste und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für AWS CloudTrail
- Empfangen von AWS CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von AWS CloudTrail Protokolldateien von mehreren Konten

CloudTrail protokolliert alle AWS Service Catalog Aktionen. Beispielsweise generieren Aufrufe von `CreateProduct` und `UpdateProvisionedProduct` Aktionen Einträge in den CloudTrail Protokolldateien. `CreatePortfolio`

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter CloudTrail -Element userIdentity.

# AWS Service Catalog Logdateieinträge verstehen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 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, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.
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"
}
```

# Einstellungen für das Konsolen-Branding

AWS Service Catalog ermöglicht es Administratoren, die Einstellungen für das Konsolen-Branding für Konten festzulegen. Administratoren können mithilfe des Konsolen-Brandings einen Firmennamen, ein Logobild sowie eine Primär- und Sekundärfarbe (Akzent) für eine Vielzahl von Seitenkomponenten angeben. Diese Branding-Einstellungen sind sowohl für Administratoren als auch für Endbenutzer sichtbar, wenn sie die Konsole verwenden.

Die Einstellungen für das Konsolen-Branding verbessern das Erscheinungsbild eines Kontos und bewirken Folgendes:

- Sorgt für einen nahtlosen visuellen Übergang zwischen der Konsole und internen Anwendungen
- Unterscheidet Konten, die von verschiedenen internen Teams innerhalb desselben Unternehmens verwendet werden
- Unterscheidet Konten in verschiedenen Umgebungen, z. B. in der Entwicklungs-, Bereitstellungs- oder Produktionsumgebung

> **Note**
>
> Administratoren legen die Einstellungen für das Konsolen-Branding auf Kontoebene fest.

Um die Einstellungen für das Konsolen-Branding festzulegen

1. Wählen Sie im linken Navigationsmenü Einstellungen aus.
2. Wählen Sie „Bearbeiten“ für die Branding-Einstellungen „Hellmodus“ oder „Dunkelmodus“.
3. Laden Sie ein Logo hoch, geben Sie einen Markennamen ein und wählen Sie dann die Primärfarbe und die Sekundärfarbe aus.
4. Wählen Sie Save (Speichern) aus.

Eine Liste der Regionen, in denen AWS Service Catalog das Konsolen-Branding unterstützt wird, finden Sie AWS-Region unter Support für Konsolen-Branding.

# AWS-Region Unterstützung für Konsolen-Branding-Einstellungen

AWS Service Catalog unterstützt die in der Tabelle unten AWS-Regionen aufgeführten Einstellungen für das Konsolen-Branding.

| 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 |
| USA 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 |
| Asia Pacific (Osaka) | ap-northeast-3 |
| Asien-Pazifik (Seoul) | ap-northeast-2 |
| Asien-Pazifik (Singapur) | ap-southeast-1 |
| Asien-Pazifik (Sydney) | ap-southeast-2 |
| Asien-Pazifik (Tokio) | ap-northeast-1 |
| Kanada (Zentral) | ca-central-1 |
| Europa (Frankfurt) | eu-central-1 |
| Europa (Irland) | eu-west-1 |
| Europa (London) | eu-west-2 |

| AWS-Region Name | AWS-Region Identität |
| --- | --- |
| Europa (Mailand) | eu-south-1 |
| Europa (Paris) | eu-west-3 |
| Europa (Stockholm) | eu-north-1 |
| Naher Osten (Bahrain) | me-south-1 |
| Südamerika (São Paulo) | sa-east-1 |
| AWS GovCloud (US-Ost) | us-gov-east-1 |
| AWS GovCloud (US-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 Instructure-as-Code-Tools (IaC) zu ermöglichen. Weitere Informationen finden Sie unter Externe Engines für. AWS Service Catalog | 16. Mai 2024 |
| Sicherheits-IAM-Update | AWS Service Catalog aktualisiert die `AWSServiceCatalogSyncServic` | 7. Mai 2024 |

| | | |
|---|---|---|
| | eRolePolicy Richtlinie, zu der gewechselt codestar-connections werden sollcodeconnections . 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. Aktualisierung vorhandener Terraform Open Source-Produkte und bereitgestellter Produkte auf den Produkttyp External | 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.