



Guida per l'amministratore

AWS Service Catalog



AWS Service Catalog: Guida per l'amministratore

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

| | |
|--|----|
| Che cos'è Service Catalog? | 1 |
| Video: Introduzione a AWS Service Catalog | 2 |
| Panoramica di | 2 |
| Utenti | 2 |
| Prodotti | 2 |
| HashiCorp Supporto per Terraform Open Source e Terraform Cloud | 3 |
| Prodotti con provisioning | 3 |
| Portafogli | 3 |
| Controllo delle versioni | 4 |
| Permissions | 4 |
| Vincoli | 4 |
| Flusso di lavoro iniziale per un amministratore | 5 |
| Flusso di lavoro iniziale per un utente finale | 5 |
| Quote | 6 |
| AWS Organizations | 6 |
| Quote con vincoli | 6 |
| Quote di portafoglio | 6 |
| Quote di prodotti | 6 |
| Quote di prodotto sottoposte a provisioning | 6 |
| Quote regionali | 7 |
| Quote di operazioni di servizi | 7 |
| TagOptions quote | 7 |
| Configurazione | 8 |
| Registrati per un Account AWS | 8 |
| Crea un utente con accesso amministrativo | 9 |
| Concedere le autorizzazioni agli amministratori | 11 |
| Concedi le autorizzazioni agli utenti finali | 13 |
| Installa e configura il motore di provisioning Terraform | 14 |
| Determinazione della coda | 15 |
| Aggiungere Confused Deputy al motore di provisioning Terraform | 15 |
| Nozioni di base | 20 |
| Libreria introduttiva | 20 |
| Prerequisiti | 21 |
| Ulteriori informazioni | 21 |

| | |
|---|----|
| Guida introduttiva a un CloudFormation prodotto | 21 |
| Passaggio 1: scarica il modello | 22 |
| Fase 2: crea una coppia di chiavi | 26 |
| Fase 3: Creare un portfolio | 27 |
| Fase 4: Creare un nuovo prodotto nel portafoglio | 28 |
| Fase 5: Aggiungere un vincolo per il modello | 29 |
| Fase 6: Aggiungere un vincolo di avvio | 30 |
| Fase 7: concedere agli utenti finali l'accesso al portafoglio | 33 |
| Fase 8: Verificare l'esperienza dell'utente finale | 33 |
| Guida introduttiva a un prodotto Terraform | 34 |
| Aggiornamento al tipo di prodotto esterno | 36 |
| Prerequisito: configura il tuo motore di provisioning Terraform | 37 |
| Passaggio 1: download del file di configurazione Terraform | 38 |
| Passaggio 2: creare un prodotto Terraform | 39 |
| Fase 3: Creare un portfolio | 41 |
| Fase 4: Aggiungere il prodotto al portafoglio | 41 |
| Fase 5: Creare ruoli di lancio | 42 |
| Passaggio 6: aggiungere un vincolo di avvio | 45 |
| Fase 7: concedere l'accesso all'utente finale | 46 |
| Fase 8: Condivisione del portafoglio con l'utente finale | 47 |
| Fase 9: Verificare l'esperienza dell'utente finale | 48 |
| Fase 10: monitoraggio delle operazioni di approvvigionamento di Terraform | 49 |
| Sicurezza | 50 |
| Protezione dei dati | 51 |
| Protezione dei dati con crittografia | 52 |
| Identity and Access Management | 52 |
| Destinatari | 52 |
| Esempi di policy basate sull'identità per AWS Service Catalog | 53 |
| AWS politiche gestite | 59 |
| Uso di ruoli collegati ai servizi | 70 |
| Risoluzione dei problemi di AWS Service Catalog identità e accesso | 75 |
| Controllo dell'accesso | 77 |
| Registrazione e monitoraggio | 78 |
| Convalida della conformità | 78 |
| Resilienza | 79 |
| Sicurezza dell'infrastruttura | 80 |

| | |
|--|-----|
| Best practice di sicurezza | 80 |
| Gestione di cataloghi | 82 |
| Gestione di portafogli | 82 |
| Creazione, visualizzazione ed eliminazione di portafogli | 83 |
| Visualizzazione dei dettagli di un portafoglio | 83 |
| Creazione ed eliminazione di portafogli | 83 |
| Aggiungere prodotti | 84 |
| Aggiunta di vincoli | 87 |
| Concessione dell'accesso agli utenti | 88 |
| Condivisione di un portafoglio | 89 |
| Condivisione e importazione di portafogli | 97 |
| Gestione di prodotti | 101 |
| Visualizzazione della pagina dei prodotti | 101 |
| Creazione di prodotti | 102 |
| Aggiungere prodotti ai portafogli | 105 |
| Aggiornamento dei prodotti | 105 |
| Sincronizzazione dei prodotti con file modello da archivi esterni | 107 |
| Eliminazione di prodotti | 115 |
| Gestione delle versioni | 124 |
| Utilizzo di vincoli | 125 |
| Vincoli di avvio di | 125 |
| Vincoli di notifica di | 131 |
| Vincoli di aggiornamento dei tag | 132 |
| Vincoli del set di stack | 133 |
| Vincoli di modello di | 133 |
| Utilizzo delle operazioni di servizio | 138 |
| Prerequisiti | 138 |
| Fase 1: configurazione delle autorizzazioni degli utenti finali | 139 |
| Fase 2: creazione di un'operazione di servizio | 140 |
| Fase 3: associare l'operazione di servizio a una versione del prodotto | 141 |
| Fase 4. Test dell'esperienza dell'utente finale | 141 |
| Fase 5: Gestione delle azioni di servizio con AWS CloudFormation | 142 |
| Fase 6: Risoluzione dei problemi | 142 |
| Aggiungere Marketplace AWS prodotti al tuo portafoglio | 144 |
| Gestione dei Marketplace AWS prodotti utilizzando AWS Service Catalog | 145 |
| Gestione e aggiunta manuale Marketplace AWS dei prodotti | 145 |

| | |
|--|-----|
| Usando CloudFormation StackSets | 150 |
| Set di stack e istanze di stack | 151 |
| Vincoli del set di stack | 151 |
| Gestione dei budget | 151 |
| Prerequisiti | 152 |
| Creazione di un budget | 154 |
| Associazione di un budget | 154 |
| Visualizzazione di un budget | 155 |
| Disassociazione di un budget | 155 |
| Gestione di prodotti con provisioning | 157 |
| Gestione dei prodotti forniti in qualità di amministratore | 157 |
| Modifica del proprietario del prodotto con provisioning | 158 |
| Vedi anche | 159 |
| Aggiornamento dei modelli per i prodotti forniti | 159 |
| Esercitazione: identificazione dell'utente per l'allocazione delle risorse | 160 |
| Gestione degli errori di stato del prodotto Terraform Open Source | 164 |
| Esempi di errori di stato | 164 |
| Gestione del file di stato del prodotto Terraform Open Source | 165 |
| Gestione dei tag | 166 |
| AutoTags | 166 |
| TagOption Biblioteca | 167 |
| Lancio di un prodotto con TagOptions | 168 |
| Gestire TagOptions | 172 |
| Utilizzo TagOptions con le politiche dei AWS Organizations tag | 174 |
| Motori esterni | 178 |
| Considerazioni | 179 |
| Analisi dei parametri | 179 |
| Fornitura | 182 |
| Aggiornamento in corso | 186 |
| Terminare | 189 |
| Assegnazione di tag | 190 |
| Monitoraggio | 192 |
| Strumenti di monitoraggio | 192 |
| Strumenti automatici | 192 |
| CloudWatch Metriche | 193 |
| Abilitazione delle CloudWatch metriche | 193 |

| | |
|--|--------|
| Parametri e dimensioni disponibili | 193 |
| Visualizzazione delle metriche AWS Service Catalog | 195 |
| CloudTrail registri | 196 |
| AWS Service Catalog informazioni in CloudTrail | 196 |
| Comprensione delle AWS Service Catalog voci dei file di registro | 197 |
| Branding della console | 199 |
| Regione AWS supporto per il branding delle console | 199 |
| Cronologia dei documenti | 202 |
| Aggiornamenti precedenti | 203 |
| | ccviii |

Che cos'è Service Catalog?

Service Catalog consente alle organizzazioni di creare e gestire cataloghi di servizi IT approvati AWS. Questi servizi IT possono includere qualsiasi cosa, da immagini di macchine virtuali, server, software, database e altro ancora a architetture applicative multilivello complete.

Service Catalog consente alle organizzazioni di gestire centralmente i servizi IT più diffusi e aiuta le organizzazioni a raggiungere una governance coerente e soddisfare i requisiti di conformità. Gli utenti finali possono distribuire rapidamente soltanto i servizi IT approvati di cui hanno bisogno, in accordo con i vincoli stabiliti dall'organizzazione.

Service Catalog offre i seguenti vantaggi:

- Standardizzazione

Amministra e gestisci asset approvati limitando la posizione di avvio del prodotto, il tipo di istanza che può essere utilizzato e molte altre opzioni di configurazione. Il risultato è un ambiente standardizzato per il provisioning dei prodotti per l'intera organizzazione.

- Ricerca e avvio self-service

Gli utenti esaminano gli elenchi di prodotti (servizi o applicazioni) a cui hanno accesso, trovano il prodotto che intendono utilizzare e lo avviano come prodotto con provisioning.

- Controllo granulare degli accessi

Gli amministratori assemblano portafogli di prodotti dal proprio catalogo, aggiungono vincoli e tag di risorse da utilizzare durante il provisioning e quindi concedono l'accesso al portafoglio tramite utenti e gruppi AWS Identity and Access Management (IAM).

- Estensibilità e controllo della versione

Gli amministratori possono aggiungere un prodotto a un qualsiasi numero di portafogli e limitarlo senza creare un'altra copia. Quando si aggiorna il prodotto a una nuova versione, l'aggiornamento è propagato a tutti i prodotti di tutti i portafogli che vi fanno riferimento.

Per ulteriori informazioni, consulta la [pagina dei dettagli del Service Catalog](#).

L'API Service Catalog fornisce il controllo programmatico su tutte le azioni dell'utente finale in alternativa all'utilizzo di Console di gestione AWS. Per ulteriori informazioni, vedere [Service Catalog Developer Guide](#).

Video: Introduzione a AWS Service Catalog

Questo video (7:27) descrive come creare, organizzare e gestire un catalogo curato di prodotti e condividere AWS prodotti con livelli di autorizzazione. Di conseguenza, gli utenti finali possono fornire rapidamente risorse IT approvate senza accesso diretto ai servizi sottostanti. AWS

[Introduzione a AWS Service Catalog](#)

Panoramica del Service Catalog

Iniziando a usare Service Catalog, trarrai vantaggio dalla comprensione dei suoi componenti e dei flussi di lavoro iniziali per amministratori e utenti finali.

Utenti

Service Catalog supporta i seguenti tipi di utenti:

- Amministratori del catalogo (amministratori): gestiscono un catalogo di prodotti (applicazioni e servizi), organizzandoli in portafogli e concedendo l'accesso agli utenti finali. Gli amministratori del catalogo preparano CloudFormation modelli, configurano vincoli e gestiscono i ruoli IAM per i prodotti per fornire una gestione avanzata delle risorse.
- Utenti finali: ricevono AWS le credenziali dal reparto o dal responsabile IT e le utilizzano Console di gestione AWS per lanciare i prodotti a cui hanno ottenuto l'accesso. Agli utenti finali (a volte denominati semplicemente utenti) vengono concesse autorizzazioni differenti a seconda delle esigenze operative. Ad esempio, un utente può disporre del livello di autorizzazione massimo (per avviare e gestire tutte le risorse necessarie per i prodotti che utilizzano) o unicamente dell'autorizzazione per utilizzare specifiche caratteristiche del servizio.

Prodotti

Un prodotto è un servizio IT che si desidera rendere disponibile per l'implementazione. AWS Un prodotto è costituito da una o più AWS risorse, come EC2 istanze, volumi di storage, database, configurazioni di monitoraggio e componenti di rete o prodotti confezionati Marketplace AWS . Un prodotto può essere una singola istanza di elaborazione che esegue AWS Linux, un'applicazione Web multilivello completamente configurata in esecuzione nel proprio ambiente o qualsiasi altra cosa intermedia.

Puoi creare un prodotto importando un modello. AWS CloudFormation i modelli definiscono le AWS risorse necessarie per il prodotto, le relazioni tra le risorse e i parametri che gli utenti finali possono inserire quando lanciano il prodotto per configurare gruppi di sicurezza, creare coppie di chiavi ed eseguire altre personalizzazioni.

HashiCorp Supporto per Terraform Open Source e Terraform Cloud

AWS Service Catalog consente un approvvigionamento rapido e self-service con governance per le configurazioni HashiCorp Terraform Open Source e Terraform Cloud interne. AWS Puoi utilizzare Service Catalog come unico strumento per organizzare, governare e distribuire le configurazioni Terraform su larga scala all'interno. AWS È possibile accedere alle funzionalità principali di Service Catalog, tra cui la catalogazione di modelli Terraform standardizzati e preapprovati, il controllo degli accessi, il provisioning con privilegi minimi, il controllo delle versioni, l'etichettatura e la condivisione con migliaia di account. AWS Gli utenti finali visualizzano un semplice elenco di prodotti e versioni a cui hanno accesso e possono quindi distribuire tali prodotti con un'unica azione.

Per saperne di più e per completare un tutorial sui prodotti Terraform, consulta [Guida introduttiva a un prodotto Terraform](#)

Prodotti con provisioning

AWS CloudFormation gli stack semplificano la gestione del ciclo di vita del prodotto consentendoti di effettuare il provisioning, etichettare, aggiornare e terminare l'istanza del prodotto come una singola unità. Uno AWS CloudFormation stack include un AWS CloudFormation modello, scritto in formato JSON o YAML, e la raccolta di risorse associata. Un prodotto con provisioning è uno stack. Quando un utente finale lancia un prodotto, l'istanza del prodotto fornita da Service Catalog è uno stack con le risorse necessarie per eseguire il prodotto. Per ulteriori informazioni, consulta la [Guida per l'utente di AWS CloudFormation](#).

Portafogli

Un portfolio è una raccolta di prodotti che contiene informazioni di configurazione. I portafogli consentono di determinare chi può utilizzare specifici prodotti e come. Con Service Catalog, puoi creare un portfolio personalizzato per ogni tipo di utente della tua organizzazione e concedere selettivamente l'accesso al portafoglio appropriato. Quando aggiungi una nuova versione di un prodotto a un portafoglio, quella versione è automaticamente disponibile per tutti gli utenti correnti.

Puoi anche condividere i tuoi portafogli con altri AWS account e consentire all'amministratore di tali account di distribuirli con vincoli aggiuntivi, come limitare le istanze che EC2 un utente può

creare. Grazie all'utilizzo di portafogli, autorizzazioni, condivisioni e vincoli, gli utenti avviano prodotti correttamente configurati per le esigenze e gli standard dell'organizzazione.

Controllo delle versioni

Service Catalog ti consente di gestire più versioni dei prodotti del tuo catalogo. Questo approccio consente di aggiungere nuove versioni dei modelli e delle risorse associate in base agli aggiornamenti del software o alle modifiche alla configurazione.

Quando crei una nuova versione di un prodotto, l'aggiornamento viene automaticamente distribuito a tutti gli utenti che hanno accesso al prodotto, consentendo all'utente di selezionare la versione del prodotto da utilizzare. Gli utenti possono aggiornare rapidamente e facilmente le istanze in esecuzione del prodotto alla nuova versione.

Permissions

Quando a un utente si concede l'accesso a un portafoglio, gli si consente di consultare il portafoglio e di avviare i prodotti che contiene. Applichi le autorizzazioni AWS Identity and Access Management (IAM) per controllare chi può visualizzare e modificare il tuo catalogo. Le autorizzazioni IAM possono essere assegnate a utenti, gruppi e ruoli IAM.

Quando un utente avvia un prodotto a cui è assegnato un ruolo IAM, Service Catalog utilizza il ruolo per avviare le risorse cloud del prodotto utilizzando CloudFormation. Assegnando un ruolo IAM a ciascun prodotto, puoi evitare di concedere agli utenti le autorizzazioni per eseguire operazioni non approvate e consentire loro di fornire risorse utilizzando il catalogo.

Vincoli

I vincoli controllano i modi in cui è possibile distribuire risorse specifiche per un prodotto. AWS Puoi utilizzarli per applicare limiti ai prodotti allo scopo di controllare governance o costi. Esistono diversi tipi di AWS Service Catalog vincoli: vincoli di avvio, vincoli di notifica e vincoli di modello.

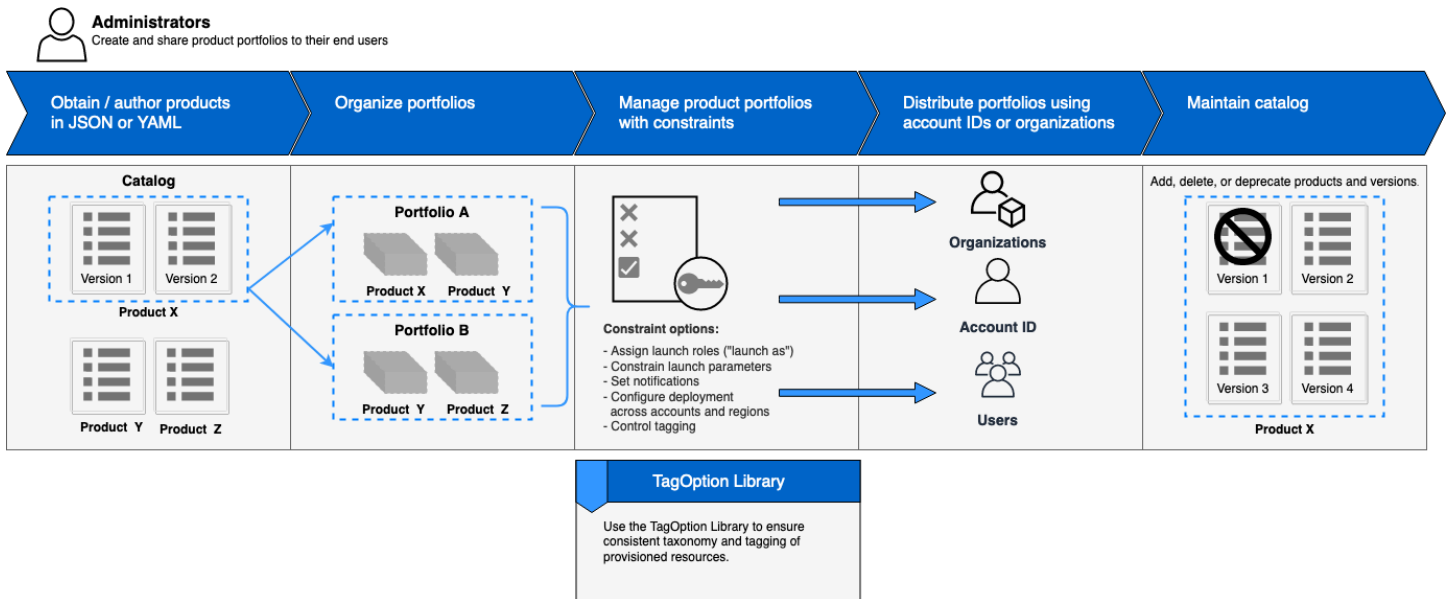
I vincoli di avvio ti consentono di specificare un ruolo per un prodotto in un portafoglio. Utilizza questo ruolo per fornire le risorse al momento del lancio, in modo da poter limitare le autorizzazioni degli utenti senza influire sulla capacità degli utenti di fornire prodotti dal catalogo.

I vincoli di notifica consentono di ricevere notifiche sugli eventi dello stack utilizzando un argomento di Amazon SNS.

I vincoli del modello limitano i parametri di configurazione disponibili per l'utente all'avvio del prodotto (ad esempio, tipi di EC2 istanze o intervalli di indirizzi IP). Questi vincoli ti consentono di riutilizzare modelli di AWS CloudFormation generici per i prodotti e di applicare restrizioni ai modelli per ogni prodotto o portafoglio.

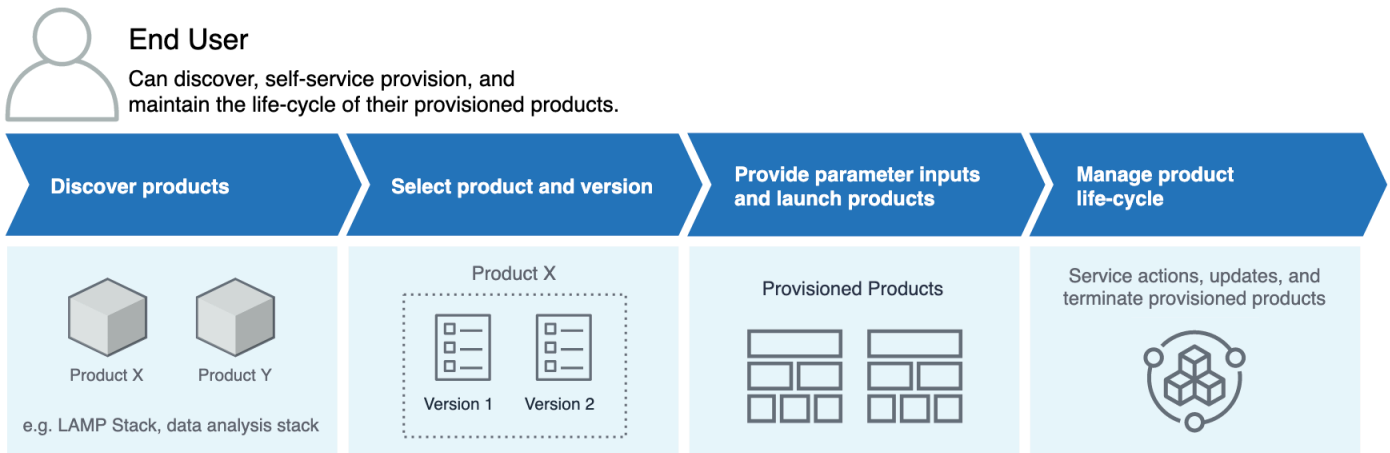
Flusso di lavoro iniziale per un amministratore

Questo diagramma mostra il flusso di lavoro iniziale di un amministratore per creare un catalogo.



Flusso di lavoro iniziale per un utente finale

Questo diagramma mostra il flusso di lavoro iniziale per un utente finale.



AWS Service Catalog quote di servizio predefinite

Il tuo AWS account ha le seguenti quote predefinite per: vincolo AWS Organizations, portafoglio, prodotto, prodotto fornito, regionale, azione di servizio e. TagOptions

AWS Organizations

- AWS Service Catalog amministratori delegati per organizzazione: 50

Quote con vincoli

- Vincoli per prodotto per portafoglio: 100

Quote di portafoglio

- Utenti, gruppi e ruoli per portafoglio: 100
- Prodotti per portafoglio: 150
- Tag per portafoglio: 20
- Account condivisi per portafoglio: 5000
- Valori tag per chiave tag: 25

Quote di prodotti

- Utenti, gruppi e ruoli per prodotto: 200
- Versioni di prodotto per prodotto: 100
- Tag per prodotto: 20
- Valori tag per chiave tag: 25

Quote di prodotto sottoposte a provisioning

- Tag per prodotto con provisioning: 50

Quote regionali

- Portafogli: 100
- Prodotti: 350

Quote di operazioni di servizi

- Operazioni di servizio per regione: 200
- Associazioni di operazioni di servizio per versione di prodotto: 25

TagOptions quote

- TagOptions per risorsa: 25
- Valori per TagOption: 25

Configurazione AWS Service Catalog

Prima di iniziare AWS Service Catalog, completa le seguenti attività.

Argomenti

- [Registrati per un Account AWS](#)
- [Crea un utente con accesso amministrativo](#)
- [Concedere le autorizzazioni agli amministratori AWS Service Catalog](#)
- [Concedere le autorizzazioni agli utenti AWS Service Catalog finali](#)
- [Installa e configura il motore di provisioning Terraform](#)

Registrati per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la <https://portal.aws.amazon.com/billing/registrazione>.
2. Segui le istruzioni online.

Nel corso della procedura di registrazione riceverai una telefonata o un messaggio di testo e ti verrà chiesto di inserire un codice di verifica attraverso la tastiera del telefono.

Quando ti iscrivi a un Account AWS, Utente root dell'account AWS viene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire [attività che richiedono l'accesso di un utente root](#).

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a <https://aws.amazon.com/> e scegliendo Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi [Console di gestione AWS](#) come proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

Per informazioni sull'accesso utilizzando un utente root, consulta la pagina [Accedere come utente root](#) nella Guida per l'utente di Accedi ad AWS .

2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

Per istruzioni, consulta [Abilitare un dispositivo MFA virtuale per l'utente Account AWS root \(console\)](#) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita il Centro identità IAM.

Per istruzioni, consulta [Abilitazione del AWS IAM Identity Center](#) nella Guida per l'utente di AWS IAM Identity Center .

2. Nel Centro identità IAM, assegna l'accesso amministrativo a un utente.

Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta [Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory](#) nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere come utente del Centro identità IAM, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente del Centro identità IAM.

Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta [AWS Accedere al portale di accesso](#) nella Guida per l'Accedi ad AWS utente.

Assegnazione dell'accesso ad altri utenti

1. Nel Centro identità IAM, crea un set di autorizzazioni conforme alla best practice per l'applicazione di autorizzazioni con il privilegio minimo.

Segui le istruzioni riportate nella pagina [Creazione di un set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center .

2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

Per istruzioni, consulta [Aggiungere gruppi](#) nella Guida per l'utente di AWS IAM Identity Center .

Argomenti

- [Concedere le autorizzazioni agli amministratori AWS Service Catalog](#)
- [Concedere le autorizzazioni agli utenti AWS Service Catalog finali](#)
- [Installa e configura il motore di provisioning Terraform](#)

Per fornire l'accesso, aggiungi autorizzazioni agli utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina [Create a permission set](#) (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .

- Utenti gestiti in IAM tramite un provider di identità:

Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina [Create a role for a third-party identity provider \(federation\)](#) della Guida per l'utente IAM.

- Utenti IAM:

- Crea un ruolo che l'utente possa assumere. Segui le istruzioni riportate nella pagina [Create a role for an IAM user](#) della Guida per l'utente IAM.

- (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina [Aggiunta di autorizzazioni a un utente \(console\)](#) nella Guida per l'utente IAM.

Concedere le autorizzazioni agli amministratori AWS Service Catalog

In qualità di amministratore del catalogo, è necessario accedere alla visualizzazione della console di AWS Service Catalog amministrazione e alle autorizzazioni IAM che consentono di eseguire attività come le seguenti:

- Creazione e gestione di portafogli
- Creazione e gestione di prodotti
- Aggiunta di vincoli di modello per controllare le opzioni disponibili per gli utenti finali quando avviano un prodotto
- Aggiungere vincoli di lancio per definire i ruoli IAM da AWS Service Catalog assumere quando gli utenti finali lanciano i prodotti
- Concessione dell'accesso ai prodotti agli utenti finali

Tu o un amministratore che gestisce le tue autorizzazioni IAM dovete allegare all'utente, al gruppo o al ruolo IAM le policy necessarie per completare questo tutorial.

Concessione di autorizzazioni a un amministratore di catalogo

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione, scegli Gestione degli accessi, quindi scegli Utenti. Se hai già creato un utente IAM che desideri utilizzare come amministratore del catalogo, scegli il nome utente, quindi scegli Aggiungi autorizzazioni. In caso contrario, crea un utente come segue:
 - a. Scegli Add user (Aggiungi utente).
 - b. Per Nome utente, digita **ServiceCatalogAdmin**.
 - c. Seleziona Accesso programmatico e Console di gestione AWS Accesso.
 - d. Scegli Successivo: autorizzazioni.
3. Scegli Attach existing policies directly (Collega direttamente le policy esistenti).
4. Scegli Crea policy, quindi procedi come segue:
 - a. Scegli la scheda JSON.
 - b. Copia la seguente politica di esempio e incollala nel documento di policy:

```
{
  "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. Scegli Successivo: Tag.
- d. (Facoltativo) Scegliete Aggiungi tag per associare una coppia chiave-valore alla risorsa. È possibile aggiungere un massimo di 50 tag.

Note

I tag sono coppie chiave-valore che puoi aggiungere alle risorse. Questo aiuta a identificare, organizzare e cercare risorse. Per ulteriori informazioni, consulta [Taggare AWS le risorse](#) nella Guida Riferimenti generali di AWS di riferimento.

- e. Scegli Prossimo: Rivedi.

- f. Per Policy name (Nome policy), digitare **ServiceCatalogAdmin-AdditionalPermissions**.

⚠ Important

È necessario concedere agli amministratori le autorizzazioni Amazon S3 per accedere ai modelli AWS Service Catalog archiviati in Amazon S3. Per ulteriori informazioni, consulta [Esempi di policy per gli utenti](#) nella Guida per l'utente di Amazon Simple Storage Service.

- g. Scegli Crea policy.
5. Tornare alla finestra del browser con la pagina delle autorizzazioni e selezionare Refresh (Aggiorna).
6. Nel campo di ricerca, digitare **ServiceCatalog** per filtrare l'elenco di policy.
7. Seleziona le caselle di controllo relative alle **ServiceCatalogAdmin-AdditionalPermissions** politiche **AWSServiceCatalogAdminFullAccess** quindi scegli Avanti: revisione.
8. Se si sta aggiornando un utente, selezionare Add permissions (Aggiungi autorizzazioni).

Se si sta creando un utente, selezionare Create user (Crea utente). È possibile scaricare o copiare le credenziali e quindi selezionare Close (Chiudi).
9. Per accedere come amministratore di catalogo, utilizza l'URL specifico del tuo account. Per trovare questo URL, selezionare Dashboard (Pannello di controllo) nel riquadro di navigazione, quindi selezionare Copy Link (Copia collegamento). Incolla il collegamento nel tuo browser e utilizza il nome e la password dell'utente IAM che hai creato o aggiornato in questa procedura.

Concedere le autorizzazioni agli utenti AWS Service Catalog finali

Prima che l'utente finale possa utilizzarlo AWS Service Catalog, devi concedere l'accesso alla visualizzazione della console dell'utente AWS Service Catalog finale. Per concedere l'accesso, alleggi le policy all'utente, al gruppo o al ruolo IAM utilizzato dall'utente finale. Nella procedura seguente, alleghiamo la **AWSServiceCatalogEndUserFullAccess** policy a un gruppo IAM.

Concessione di autorizzazioni a un gruppo di utenti finali

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.

2. Nel pannello di navigazione, seleziona Gruppi di utenti.
3. Scegli Crea gruppo ed esegui le seguenti operazioni:
 - a. Per Nome del gruppo di utenti, digitate **Endusers**.
 - b. Nel campo di ricerca, digitare **AWSServiceCatalog** per filtrare l'elenco di policy.
 - c. Seleziona la casella di controllo relativa alla **AWSServiceCatalogEndUserFullAccess** politica. Hai anche la possibilità di scegliere invece **AWSServiceCatalogEndUserReadOnlyAccess**.
 - d. Selezionare Create Group (Crea gruppo).
4. Nel pannello di navigazione, seleziona Utenti.
5. Scegli Aggiungi utenti ed esegui le seguenti operazioni:
 - a. In User name (Nome utente), digitare un nome per l'utente.
 - b. Seleziona Password - Accesso alla console di AWS gestione.
 - c. Scegli Successivo: autorizzazioni.
 - d. Scegli Add user to group (Aggiungi utente al gruppo).
 - e. Selezionare la casella di controllo per il gruppo Endusers (Enduser) e Next: Tags (Successivo: Tag), quindi Next: Review (Successivo: Verifica).
 - f. Nella pagina Review (Verifica) scegli Create user (Crea utente). Scaricare o copiare le credenziali, quindi selezionare Close (Chiudi).

Installa e configura il motore di provisioning Terraform

Per utilizzare correttamente i prodotti Terraform con AWS Service Catalog, devi installare e configurare un motore di provisioning Terraform nello stesso account in cui amministrerai i prodotti Terraform. Per iniziare, puoi utilizzare il motore di provisioning Terraform fornito da AWS, che installa e configura il codice e l'infrastruttura necessari per il funzionamento del motore di provisioning Terraform. AWS Service Catalog Questa configurazione unica richiede circa 30 minuti. AWS Service Catalog fornisce un GitHub repository con istruzioni sull'[installazione e la configurazione del motore di provisioning Terraform](#).

Determinazione della coda

Quando si richiama un'operazione di provisioning, AWS Service Catalog prepara un messaggio di payload da inviare alla coda pertinente nel motore di provisioning. Per creare l'ARN per la coda, si basa sui seguenti AWS Service Catalog presupposti:

- Il motore di approvvigionamento si trova nell'account del proprietario del prodotto
- Il motore di provisioning si trova nella stessa regione in cui è stata effettuata la chiamata a AWS Service Catalog
- Le code del motore di provisioning seguono lo schema di denominazione documentato descritto di seguito

Ad esempio, se ProvisionProduct viene richiamato us-east-1 dall'account 111111111111 utilizzando un prodotto creato dall'account 0000000000000, AWS Service Catalog presuppone che l'ARN SQS corretto sia. `arn:aws:sqs:us-east-1:000000000000:ServiceCatalogTerraformOSProvisionOperationQueue`

La stessa logica si applica alla funzione Lambda chiamata da. `DescribeProvisioningParameters`

Aggiungere Confused Deputy al motore di provisioning Terraform

Chiavi contestuali Confused Deputy sugli endpoint per limitare l'accesso alle operazioni **lambda:Invoke**

La funzione Lambda del parser parametrico creata AWS Service Catalog dai motori forniti ha una politica di accesso che concede l'autorizzazione `lambda:Invoke` tra account solo al principale del servizio: AWS Service Catalog

JSON

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

```

    },
    "Action": "lambda:InvokeFunction",
    "Resource": "arn:aws:lambda:us-
east-1:111122223333:function:ServiceCatalogTerraform0SParameterParser"
  }
]
}

```

Questa dovrebbe essere l'unica autorizzazione necessaria per il corretto funzionamento dell'integrazione con AWS Service Catalog. Tuttavia, è possibile limitarlo ulteriormente utilizzando la chiave contestuale `aws:SourceAccount` [Confused Deputy](#). Quando AWS Service Catalog invia messaggi a queste code, AWS Service Catalog compila la chiave con l'ID dell'account di provisioning. Ciò è utile quando intendi distribuire prodotti tramite la condivisione del portafoglio e vuoi assicurarti che solo account specifici utilizzino il tuo motore.

Ad esempio, puoi limitare il tuo motore in modo da consentire solo le richieste che provengono da 000000000000 e 1111 utilizzando la condizione mostrata di seguito:

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "servicecatalog.amazonaws.com"
      },
      "Action": "lambda:InvokeFunction",
      "Resource": "arn:aws:lambda:us-
east-1:111122223333:function:ServiceCatalogTerraform0SParameterParser",
      "Condition": {
        "StringLike": {
          "aws:SourceAccount": [
            "000000000000",
            "111111111111"
          ]
        }
      }
    }
  ]
}

```

}

Chiavi contestuali Deputy confuse sugli endpoint per limitare l'accesso alle operazioni **sqs:SendMessage**

Le code di presa in carico delle operazioni di provisioning create AWS Service Catalog dai motori forniti da -provided hanno una politica di accesso che concede autorizzazioni `sqs:SendMessage` multiaccount (e KMS associate) solo al responsabile del servizio: AWS Service Catalog

JSON

```
{
  "Version": "2012-10-17",
  "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-1:111122223333: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:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:GenerateDataKey"
      ],
      "Resource": "arn:aws:kms:us-east-1:111122223333:key/key_id"
    }
  ]
}
```

```

    }
  ]
}

```

Questa dovrebbe essere l'unica autorizzazione necessaria per il corretto funzionamento dell'integrazione con AWS Service Catalog. Tuttavia, è possibile limitarlo ulteriormente utilizzando la chiave contestuale `aws:SourceAccount` [Confused Deputy](#). Quando AWS Service Catalog invia messaggi a queste code, AWS Service Catalog compila le chiavi con l'ID dell'account di provisioning. Ciò è utile quando intendi distribuire prodotti tramite la condivisione del portafoglio e vuoi assicurarti che solo account specifici utilizzino il tuo motore.

Ad esempio, puoi limitare il tuo motore in modo da consentire solo le richieste che provengono da 000000000000 e 1111 utilizzando la condizione mostrata di seguito:

JSON

```

{
  "Version": "2012-10-17",
  "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-1:111122223333:ServiceCatalogTerraform0SProvision0perationQueue"
      ],
      "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:ReEncryptFrom",
      "kms:ReEncryptTo",
      "kms:GenerateDataKey"
    ],
    "Resource": "arn:aws:kms:us-east-1:111122223333:key/key_id"
  }
]
}
```

Nozioni di base

Puoi iniziare AWS Service Catalog utilizzando uno dei modelli di prodotto ben progettati disponibili nella libreria Getting Started o seguendo i passaggi di uno dei tutorial introduttivi.

Nel tutorial, svolgi attività come amministratore del catalogo e utente finale. In qualità di amministratore del catalogo, crei un portfolio e quindi un prodotto. In qualità di utente finale, verifichi di poter accedere alla console dell'utente finale e avviare il prodotto. Il prodotto è uno dei seguenti:

- Un ambiente di sviluppo cloud che funziona su Amazon Linux e si basa su un CloudFormation modello che definisce le AWS risorse che il prodotto può utilizzare.
- Un ambiente open source che funziona su un motore di provisioning Terraform e si basa su un file di configurazione tar.gz che definisce AWS le risorse che il prodotto può utilizzare.

Note

Prima di iniziare, assicurati di completare le azioni in [Configurazione AWS Service Catalog](#)

Argomenti

- [Libreria introduttiva](#)
- [Guida introduttiva a un CloudFormation prodotto](#)
- [Guida introduttiva a un prodotto Terraform](#)

Libreria introduttiva

AWS Service Catalog offre una libreria introduttiva di modelli di prodotto ben progettati per iniziare rapidamente. Puoi copiare tutti i prodotti presenti nel portfolio della libreria introduttiva sul tuo account, quindi personalizzarli in base alle tue esigenze.

Argomenti

- [Prerequisiti](#)
- [Ulteriori informazioni](#)

Prerequisiti

Prima di utilizzare i modelli nella nostra libreria introduttiva, assicurati di disporre di quanto segue:

- Le autorizzazioni necessarie per utilizzare i modelli. CloudFormation Per ulteriori informazioni, vedere [Controllo dell'accesso con AWS Identity and Access Management](#).
- Le autorizzazioni di amministratore necessarie per la gestione di AWS Service Catalog. Per ulteriori informazioni, consulta [the section called "Identity and Access Management"](#).

Ulteriori informazioni

[Per ulteriori informazioni sul framework well-architected, vedere Well-Architected.AWS](#)

Guida introduttiva a un CloudFormation prodotto

Puoi iniziare AWS Service Catalog utilizzando uno dei modelli di prodotto ben progettati disponibili nella libreria Getting Started o seguendo i passaggi del tutorial introduttivo.

Nel tutorial, svolgi attività come amministratore del catalogo e utente finale. In qualità di amministratore del catalogo, crei un portafoglio e quindi un prodotto. In qualità di utente finale, verifichi di poter accedere alla console dell'utente finale e avviare il prodotto. Il prodotto è un ambiente di sviluppo cloud che funziona su Amazon Linux e si basa su un CloudFormation modello che definisce le AWS risorse che il prodotto può utilizzare.

Note

Prima di iniziare, assicurati di completare le azioni riportate in [Configurazione AWS Service Catalog](#).

Argomenti

- [Passaggio 1: scarica il CloudFormation modello](#)
- [Fase 2: crea una coppia di chiavi](#)
- [Fase 3: Creare un portfolio](#)
- [Fase 4: Creare un nuovo prodotto nel portafoglio](#)
- [Passaggio 5: aggiungere un vincolo di modello per limitare la dimensione dell'istanza](#)
- [Passaggio 6: aggiungere un vincolo di avvio per assegnare un ruolo IAM](#)

- [Fase 7: concedere agli utenti finali l'accesso al portafoglio](#)
- [Fase 8: Verificare l'esperienza dell'utente finale](#)

Passaggio 1: scarica il CloudFormation modello

Puoi utilizzare i CloudFormation modelli per configurare ed effettuare il provisioning di portafogli e prodotti. Questi modelli sono file di testo che possono essere formattati in JSON o YAML e descrivono le risorse che si desidera fornire. Per ulteriori informazioni, consulta [Formati di modello](#) nella Guida per l'utente CloudFormation . Puoi utilizzare l' AWS CloudFormation editor o un editor di testo a tua scelta per creare e salvare modelli. In questo tutorial, forniamo un modello semplice, per iniziare. Il modello avvia una singola istanza Linux configurata per l'accesso SSH.

Note

L'utilizzo dei CloudFormation modelli richiede autorizzazioni speciali. Prima di iniziare, assicurati di disporre delle autorizzazioni corrette. Per ulteriori informazioni, consulta i prerequisiti in. [Libreria introduttiva](#)

Download del modello

Il modello di esempio fornito per questo tutorial è disponibile all'indirizzo <https://awsdocs.s3.amazonaws.com/servicecatalog/development-environment.template>. development-environment.template

Panoramica del modello

Di seguito è riportato il testo del modello di esempio:

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

```

Risorse del modello

Il modello dichiara le risorse da creare all'avvio del prodotto e comporta le seguenti sezioni:

- `AWSTemplateFormatVersion` (opzionale) — La versione del [formato AWS modello utilizzata per creare questo modello](#). L'ultima versione del formato modello è il 2010-09-09 ed è attualmente l'unico valore valido.
- `Descrizione` (opzionale): una descrizione del modello.
- `Parametri` (facoltativi): i parametri che l'utente deve specificare per avviare il prodotto. Per ogni parametro, il modello include una descrizione e i vincoli che devono essere soddisfatti dal valore digitato. Per ulteriori informazioni sui vincoli, consulta [Utilizzo dei AWS Service Catalog vincoli](#).

Il `KeyName` parametro consente di specificare il nome di una coppia di chiavi Amazon Elastic Compute Cloud (Amazon EC2) che gli utenti finali devono fornire quando utilizzano AWS Service Catalog per lanciare il prodotto. La coppia di chiavi sarà creata nella fase successiva.

- `Metadati` (facoltativi): oggetti che forniscono informazioni aggiuntive sul modello. La chiave [AWS::CloudFormation::Interface](#) definisce il modo in cui la visualizzazione della console dell'utente finale mostra i parametri. La proprietà `ParameterGroups` definisce il modo in cui i parametri sono raggruppati e le intestazioni per quei gruppi. La proprietà `ParameterLabels` definisce nomi di parametro descrittivi. Quando un utente specifica dei parametri per avviare un prodotto basato su questo modello, la vista della console utente finale visualizza il parametro etichettato `Server size:` sotto l'intestazione `Instance configuration` e visualizza i parametri etichettati `Key pair:` e `CIDR range:` sotto l'intestazione `Security configuration`.
- `Mappature` (opzionale): una mappatura delle chiavi e dei valori associati che è possibile utilizzare per specificare i valori dei parametri condizionali, in modo simile a una tabella di ricerca. È possibile abbinare una chiave a un valore corrispondente utilizzando la funzione `FindInMap` intrinseca [Fn:: nelle sezioni Risorse](#) e `Uscite`. Il modello sopra riportato include un elenco di AWS regioni e l'Amazon Machine Image (AMI) corrispondente a ciascuna di esse. AWS Service Catalog utilizza

questa mappatura per determinare quale AMI utilizzare in base alla AWS regione selezionata dall'utente in. Console di gestione AWS

- Risorse (obbligatorie): impila le risorse e le relative proprietà. Puoi fare riferimento alle risorse nelle sezioni Risorse e Output del modello. Nel modello precedente, specifichiamo un' EC2 istanza che esegue Amazon Linux e un gruppo di sicurezza che consente l'accesso SSH all'istanza. La sezione Properties della risorsa dell' EC2 istanza utilizza le informazioni digitate dall'utente per configurare il tipo di istanza e un nome chiave per l'accesso SSH.

CloudFormation utilizza la AWS regione corrente per selezionare l'ID AMI dalle mappature definite in precedenza e gli assegna un gruppo di sicurezza. Il gruppo di sicurezza è configurato per consentire l'accesso in entrata sulla porta 22 a partire dall'intervallo di indirizzi IP CIDR specificato dall'utente.

- Output (opzionale): testo che indica all'utente quando il lancio del prodotto è completo. Il modello fornito ottiene il nome DNS pubblico dell'istanza avviata e lo visualizza per l'utente. L'utente necessita del nome DNS per eseguire la connessione all'istanza tramite SSH.

Per ulteriori informazioni sulla pagina di anatomia del modello, consulta il [riferimento al modello nella Guida](#) per l'CloudFormation utente.

Fase 2: crea una coppia di chiavi

Per consentire agli utenti finali di lanciare il prodotto basato sul modello di esempio di questo tutorial, devi creare una coppia di EC2 chiavi Amazon. Una coppia di chiavi è una combinazione di una chiave pubblica utilizzata per crittografare i dati e una chiave privata utilizzata per decrittografarli. Per ulteriori informazioni sulle coppie di chiavi, assicurati di aver effettuato l'accesso alla AWS console, quindi consulta [Amazon EC2 Key Pairs](#) nella Amazon EC2 User Guide.

Il CloudFormation modello per questo tutorial include il KeyName parametro: `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"
    },
  },
```


. . .

Gli utenti finali devono specificare il nome di una key pair quando la utilizzano AWS Service Catalog per lanciare il prodotto basato sul modello.

Se intendi utilizzare una coppia di chiavi disponibile nel tuo account, puoi passare alla [Fase 3: Creare un portfolio](#). In alternativa, completa la procedura seguente.

Come creare una coppia di chiavi

1. Apri la EC2 console Amazon all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel riquadro di navigazione, sotto Network & Security (Rete e sicurezza), scegliere Key Pairs (Coppie di chiavi).
3. Nella pagina Key Pairs (Coppie di chiavi), scegliere Create Key Pair (Crea coppia di chiavi).
4. Per Key pair name (Nome di coppia di chiavi), digitare un nome facile da ricordare, quindi scegliere Create (Crea).
5. Quando la console richiede di salvare il file della chiave privata, salvarlo in un luogo sicuro.

 Important

Questo è l'unico momento in cui salvare il file della chiave privata.

Fase 3: Creare un portfolio

Per fornire prodotti agli utenti, crea innanzi tutto un portafoglio per tali prodotti.

Come creare un portafoglio

1. Aprire la console Service Catalog all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Nel pannello di navigazione a sinistra, scegli Portfolio, quindi scegli Crea portfolio.
3. Digita i seguenti valori:
 - Portfolio name (Nome portafoglio) - **Engineering Tools**
 - Descrizione del portfolio: **Sample portfolio that contains a single product.**
 - Proprietario — **IT (it@example.com)**
4. Scegli Create (Crea).

Fase 4: Creare un nuovo prodotto nel portafoglio

Dopo aver creato un portfolio, sei pronto per creare un prodotto all'interno del portfolio. Per questo tutorial, creerai un prodotto chiamato Linux Desktop, un ambiente di sviluppo cloud che funziona su Amazon Linux, all'interno del portafoglio Engineering Tool.

Per creare un prodotto all'interno di un portafoglio

1. Se si è appena completata la fase precedente, la pagina Portfolios (Portafogli) è già visualizzata. In caso contrario, apri <https://console.aws.amazon.com/servicecatalog/>.
2. Scegli e apri il portafoglio di strumenti di ingegneria che hai creato nella fase 2.
3. Scegliere Upload new product (Carica un nuovo prodotto).
4. Nella pagina Crea prodotto nella sezione Dettagli del prodotto, inserisci quanto segue:
 - Product name (Nome prodotto) – **Linux Desktop**
 - Descrizione del prodotto — **Cloud development environment configured for engineering staff. Runs AWS Linux.**
 - Proprietario — **IT**
 - Distributore — (vuoto)
5. Nella pagina dei dettagli della versione, scegli Usa un CloudFormation modello. Quindi scegli Specificare un URL del modello Amazon S3 e inserisci quanto segue:
 - Select template (Seleziona modello) – **https://awsdocs.s3.amazonaws.com/servicecatalog/development-environment.template**
 - Titolo della versione: **v1.0**
 - Descrizione: **Base Version**
6. Nella sezione Dettagli del supporto, inserisci quanto segue:
 - Contatto via e-mail — **ITSupport@example.com**
 - Link di supporto — **https://wiki.example.com/IT/support**
 - Descrizione del supporto — **Contact the IT department for issues deploying or connecting to this product.**
7. Scegli Crea prodotto.

Passaggio 5: aggiungere un vincolo di modello per limitare la dimensione dell'istanza

I vincoli aggiungono un ulteriore livello di controllo sui prodotti a livello di portafoglio, in quanto consentono di verificare il contesto di avvio di un prodotto (vincoli di avvio) oppure di aggiungere regole al modello di CloudFormation (vincoli di modello). Per ulteriori informazioni, consulta [Utilizzo dei AWS Service Catalog vincoli](#).

Aggiungi un vincolo relativo al modello al prodotto Linux Desktop che impedisce agli utenti di selezionare tipi di istanze di grandi dimensioni al momento dell'avvio. Il modello sviluppo-ambiente consente all'utente di selezionare tra sei tipi di istanza; questo vincolo limita i tipi di istanza validi ai due tipi più piccoli, ovvero `t2.micro` e `t2.small`. Per ulteriori informazioni, consulta le [istanze T2](#) nella Amazon EC2 User Guide.

Per aggiungere un vincolo di modello al prodotto Linux Desktop

1. Nella pagina dei dettagli del portfolio, scegli Vincoli, quindi scegli Crea vincolo.
2. Nella pagina Crea vincolo, per Prodotto, scegli Linux Desktop. Quindi, per Tipo di vincolo, scegliete Modello.
3. Nella sezione Vincolo del modello T, scegli Editor di testo.
4. Incolla quanto segue nell'editor di testo:

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

5. Per la descrizione del vincolo, immettete **Small instance sizes**
6. Scegli Create (Crea).

Passaggio 6: aggiungere un vincolo di avvio per assegnare un ruolo IAM

Un vincolo di lancio designa un ruolo IAM da AWS Service Catalog assumere quando un utente finale lancia un prodotto.

Per questo passaggio, aggiungi un vincolo di lancio al prodotto Linux Desktop, in modo da AWS Service Catalog poter utilizzare le risorse IAM che costituiscono il modello del prodotto. AWS CloudFormation

Il ruolo IAM assegnato a un prodotto come vincolo di lancio deve avere le seguenti autorizzazioni

1. AWS CloudFormation
2. Servizi inclusi nel modello del prodotto AWS CloudFormation
3. Accesso in lettura al AWS CloudFormation modello in un bucket Amazon S3 di proprietà del servizio.

Questo vincolo di avvio consente all'utente finale di lanciare il prodotto e, dopo il lancio, di gestirlo come prodotto fornito. Per ulteriori informazioni, consulta [AWS Service Catalog Launch Constraints \(Vincoli di lancio di SC\)](#).

Senza vincoli di lancio, è necessario concedere autorizzazioni IAM aggiuntive agli utenti finali prima che possano utilizzare il prodotto Linux Desktop. Ad esempio, la `ServiceCatalogEndUserAccess` policy concede le autorizzazioni IAM minime necessarie per accedere alla visualizzazione della console dell' AWS Service Catalog utente finale.

L'utilizzo di un vincolo di avvio consente di seguire la best practice IAM di ridurre al minimo le autorizzazioni IAM degli utenti finali. Per ulteriori informazioni, consulta [Assegnare il privilegio minimo](#) nella Guida per l'utente IAM.

Aggiunta di un vincolo di avvio

1. Segui le istruzioni per [creare nuove politiche nella scheda JSON nella guida per l'utente IAM](#).
2. Incolla il seguente documento di policy JSON:
 - `cloudformation`— Consente le autorizzazioni AWS Service Catalog complete per creare, leggere, aggiornare, eliminare, elencare e contrassegnare pile di tag CloudFormation .
 - `ec2`— Consente le autorizzazioni AWS Service Catalog complete per elencare, leggere, scrivere, fornire ed etichettare le risorse Amazon Elastic Compute Cloud (Amazon EC2) che

fanno parte del prodotto. AWS Service Catalog A seconda della AWS risorsa che desideri distribuire, questa autorizzazione potrebbe cambiare.

- **ec2**— Crea una nuova policy gestita per il tuo AWS account e allega la policy gestita specificata al ruolo IAM specificato.
- **s3**— Consente l'accesso ai bucket Amazon S3 di proprietà di. AWS Service Catalog Per distribuire il prodotto, è AWS Service Catalog necessario accedere agli artefatti di provisioning.
- **servicecatalog**— Consente AWS Service Catalog le autorizzazioni per elencare, leggere, scrivere, etichettare e avviare risorse per conto dell'utente finale.
- **sns**— Consente AWS Service Catalog le autorizzazioni per elencare, leggere, scrivere ed etichettare gli argomenti di Amazon SNS per il vincolo di avvio.

Note

A seconda delle risorse sottostanti che desideri distribuire, potrebbe essere necessario modificare la policy JSON di esempio.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "cloudformation:GetTemplateSummary",
        "cloudformation:SetStackPolicy",
        "cloudformation:ValidateTemplate",
        "cloudformation:UpdateStack",
        "ec2:*",
        "servicecatalog:*",
        "sns:*"
      ],
      "Resource": "*"
    }
  ]
}
```

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

3. Scegli Avanti, Tag.
4. Scegli Avanti, Rivedi.
5. Nella pagina della politica di revisione, per il nome, inserisci **linuxDesktopPolicy**.
6. Scegli Crea policy.
7. Nel riquadro di navigazione, seleziona Ruoli. Quindi scegli Crea ruolo ed esegui le seguenti operazioni:
 - a. Per Seleziona entità affidabile, scegli AWS servizio e quindi in Caso d'uso per altri AWS servizi scegli Service Catalog. Seleziona lo use case Service Catalog, quindi scegli Avanti.
 - b. Cerca la linuxDesktopPolicy politica, quindi seleziona la casella di controllo.
 - c. Scegli Next (Successivo).
 - d. Per Role name (Nome ruolo), digita **linuxDesktopLaunchRole**.
 - e. Scegli Crea ruolo.
8. Apri la AWS Service Catalog console in <https://console.aws.amazon.com/servicecatalog>.
9. Selezionare il portafoglio Engineering Tools (Strumenti di progettazione).
10. Nella pagina dei dettagli del portfolio, scegli la scheda Vincoli, quindi scegli Crea vincolo.
11. Per Prodotto, scegli Linux Desktop e, per il tipo di vincolo, scegli Launch.
12. Scegli Seleziona il ruolo IAM. Quindi scegli linuxDesktopLaunchRuolo, quindi scegli Crea.

Fase 7: concedere agli utenti finali l'accesso al portafoglio

Dopo aver creato un portafoglio e aggiunto un prodotto, puoi concedere l'accesso agli utenti finali.

Prerequisiti

Se non hai creato un gruppo IAM per gli utenti finali, consulta [Concedere le autorizzazioni agli utenti AWS Service Catalog finali](#).

Concessione dell'accesso al portafoglio

1. Nella pagina dei dettagli del portfolio, scegli la scheda Accesso.
2. Selezionare Grant access (Concedi accesso).
3. Nella scheda Gruppi, seleziona la casella di controllo relativa al gruppo IAM per gli utenti finali.
4. Scegli Aggiungi accesso.

Fase 8: Verificare l'esperienza dell'utente finale

Per verificare che l'utente finale possa accedere correttamente alla visualizzazione della console dell'utente finale e lanciare il prodotto, accedi AWS come utente finale ed esegui tali attività.

Verifica dell'accesso dell'utente finale alla console utente finale

1. Segui le istruzioni per [accedere come utente IAM](#) nella guida per l'utente IAM.
2. Nella barra dei menu, scegli la AWS regione in cui hai creato il Engineering Tools portfolio. Per questo tutorial, scegli la regione us-east-1.
3. Apri la AWS Service Catalog console all'indirizzo <https://console.aws.amazon.com/servicecatalog/> per vedere:
 - Products (Prodotti) – I prodotti che l'utente può utilizzare.
 - Provisioned products (Prodotti con provisioning) – I prodotti con provisioning che l'utente ha avviato.

Per verificare che l'utente finale possa avviare il prodotto Linux Desktop

Nota che per questo tutorial, scegli la regione us-east-1.

1. Nella sezione Prodotti della console, scegli Linux Desktop.

2. Scegli Launch product per avviare la procedura guidata che configura il prodotto.
3. Nella pagina Launch: Linux Desktop, inserisci **Linux-Desktop** il nome del prodotto fornito.
4. Nella pagina Parametri, inserisci quanto segue e scegli Avanti:
 - Dimensioni del server: scegli **t2.micro**.
 - Key pair (Coppia di chiavi) – Seleziona la coppia di chiavi che hai creato in [Fase 2: crea una coppia di chiavi](#).
 - Intervallo CIDR: immettere un intervallo CIDR valido per l'indirizzo IP da connettere all'istanza. Puoi utilizzare il valore predefinito (0.0.0.0/0) per consentire l'accesso da qualsiasi indirizzo IP, quindi il tuo indirizzo IP, seguito da **/32** per limitare l'accesso solo al tuo indirizzo IP o qualcosa di intermedio.
5. Scegli Launch product per lanciare lo stack. La console visualizza la pagina dei dettagli dello stack Linux-Desktop. Lo stato iniziale del prodotto è In corso di modifica. Il lancio del prodotto richiede alcuni minuti. AWS Service Catalog Per visualizzare lo stato corrente, aggiorna il browser. Dopo il lancio del prodotto, lo stato è A disponibile.

Guida introduttiva a un prodotto Terraform

AWS Service Catalog [consente un approvvigionamento rapido e self-service con governance interna per le HashiCorp configurazioni Terraform](#). AWS Puoi utilizzarle AWS Service Catalog come unico strumento per organizzare, governare e distribuire le tue configurazioni Terraform su larga scala. AWS AWS Service Catalog supporta Terraform attraverso diverse funzionalità chiave, tra cui la catalogazione di modelli Terraform standardizzati e preapprovati, il controllo degli accessi, il controllo delle versioni, l'etichettatura e la condivisione con altri account. AWS In AWS Service Catalog, gli utenti finali visualizzano un semplice elenco di prodotti e versioni a cui hanno accesso e possono quindi distribuire tali prodotti con un'unica azione.

Note

Per continuare a supportare HashiCorp le tecnologie, a seguito delle recenti modifiche alle licenze di Terraform, sono stati AWS Service Catalog modificati tutti i riferimenti precedenti di Terraform Open Source a External. Il tipo di prodotto External include il supporto per Terraform Community Edition, precedentemente nota come Terraform Open Source. Per ulteriori informazioni e istruzioni sulla migrazione dei prodotti Terraform Open Source

esistenti e dei prodotti forniti al tipo di prodotto External, consulta. [Aggiornamento dei prodotti Terraform Open Source esistenti e dei prodotti forniti al tipo di prodotto esterno](#)

I passaggi del seguente tutorial ti aiuteranno a iniziare con un prodotto Terraform in AWS Service Catalog

In qualità di amministratore del catalogo, lavori in un account amministratore centrale (account hub). Sia i prodotti Terraform Community Edition che Terraform Cloud richiedono un motore di provisioning Terraform, sul quale puoi trovare ulteriori informazioni in and. [Motore di provisioning per Terraform Community Edition \(tipo di prodotto esterno\)](#) [Motore di provisioning per Terraform Cloud](#)

Durante il tutorial, esegui le seguenti attività nell'account amministratore:

- Crea un prodotto Terraform utilizzando il tipo di prodotto Terraform Cloud o External. Service Catalog utilizza il tipo di prodotto External per supportare i prodotti Terraform Community Edition.
- Associa il prodotto a un portafoglio
- Crea un vincolo di lancio per consentire agli utenti finali di fornire il prodotto
- Etichetta il prodotto
- Condividi il portafoglio e il prodotto Terraform con l'account utente finale (account spoke)

Nel tutorial, condividi un portafoglio utilizzando l'opzione di condivisione dell'organizzazione dall'account admin hub, che è anche l'account di gestione dell'organizzazione. Per ulteriori informazioni sulla condivisione dell'organizzazione, consulta [Condivisione di un portafoglio](#).

La AWS risorsa contenuta nel prodotto Terraform che crei nel tutorial è un semplice bucket Amazon S3.

Note

Prima di iniziare, assicurati di completare le azioni riportate in. [Configurazione AWS Service Catalog](#)

Argomenti

- [Aggiornamento dei prodotti Terraform Open Source esistenti e dei prodotti forniti al tipo di prodotto esterno](#)

- [Prerequisito: configura il tuo motore di provisioning Terraform](#)
- [Passaggio 1: download del file di configurazione Terraform](#)
- [Passaggio 2: creare un prodotto Terraform](#)
- [Fase 3: Creare un AWS Service Catalog portfolio](#)
- [Fase 4: Aggiungere il prodotto al portafoglio](#)
- [Fase 5: Creare ruoli di lancio](#)
- [Passaggio 6: aggiungi un vincolo di lancio al tuo prodotto Terraform](#)
- [Fase 7: concedere l'accesso all'utente finale](#)
- [Fase 8: Condivisione del portafoglio con l'utente finale](#)
- [Fase 9: Verificare l'esperienza dell'utente finale](#)
- [Fase 10: Monitoraggio delle operazioni di approvvigionamento di Terraform](#)

Aggiornamento dei prodotti Terraform Open Source esistenti e dei prodotti forniti al tipo di prodotto esterno

Per continuare a supportare HashiCorp le tecnologie, a seguito delle recenti modifiche alle licenze di Terraform, tutti i riferimenti precedenti di Terraform Open AWS Service Catalog Source sono stati modificati in External. Il tipo di prodotto External include il supporto per Terraform Community Edition, precedentemente noto come Terraform Open Source. AWS Service Catalog non supporta più Terraform Open Source come tipo di prodotto valido per nuovi prodotti o prodotti forniti. Puoi solo aggiornare o terminare le risorse Open Source Terraform esistenti, incluse le versioni del prodotto e i prodotti forniti.

Se non l'hai già fatto, devi trasferire tutti i prodotti Terraform Open Source esistenti e i prodotti forniti a prodotti esterni, seguendo le istruzioni in questa sezione.

1. Aggiorna il tuo Terraform Reference Engine esistente per AWS Service Catalog includere il supporto per i tipi di prodotti External e Terraform Open Source. [Per istruzioni sull'aggiornamento del tuo Terraform Reference Engine, consulta il nostro Repository. GitHub](#)
2. Ricrea tutti i prodotti Terraform Open Source esistenti utilizzando il nuovo tipo di prodotto esterno.
3. Elimina tutti i prodotti esistenti che utilizzano il tipo di prodotto Terraform Open Source.
4. Riassegna le risorse rimanenti per utilizzare il nuovo tipo di prodotto esterno.
5. Termina tutti i prodotti forniti esistenti che utilizzano il tipo di prodotto Terraform Open Source.

Dopo la transizione dei prodotti esistenti, utilizza il tipo di prodotto esterno per tutti i nuovi prodotti che utilizzano un file di configurazione tar.gz.

AWS Service Catalog supporterà i clienti durante questa modifica, se necessario. Se queste modifiche richiedono un notevole impegno per il tuo account o influiscono sui carichi di lavoro critici dei prodotti, contatta il rappresentante del tuo account per richiedere assistenza.

Prerequisito: configura il tuo motore di provisioning Terraform

Come prerequisito per creare prodotti Terraform in AWS Service Catalog, è necessario installare e configurare un motore di provisioning nel proprio account amministratore di Service Catalog (account hub). Il motore di provisioning è necessario sia per i prodotti Terraform Community Edition (utilizzando il tipo di prodotto External) sia per i prodotti Terraform Cloud (che utilizzano il tipo di prodotto Terraform Cloud).

Note

La configurazione del motore è una configurazione unica che richiede circa 30 minuti.

Motore di provisioning per Terraform Community Edition (tipo di prodotto esterno)

AWS Service Catalog utilizza il tipo di prodotto External per supportare i prodotti Terraform Community Edition. Il tipo di prodotto esterno supporta anche altri strumenti di provisioning, tra cui Pulumi, Ansible, Chef e altri, basati sulla configurazione del motore di provisioning.

Per AWS Service Catalog i prodotti che utilizzano il tipo di prodotto esterno con Terraform Community Edition, HashiCorp è necessario installare e configurare un motore di provisioning Terraform nel proprio AWS Service Catalog account amministratore (account hub). AWS gestisce questo motore e le sue risorse.

AWS Service Catalog fornisce un GitHub repository con istruzioni sull'[installazione e la configurazione del motore di provisioning AWS Terraform fornito](#). Il repository include le seguenti informazioni:

- Strumenti di installazione richiesti
- Compilazione del codice
- Distribuzione su un account AWS

- Informazioni aggiuntive sul provisioning dei flussi di lavoro, sul controllo della qualità e sulle limitazioni

Motore di provisioning per Terraform Cloud

Per AWS Service Catalog i prodotti che utilizzano il tipo di prodotto Terraform Cloud con Terraform Cloud, HashiCorp è necessario installare e configurare un motore di provisioning Terraform nel proprio account amministratore (account hub). AWS Service Catalog HashiCorp gestisce questo motore in un ambiente remoto.

HashiCorp fornisce un GitHub repository con istruzioni sulla configurazione del motore [Terraform Cloud](#) per. AWS Service Catalog Il repository include le seguenti informazioni:

- Strumenti di installazione richiesti
- Compilazione del codice
- Distribuzione su un account AWS
- Informazioni aggiuntive sul provisioning dei flussi di lavoro, sul controllo della qualità e sulle limitazioni

Passaggio 1: download del file di configurazione Terraform

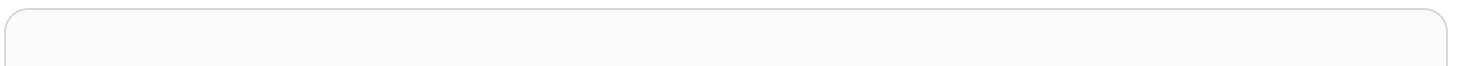
Puoi utilizzare un file di configurazione Terraform per creare e fornire prodotti HashiCorp Terraform. Queste configurazioni sono file di testo semplice e descrivono le risorse che si desidera fornire. È possibile utilizzare l'editor di testo desiderato per creare, aggiornare e salvare le configurazioni. Per la creazione del prodotto, è necessario caricare le configurazioni Terraform come file tar.gz. In questo tutorial, AWS Service Catalog fornisce un semplice file di configurazione per iniziare. La configurazione crea un bucket Amazon S3.

Download del file di configurazione

AWS Service Catalog fornisce un file [simple-s3-bucket.tar.gz](#) di configurazione di esempio da utilizzare in questo tutorial.

Panoramica del file di configurazione

Segue il testo del file di configurazione di esempio:



```
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
}
```

Risorse di configurazione

Il file di configurazione dichiara le risorse da creare durante il AWS Service Catalog provisioning del prodotto. e comporta le seguenti sezioni:

- **Variabile (opzionale):** le definizioni dei valori che un utente amministratore (amministratore dell'account hub) può assegnare per personalizzare la configurazione. Le variabili forniscono un'interfaccia coerente per modificare il comportamento di una determinata configurazione. L'etichetta dopo la parola chiave `variable` è un nome per la variabile, che deve essere univoco tra tutte le variabili dello stesso modulo. Questo nome viene utilizzato per assegnare un valore esterno alla variabile e per fare riferimento al valore della variabile dall'interno del modulo.
- **Provider (opzionale):** il fornitore di servizi cloud per la fornitura di risorse, che è. AWS AWS Service Catalog supporta solo AWS come provider. Di conseguenza, il motore di provisioning Terraform sostituisce qualsiasi altro provider elencato. AWS
- **Risorsa (richiesta):** la risorsa dell' AWS infrastruttura per il provisioning. Per questo tutorial, il file di configurazione Terraform specifica Amazon S3.
- **Output (opzionale):** le informazioni o il valore restituiti, simili ai valori restituiti in un linguaggio di programmazione. È possibile utilizzare i dati di output per configurare il flusso di lavoro dell'infrastruttura con strumenti di automazione.

Passaggio 2: creare un prodotto Terraform

Dopo aver installato il motore di provisioning Terraform, sei pronto per creare un prodotto HashiCorp Terraform in. AWS Service Catalog In questo tutorial, crei un prodotto Terraform contenente un semplice bucket Amazon S3.

Per creare un prodotto Terraform

1. Apri la AWS Service Catalog console all'indirizzo <https://console.aws.amazon.com/servicecatalog/> e accedi come utente amministratore.
2. Vai alla sezione Amministrazione, quindi scegli Elenco prodotti.
3. Scegli Crea prodotto.
4. Nella pagina Crea prodotto nella sezione Dettagli del prodotto, scegli il tipo di prodotto External o Terraform Cloud. Service Catalog utilizza il tipo di prodotto External per supportare i prodotti Terraform Community Edition.
5. Inserisci i seguenti dettagli del prodotto:
 - Product name (Nome prodotto) – **Simple S3 bucket**
 - Descrizione del prodotto: prodotto Terraform contenente un bucket Amazon S3.
 - Proprietario — **IT**
 - Distributore — (vuoto)
6. Nel riquadro dei dettagli della versione, scegli Carica un file modello, quindi scegli Scegli file. Seleziona il file in cui hai scaricato [Passaggio 1: download del file di configurazione Terraform](#).
7. Immetti i seguenti dati:
 - Nome della versione: **v1.0**
 - Descrizione della versione: **Base Version**
8. Nella sezione Dettagli del supporto, inserisci quanto segue e quindi scegli Crea prodotto.
 - Contatto via e-mail: **ITSupport@example.com**
 - Link di supporto — **https://wiki.example.com/IT/support**
 - Descrizione del supporto — **Contact the IT department for issues deploying or connecting to this product.**
9. Scegli Crea prodotto.

Dopo aver creato correttamente il prodotto, AWS Service Catalog visualizza un banner di conferma nella pagina del prodotto.

Fase 3: Creare un AWS Service Catalog portfolio

Puoi creare un portfolio nel tuo account AWS Service Catalog amministratore (account hub) per organizzare e distribuire facilmente il prodotto agli account degli utenti finali (account spoke).

Come creare un portafoglio

1. Apri la AWS Service Catalog console all'indirizzo <https://console.aws.amazon.com/servicecatalog/> e accedi come amministratore.
2. Nel pannello di navigazione a sinistra, scegli Portfolio, quindi scegli Crea portfolio.
3. Immetti uno dei seguenti valori:
 - Portfolio name (Nome portafoglio) - **S3 bucket**
 - Descrizione del portfolio: **Sample portfolio for Terraform configurations.**
 - Proprietario — **IT (it@example.com)**
4. Scegli Create (Crea).

Fase 4: Aggiungere il prodotto al portafoglio

Dopo aver creato un portfolio, puoi aggiungere il prodotto HashiCorp Terraform che hai creato nella fase 2.

Per aggiungere un prodotto a un portafoglio

1. Vai alla pagina con l'elenco dei prodotti.
2. Seleziona il prodotto Terraform con bucket Simple S3 che hai creato nel passaggio 2, quindi scegli Azioni. Dal menu a discesa, scegli Aggiungi prodotto al portafoglio. AWS Service Catalog visualizza il riquadro Aggiungi un bucket Simple S3 al portafoglio.
3. Seleziona il portafoglio di bucket S3, quindi disattiva Create launch constraint. Il vincolo di avvio verrà creato più avanti nel tutorial.
4. Scegli Aggiungi prodotto al portafoglio.

Dopo aver aggiunto correttamente il prodotto al portafoglio, AWS Service Catalog visualizza un banner di conferma nella pagina con l'elenco dei prodotti.

Fase 5: Creare ruoli di lancio

In questo passaggio, creerai un ruolo IAM (ruolo di lancio) che specifica le autorizzazioni che il motore di provisioning Terraform e il motore di provisioning Terraform AWS Service Catalog possono assumere quando un utente finale lancia un prodotto Terraform. HashiCorp

Il ruolo IAM (ruolo di lancio) che successivamente assegnerai al tuo semplice prodotto Terraform con bucket Amazon S3 come vincolo di lancio deve avere le seguenti autorizzazioni:

- Accesso alle risorse di base per il tuo prodotto Terraform. AWS In questo tutorial, è incluso l'accesso alle `s3:DeleteBucket*` operazioni `s3:CreateBucket*s3:Get*`, `s3:List*`, e `s3:PutBucketTagging` Amazon S3.
- Accesso in lettura al modello Amazon S3 in un bucket Amazon AWS Service Catalog S3 di proprietà
- Accesso alle operazioni del gruppo di `CreateGroup` risorse `ListGroupResources`, `DeleteGroup`, e `Tag`. Queste operazioni consentono AWS Service Catalog di gestire gruppi di risorse e tag

Per creare un ruolo di lancio nell'account AWS Service Catalog amministratore

1. Dopo aver effettuato l'accesso all'account AWS Service Catalog amministratore, segui le istruzioni per [creare nuove politiche nella scheda JSON](#) nella guida per l'utente IAM.
2. Crea una policy per il tuo semplice prodotto Terraform con bucket Amazon S3. Questa politica deve essere creata prima di creare il ruolo di lancio e comprende le seguenti autorizzazioni:
 - `s3`— Consente le autorizzazioni AWS Service Catalog complete per elencare, leggere, scrivere, fornire ed etichettare il prodotto Amazon S3.
 - `s3`— Consente l'accesso ai bucket Amazon S3 di proprietà di. AWS Service Catalog Per distribuire il prodotto, è AWS Service Catalog necessario accedere agli artefatti di provisioning.
 - `resourcegroups`— Consente di creare, AWS Service Catalog elencare, eliminare e contrassegnare. AWS Resource Groups
 - `tag`— Consente le autorizzazioni di AWS Service Catalog etichettatura.

Note

A seconda delle risorse sottostanti che si desidera distribuire, potrebbe essere necessario modificare la policy JSON di esempio.

Incolla il seguente documento di policy JSON:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "s3:GetObject",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "s3:ExistingObjectTag/servicecatalog:provisioning":
"true"
        }
      }
    },
    {
      "Action": [
        "s3:CreateBucket*",
        "s3>DeleteBucket*",
        "s3:Get*",
        "s3:List*",
        "s3:PutBucketTagging"
      ],
      "Resource": "arn:aws:s3:::*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "resource-groups:CreateGroup",
        "resource-groups:ListGroupResources",
```

```

        "resource-groups:DeleteGroup",
        "resource-groups:Tag"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Action": [
        "tag:GetResources",
        "tag:GetTagKeys",
        "tag:GetTagValues",
        "tag:TagResources",
        "tag:UntagResources"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
]
}

```

3.
 - a. Scegli Avanti, Tags.
 - b. Scegli Avanti, Rivedi.
 - c. Nella pagina della politica di revisione, per il nome, inserisci **S3ResourceCreationAndArtifactAccessPolicy**.
 - d. Scegli Crea policy.
4. Nel pannello di navigazione, scegli Ruoli e quindi Crea ruolo.
5. Per Seleziona entità attendibile, scegli Politica di fiducia personalizzata, quindi inserisci la seguente politica JSON:
6. Scegli Next (Successivo).
7. Nell'elenco Politiche, seleziona quella S3ResourceCreationAndArtifactAccessPolicy che hai appena creato.
8. Scegli Next (Successivo).
9. Per Nome ruolo, inserisci **SCLaunch-S3product**.

 Important

I nomi dei ruoli di avvio devono iniziare con SCLaunch "" seguito dal nome del ruolo desiderato.

10. Scegli Crea ruolo.

Important

Dopo aver creato il ruolo di avvio nell'account AWS Service Catalog amministratore, è necessario creare anche un ruolo di avvio identico nell'account dell'utente AWS Service Catalog finale. Il ruolo nell'account dell'utente finale deve avere lo stesso nome e includere la stessa politica del ruolo nell'account amministratore.

Per creare un ruolo di lancio nell'account dell'utente AWS Service Catalog finale

1. Accedi come amministratore all'account dell'utente finale, quindi segui le istruzioni per [creare nuove politiche nella scheda JSON](#) nella guida per l'utente IAM.
2. Ripeti i passaggi da 2 a 10 da Per creare un ruolo di avvio nell'account AWS Service Catalog amministratore riportato sopra.

Note

Quando crei un ruolo di avvio nell'account dell'utente AWS Service Catalog finale, assicurati di utilizzare lo stesso amministratore **AccountId** nella politica di fiducia personalizzata.

Ora che hai creato un ruolo di lancio sia nell'account amministratore che in quello dell'utente finale, puoi aggiungere un vincolo di avvio al prodotto.

Passaggio 6: aggiungi un vincolo di lancio al tuo prodotto Terraform

Important

È necessario creare un vincolo di lancio per i prodotti Terraform. HashiCorp Senza un vincolo di lancio, gli utenti finali non possono fornire il prodotto.

Dopo aver creato un ruolo di lancio nel tuo account amministratore, sei pronto per associare il ruolo di lancio a un vincolo di lancio sul tuo prodotto External o Terraform Cloud.

Questo vincolo di lancio consente all'utente finale di lanciare il prodotto e, dopo il lancio, gestirlo come prodotto fornito. Per ulteriori informazioni, consulta [AWS Service Catalog Launch Constraints \(Vincoli di lancio di SC\)](#).

L'utilizzo di un vincolo di lancio consente di seguire la best practice IAM di ridurre al minimo le autorizzazioni IAM degli utenti finali. Per ulteriori informazioni, consulta [Assegnare il privilegio minimo](#) nella Guida per l'utente IAM.

Per assegnare un vincolo di lancio al prodotto

1. [Apri la AWS Service Catalog console in /servicecatalog. https://console.aws.amazon.com](#)
2. Nella console di navigazione a sinistra, scegli Portfolio.
3. Scegli il portafoglio di bucket S3.
4. Nella pagina dei dettagli del portafoglio, scegli la scheda Vincoli, quindi scegli Crea vincolo.
5. Per Prodotto, scegli Simple S3 bucket. AWS Service Catalog seleziona automaticamente il tipo di vincolo Launch.
6. Scegli Inserisci il nome del ruolo, quindi scegli -S3Product. SCLaunch
7. Scegli Crea.

Note

Il nome del ruolo specificato deve esistere nell'account che ha creato il vincolo di avvio e nell'account dell'utente che lancia un prodotto con questo vincolo di lancio.

Fase 7: concedere l'accesso all'utente finale

Dopo aver applicato il vincolo di lancio al tuo prodotto HashiCorp Terraform, sei pronto a concedere l'accesso agli utenti finali nell'account spoke.

In questo tutorial, concedi l'accesso agli utenti finali utilizzando la condivisione del nome principale. I nomi principali sono nomi di gruppi, ruoli e utenti che gli amministratori possono specificare in un portfolio e quindi condividere con il portfolio. Quando condividi il portfolio, AWS Service Catalog verifica se tali nomi principali esistono già. Se esistono, associa AWS Service Catalog automaticamente i principali IAM corrispondenti al portafoglio condiviso per concedere l'accesso agli utenti finali. Per ulteriori informazioni, [consulta la sezione Condivisione di un portafoglio](#).

Prerequisiti

Se non hai creato un gruppo IAM per gli utenti finali, consulta [Concedere le autorizzazioni agli utenti AWS Service Catalog finali](#).

Concessione dell'accesso al portafoglio

1. Vai alla pagina Portfolio e scegli il portafoglio di bucket S3.
2. Scegli la scheda Accesso, quindi scegli Concedi l'accesso.
3. Nel riquadro Tipo di accesso, scegli Nome principale.
4. Nel riquadro Nome principale, seleziona il tipo di nome principale, quindi inserisci il nome principale dell'utente finale desiderato nell'account spoke.
5. Selezionare Grant access (Concedi accesso).

Fase 8: Condivisione del portafoglio con l'utente finale

L'AWS Service Catalog amministratore può distribuire i portafogli con gli account degli utenti finali utilizzando la account-to-account condivisione o AWS Organizations la condivisione. In questo tutorial, condividi il tuo portafoglio con l'organizzazione dall'account amministratore (account hub), che è anche l'account di gestione dell'organizzazione.

Per condividere il portafoglio dall'account admin hub

1. Apri la AWS Service Catalog console all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Nella pagina Portfolio, seleziona il portafoglio di bucket S3. Nel menu Azioni, scegli Condividi.
3. Scegli AWS Organizations, quindi filtra in base alla struttura organizzativa.
4. Nel riquadro AWS Organizzazione, scegli l'account dell'utente finale (account spoke).

È inoltre possibile selezionare un nodo principale per condividere il portfolio con l'intera organizzazione, un'unità organizzativa (OU) principale o un'unità organizzativa secondaria all'interno dell'organizzazione in base alla struttura dell'organizzazione. Per ulteriori informazioni, consulta [Condivisione di un portafoglio](#).

5. Nel riquadro delle impostazioni di condivisione, scegli Condivisione principale.
6. Scegli Condividi.

Dopo aver condiviso con successo il portafoglio con gli utenti finali, il passaggio successivo consiste nel verificare l'esperienza dell'utente finale e fornire il prodotto Terraform.

Fase 9: Verificare l'esperienza dell'utente finale

Per verificare che gli utenti finali possano accedere correttamente alla console dell'utente finale, visualizzare e lanciare il **Simple S3 bucket** prodotto, accedi AWS come utente finale ed esegui le attività seguenti.

Verifica dell'accesso dell'utente finale alla console utente finale

- Apri la AWS Service Catalog console all'indirizzo <https://console.aws.amazon.com/servicecatalog/> per vedere:
 - Products (Prodotti) – I prodotti che l'utente può utilizzare.
 - Provisioned products (Prodotti con provisioning) – I prodotti con provisioning che l'utente ha avviato.

Per verificare che l'utente finale possa avviare il prodotto Terraform

1. Nella sezione Prodotti della console, scegli Simple S3 bucket.
2. Scegli Avvia prodotto per avviare la procedura guidata che configura il prodotto.
3. Nella pagina del bucket Launch Simple S3, inserisci il nome del **Amazon S3 product** prodotto fornito.
4. Nella pagina Parametri, inserisci quanto segue e scegli Avanti:
 - bucket_name — Fornisce un nome univoco per il bucket Amazon S3. Ad esempio, **terraform-s3-product**.
5. Scegli Launch product. La console visualizza la pagina dei dettagli dello stack per il lancio del prodotto Amazon S3. Lo stato iniziale del prodotto è In corso di modifica. Il lancio del prodotto richiede alcuni minuti. AWS Service Catalog Per visualizzare lo stato corrente, aggiorna il browser. Dopo il lancio riuscito del prodotto, lo stato è Disponibile.

AWS Service Catalog crea un nuovo bucket Amazon S3 denominato. **terraform-s3-product**

Fase 10: Monitoraggio delle operazioni di approvvigionamento di Terraform

Se desideri monitorare le operazioni di provisioning, puoi consultare CloudWatch i log di Amazon e qualsiasi flusso di lavoro AWS Step Functions di provisioning.

Esistono due macchine a stati per il flusso di lavoro di provisioning:

- `ManageProvisionedProductStateMachine`— AWS Service Catalog richiama questa macchina a stati durante il provisioning di un nuovo prodotto Terraform e durante l'aggiornamento di un prodotto Terraform predisposto esistente.
- `TerminateProvisionedProductStateMachine`— AWS Service Catalog richiama questa macchina a stati quando termina un prodotto fornito da Terraform esistente.

Per eseguire la macchina a stati di monitoraggio

1. Apri la console di AWS gestione e accedi come amministratore nell'account dell'hub di amministrazione in cui è installato il motore di provisioning Terraform.
2. Aprire AWS Step Functions.
3. Nel pannello di navigazione a sinistra, scegli Macchine a stati.
4. Scegli `ManageProvisionedProductStateMachine`.
5. Nell'elenco Esecuzioni, inserisci l'ID del prodotto assegnato per individuare l'esecuzione.

Note

AWS Service Catalog crea l'ID del prodotto fornito quando si effettua il provisioning del prodotto. L'ID del prodotto fornito è formattato come segue: **pp-1111pwtn[ID number]**

6. Scegli l'ID di esecuzione.

Nella pagina dei dettagli di esecuzione risultante, puoi visualizzare tutti i passaggi del flusso di lavoro di provisioning. È inoltre possibile esaminare eventuali passaggi non riusciti per identificare la causa dell'errore.

Sicurezza in AWS Service Catalog

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il [modello di responsabilità condivisa](#) descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei [programmi di conformitàAWS](#).

Per ulteriori informazioni sui programmi di conformità applicabili AWS Service Catalog, consulta la sezione [AWS Servizi rientranti nell'ambito del programma di conformità](#)

- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo AWS Service Catalog. I seguenti argomenti mostrano come configurare per AWS Service Catalog soddisfare gli obiettivi di sicurezza e conformità. Verranno inoltre presentati altri AWS servizi che consentono di monitorare e proteggere le AWS Service Catalog risorse.

Argomenti

- [Protezione dei dati in AWS Service Catalog](#)
- [Identity and Access Management in AWS Service Catalog](#)
- [Registrazione e monitoraggio AWS Service Catalog](#)
- [Convalida della conformità per AWS Service Catalog](#)
- [Resilienza in AWS Service Catalog](#)
- [Sicurezza dell'infrastruttura in AWS Service Catalog](#)
- [Migliori pratiche di sicurezza per AWS Service Catalog](#)

Protezione dei dati in AWS Service Catalog

Il modello di [responsabilità AWS condivisa modello](#) di di si applica alla protezione dei dati in AWS Service Catalog. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per maggiori informazioni sulla privacy dei dati, consulta le [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al [AWS Modello di responsabilità condivisa e GDPR](#) nel AWS Blog sulla sicurezza.

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta [Lavorare con i CloudTrail percorsi](#) nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-3](#).

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori AWS Service Catalog o Servizi AWS utilizzi la console, l'API o. AWS CLI AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando si fornisce un URL a un server esterno,

suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

Protezione dei dati con crittografia

Crittografia dei dati a riposo

AWS Service Catalog utilizza bucket Amazon S3 e database Amazon DynamoDB crittografati a riposo utilizzando chiavi gestite da Amazon. Per ulteriori informazioni, consulta le informazioni sulla crittografia a riposo fornite da Amazon S3 e Amazon DynamoDB.

Crittografia dei dati in transito

AWS Service Catalog utilizza Transport Layer Security (TLS) e la crittografia lato client delle informazioni in transito tra il chiamante e AWS.

Puoi accedere in modo privato AWS Service Catalog APIs dal tuo Amazon Virtual Private Cloud (Amazon VPC) creando endpoint VPC. Con gli endpoint VPC, il routing tra il VPC e il VPC AWS Service Catalog viene gestito dalla AWS rete senza la necessità di un gateway Internet, un gateway NAT o una connessione VPN.

L'ultima generazione di endpoint VPC utilizzata da AWS Service Catalog è alimentata da AWS PrivateLink, una AWS tecnologia che consente la connettività privata tra i AWS servizi utilizzando interfacce di rete elastiche con private in your. IPs VPCs

Identity and Access Management in AWS Service Catalog

L'accesso a AWS Service Catalog richiede credenziali. Tali credenziali devono essere autorizzate ad accedere a AWS risorse, ad esempio un AWS Service Catalog portafoglio o un prodotto. AWS Service Catalog si integra con AWS Identity and Access Management (IAM) per consentirti di concedere AWS Service Catalog agli amministratori le autorizzazioni necessarie per creare e gestire i prodotti e per concedere agli utenti AWS Service Catalog finali le autorizzazioni necessarie per lanciare prodotti e gestire i prodotti forniti. Queste politiche vengono create e gestite da AWS o singolarmente da amministratori e utenti finali. Per controllare l'accesso, alleggi queste politiche agli utenti, ai gruppi e ai ruoli con AWS Service Catalog cui utilizzi.

Destinatari

Le autorizzazioni di cui disponi AWS Identity and Access Management (IAM) possono dipendere dal ruolo che ricopri. AWS Service Catalog

Le autorizzazioni di cui disponi tramite AWS Identity and Access Management (IAM) possono dipendere anche dal ruolo che ricopri. AWS Service Catalog

Amministratore: in qualità di AWS Service Catalog amministratore, hai bisogno dell'accesso completo alla console di amministrazione e alle autorizzazioni IAM che ti consentono di eseguire attività come la creazione e la gestione di portafogli e prodotti, la gestione dei vincoli e la concessione dell'accesso agli utenti finali.

Utente finale: prima che gli utenti finali possano utilizzare i tuoi prodotti, devi concedere loro le autorizzazioni che consentano loro di accedere alla console dell'utente finale. AWS Service Catalog. Possono inoltre disporre delle autorizzazioni per avviare e gestire i prodotti con provisioning.

Amministratore IAM: se sei un amministratore IAM, potresti voler saperne di più su come scrivere policy per gestire l'accesso AWS Service Catalog. Per visualizzare esempi di policy AWS Service Catalog basate sull'identità che puoi utilizzare in IAM, consulta. [the section called “AWS politiche gestite”](#)

Esempi di policy basate sull'identità per AWS Service Catalog

Argomenti

- [Accesso alla console per gli utenti finali](#)
- [Accesso al prodotto per gli utenti finali](#)
- [Esempi di politiche per la gestione dei prodotti forniti](#)

Accesso alla console per gli utenti finali

Le policy **AWSServiceCatalogEndUserFullAccess** e **AWSServiceCatalogEndUserReadOnlyAccess** autorizzano l'accesso alla visualizzazione della console dell'utente finale di AWS Service Catalog. Quando un utente che dispone di una di queste politiche sceglie AWS Service Catalog in Console di gestione AWS, la visualizzazione della console dell'utente finale mostra i prodotti che ha l'autorizzazione a lanciare.

Prima che gli utenti finali possano lanciare con successo un prodotto AWS Service Catalog a cui concedi l'accesso, devi fornire loro autorizzazioni IAM aggiuntive per consentire loro di utilizzare ciascuna delle AWS risorse sottostanti nel modello di AWS CloudFormation un prodotto. Ad esempio, se un modello di prodotto include Amazon Relational Database Service (Amazon RDS), devi concedere agli utenti le autorizzazioni Amazon RDS per lanciare il prodotto.

Per ulteriori informazioni su come consentire agli utenti finali di lanciare prodotti applicando al contempo le autorizzazioni di accesso minimo alle risorse, consulta. AWS [the section called "Utilizzo di vincoli"](#)

Se applichi la policy **AWSServiceCatalogEndUserReadOnlyAccess**, gli utenti hanno accesso alla console utente finale, ma non disporranno delle autorizzazioni necessarie per avviare prodotti e gestire prodotti con provisioning. Puoi concedere queste autorizzazioni direttamente a un utente finale utilizzando IAM, ma se desideri limitare l'accesso degli utenti finali alle AWS risorse, devi associare la policy a un ruolo di lancio. Si utilizza quindi AWS Service Catalog per applicare il ruolo di lancio a un vincolo di lancio per il prodotto. Per ulteriori informazioni sull'applicazione di un ruolo di avvio, sui limiti dei ruoli di avvio e su un ruolo di avvio di esempio, consulta [AWS Service Catalog Vincoli di avvio](#).

Note

Se concedi agli utenti le autorizzazioni IAM per gli AWS Service Catalog amministratori, viene invece visualizzata la vista della console dell'amministratore. Non concedere agli utenti finali queste autorizzazioni se non vuoi che accedano alla vista della console di amministrazione.

Accesso al prodotto per gli utenti finali

Prima che gli utenti finali possano utilizzare un prodotto a cui concedi l'accesso, devi fornire loro autorizzazioni IAM aggiuntive per consentire loro di utilizzare ciascuna delle AWS risorse sottostanti nel CloudFormation modello di un prodotto. Ad esempio, se un modello di prodotto include Amazon Relational Database Service (Amazon RDS), devi concedere agli utenti le autorizzazioni Amazon RDS per lanciare il prodotto.

Se applichi la policy **AWSServiceCatalogEndUserReadOnlyAccess**, gli utenti hanno accesso alla vista della console utente finale, ma non disporranno delle autorizzazioni necessarie per avviare prodotti e gestire prodotti con provisioning. Puoi concedere queste autorizzazioni direttamente a un utente finale in IAM, ma se desideri limitare l'accesso degli utenti finali alle AWS risorse, devi associare la policy a un ruolo di lancio. Si utilizza quindi AWS Service Catalog per applicare il ruolo di lancio a un vincolo di lancio per il prodotto. Per ulteriori informazioni sull'applicazione di un ruolo di avvio, sui limiti dei ruoli di avvio e su un ruolo di avvio di esempio, consulta [AWS Service Catalog Vincoli di avvio](#).

Esempi di politiche per la gestione dei prodotti forniti

Puoi creare policy personalizzate per soddisfare i requisiti di sicurezza della tua organizzazione. Gli esempi seguenti descrivono come personalizzare il livello di accesso per ogni azione con supporto a livello di utente, ruolo e account. Puoi concedere agli utenti l'accesso per visualizzare, aggiornare, terminare e gestire prodotti con provisioning creati esclusivamente da tali utenti oppure creati da altri utenti mediante il relativo ruolo o l'account a cui sono connessi. Questo accesso è gerarchico: la concessione dell'accesso a livello di account garantisce anche l'accesso a livello di ruolo e l'accesso a livello utente, mentre l'aggiunta dell'accesso a livello di ruolo garantisce anche l'accesso a livello utente ma non l'accesso a livello di account. Puoi specificare questi accessi nel codice JSON della policy utilizzando un blocco `Condition` come `accountLevel`, `roleLevel` o `userLevel`.

Questi esempi si applicano anche ai livelli di accesso per le operazioni di scrittura:

`UpdateProvisionedProduct` and e lettura delle AWS Service Catalog
API:`TerminateProvisionedProduct`, e. `DescribeRecord` `ScanProvisionedProducts`
`ListRecordHistory` Le operazioni API `ScanProvisionedProducts` e `ListRecordHistory`
utilizzano `AccessLevelFilterKey` come input e i valori di tale chiave corrispondono ai livelli
del blocco `Condition` presentati in questo argomento (`accountLevel` equivale a un valore
`AccessLevelFilterKey` di "Account", `roleLevel` a un valore "Role" e `userLevel` a un valore
"User"). Per ulteriori informazioni, consulta la [Service Catalog Developer Guide](#).

Esempi

- [Accesso amministrativo completo ai prodotti forniti](#)
- [Accesso dell'utente finale ai prodotti forniti](#)
- [Accesso amministrativo parziale ai prodotti forniti](#)

Accesso amministrativo completo ai prodotti forniti

La policy seguente consente l'accesso completo in lettura e scrittura a prodotti con provisioning e record nel catalogo a livello di account.

JSON

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

```

    "Effect": "Allow",
    "Action": [
      "servicecatalog:*"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "servicecatalog:accountLevel": "self"
      }
    }
  }
]
}

```

Da un punto di vista funzionale, questa policy è equivalente alla seguente policy:

JSON

```

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

```

La mancata indicazione di un Condition blocco in nessuna policy di AWS Service Catalog viene considerata come specificare "servicecatalog:accountLevel" l'accesso. Nota che l'accesso accountLevel include l'accesso roleLevel e userLevel.

Accesso dell'utente finale ai prodotti forniti

La policy seguente limita l'accesso alle operazioni di lettura e scrittura esclusivamente ai prodotti con provisioning o ai record associati che l'utente corrente ha creato.

JSON

```

{
  "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"
        }
      }
    }
  ]
}

```

Accesso amministrativo parziale ai prodotti forniti

Le due policy esposte di seguito, se applicate entrambe allo stesso utente, consentono quello che potrebbe essere definito un tipo di "accesso amministratore parziale", fornendo accesso di sola lettura completo e accesso in scrittura limitato. Ciò significa che l'utente può visualizzare qualsiasi prodotto con provisioning o record associato nell'account del catalogo, ma non è in grado di eseguire azioni su qualsiasi prodotto con provisioning o record non di proprietà di quell'utente.

La prima policy concede all'utente l'accesso a operazioni di scrittura su prodotti con provisioning che l'utente corrente ha creato, ma non su prodotti con provisioning creati da altri utenti. La seconda

policy aggiunge accesso completo alle operazioni in lettura su prodotti con provisioning creati da tutti (utente, ruolo o account).

JSON

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

JSON

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

```

```

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

```

AWS politiche gestite per AWS Service Catalog AppRegistry

AWS politica gestita: **AWSServiceCatalogAdminFullAccess**

Puoi collegarti `AWSServiceCatalogAdminFullAccess` alle tue entità IAM. AppRegistry associa inoltre questa policy a un ruolo di servizio che consente di AppRegistry eseguire azioni per tuo conto.

Questa politica concede *administrative* autorizzazioni che consentono l'accesso completo alla visualizzazione della console dell'amministratore e concede l'autorizzazione per creare e gestire prodotti e portafogli.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `servicecatalog`— Concede ai responsabili le autorizzazioni complete per la visualizzazione della console dell'amministratore e la possibilità di creare e gestire portafogli e prodotti, gestire i vincoli, concedere l'accesso agli utenti finali ed eseguire altre attività amministrative all'interno. AWS Service Catalog
- `cloudformation`— Consente le autorizzazioni AWS Service Catalog complete per elencare, leggere, scrivere ed etichettare pile. AWS CloudFormation
- `config`— Consente autorizzazioni AWS Service Catalog limitate per portafogli, prodotti e prodotti forniti tramite. AWS Config
- `iam`— Concede ai responsabili le autorizzazioni complete per visualizzare e creare utenti, gruppi o ruoli del servizio necessari per la creazione e la gestione di prodotti e portafogli.

- `ssm`— Consente di AWS Service Catalog AWS Systems Manager elencare e leggere i documenti di Systems Manager nell' AWS account e AWS nella regione correnti.

Visualizza la politica: [AWSServiceCatalogAdminFullAccess](#).

AWS politica gestita: **AWSServiceCatalogAdminReadOnlyAccess**

Puoi collegarti `AWSServiceCatalogAdminReadOnlyAccess` alle tue entità IAM. AppRegistry associa inoltre questa policy a un ruolo di servizio che consente di AppRegistry eseguire azioni per tuo conto.

Questa politica concede *read-only* autorizzazioni che consentono l'accesso completo alla visualizzazione della console dell'amministratore. Questa politica non concede l'accesso alla creazione o alla gestione di prodotti e portafogli.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `servicecatalog`— Concede ai principali permessi di sola lettura per la visualizzazione della console dell'amministratore.
- `cloudformation`— Consente autorizzazioni AWS Service Catalog limitate per elencare e leggere gli stack. AWS CloudFormation
- `config`— Consente autorizzazioni AWS Service Catalog limitate per portafogli, prodotti e prodotti forniti tramite. AWS Config
- `iam`— Concede ai responsabili autorizzazioni limitate per visualizzare gli utenti, i gruppi o i ruoli del servizio necessari per la creazione e la gestione di prodotti e portafogli.
- `ssm`— Consente di AWS Service Catalog AWS Systems Manager elencare e leggere i documenti di Systems Manager nell' AWS account e AWS nella regione correnti.

Visualizza la politica: [AWSServiceCatalogAdminReadOnlyAccess](#).

AWS politica gestita: **AWSServiceCatalogEndUserFullAccess**

Puoi collegarti `AWSServiceCatalogEndUserFullAccess` alle tue entità IAM. AppRegistry associa inoltre questa policy a un ruolo di servizio che consente di AppRegistry eseguire azioni per tuo conto.

Questa politica concede *contributor* autorizzazioni che consentono l'accesso completo alla visualizzazione della console dell'utente finale e concede l'autorizzazione per lanciare prodotti e gestire i prodotti forniti.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `servicecatalog`— Concede ai responsabili le autorizzazioni complete per la visualizzazione della console dell'utente finale e la possibilità di lanciare prodotti e gestire i prodotti forniti.
- `cloudformation`— Consente le autorizzazioni AWS Service Catalog complete per elencare, leggere, scrivere e etichettare gli stack. AWS CloudFormation
- `config`— Consente autorizzazioni AWS Service Catalog limitate per elencare e leggere dettagli su portafogli, prodotti e prodotti forniti tramite. AWS Config
- `ssm`— Consente AWS Service Catalog di leggere AWS Systems Manager i documenti di Systems Manager nell' AWS account corrente e AWS nella regione.

Visualizza la politica: [AWSServiceCatalogEndUserFullAccess](#).

AWS politica gestita: **AWSServiceCatalogEndUserReadOnlyAccess**

Puoi collegarti `AWSServiceCatalogEndUserReadOnlyAccess` alle tue entità IAM. `AppRegistry` associa inoltre questa policy a un ruolo di servizio che consente di `AppRegistry` eseguire azioni per tuo conto.

Questa politica concede *read-only* autorizzazioni che consentono l'accesso in sola lettura alla visualizzazione della console dell'utente finale. Questa politica non concede l'autorizzazione al lancio di prodotti o alla gestione dei prodotti forniti.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `servicecatalog`— Concede ai principali permessi di sola lettura per la visualizzazione della console dell'utente finale.
- `cloudformation`— Consente autorizzazioni AWS Service Catalog limitate per elencare e leggere gli stack. AWS CloudFormation
- `config`— Consente autorizzazioni AWS Service Catalog limitate per elencare e leggere dettagli su portafogli, prodotti e prodotti forniti tramite. AWS Config

- `ssm`— Consente AWS Service Catalog di leggere AWS Systems Manager i documenti di Systems Manager nell' AWS account corrente e AWS nella regione.

Visualizza la politica: [AWSServiceCatalogEndUserReadOnlyAccess](#).

AWS politica gestita: **AWSServiceCatalogSyncServiceRolePolicy**

AWS Service Catalog allega questa policy al `AWSServiceRoleForServiceCatalogSync` service-linked role (SLR), permettendo di AWS Service Catalog sincronizzare i modelli in un repository esterno con i prodotti. AWS Service Catalog

Questa politica concede autorizzazioni che consentono un accesso limitato alle AWS Service Catalog azioni (ad esempio, chiamate API) e ad altre azioni di servizio da cui dipende. AWS AWS Service Catalog

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `servicecatalog`— Consente al ruolo di sincronizzazione degli AWS Service Catalog artefatti l'accesso limitato al pubblico. AWS Service Catalog APIs
- `codeconnections`— Consente al ruolo di sincronizzazione degli AWS Service Catalog artefatti l'accesso limitato al pubblico. CodeConnections APIs
- `cloudformation`— Consente al ruolo di sincronizzazione degli AWS Service Catalog artefatti l'accesso limitato al pubblico. AWS CloudFormation APIs

Visualizza la politica: [AWSServiceCatalogSyncServiceRolePolicy](#)

Dettagli del ruolo collegato al servizio

AWS Service Catalog utilizza i dettagli di autorizzazione di cui sopra per il ruolo `AWSServiceRoleForServiceCatalogSync` collegato al servizio che viene creato quando un utente crea o aggiorna un AWS Service Catalog prodotto che utilizza. CodeConnections È possibile modificare questa politica utilizzando la AWS CLI, l' AWS API o tramite la AWS Service Catalog console. Per ulteriori informazioni su come creare, modificare ed eliminare i ruoli collegati ai servizi, consulta [Using service-linked roles \(\) for SLRs](#) AWS Service Catalog

Le autorizzazioni incluse nel ruolo `AWSServiceRoleForServiceCatalogSync` collegato al servizio consentono di eseguire le seguenti azioni AWS Service Catalog per conto del cliente.

- `servicecatalog:ListProvisioningArtifacts`— Consente al ruolo di sincronizzazione degli AWS Service Catalog artefatti di elencare gli elementi di provisioning per un determinato AWS Service Catalog prodotto sincronizzato con un file modello in un repository.
- `servicecatalog:DescribeProductAsAdmin`— Consente al ruolo di sincronizzazione degli AWS Service Catalog artefatti di utilizzare l'`DescribeProductAsAdminAPI` per ottenere dettagli su un AWS Service Catalog prodotto e sugli elementi assegnati a esso associati, sincronizzati con un file modello in un repository. Il ruolo di sincronizzazione degli artefatti utilizza l'output di questa chiamata per verificare il limite di quota di servizio del prodotto per il provisioning degli artefatti.
- `servicecatalog>DeleteProvisioningArtifact`— Consente al ruolo di sincronizzazione degli AWS Service Catalog artefatti di eliminare un artefatto fornito.
- `servicecatalog:ListServiceActionsForProvisioningArtifact`— Consente al ruolo di sincronizzazione degli AWS Service Catalog artefatti di determinare se le Service Actions sono associate a un artifact di provisioning e di garantire che l'artifact di provisioning non venga eliminato se è associata un'azione di servizio.
- `servicecatalog:DescribeProvisioningArtifact`— Consente al ruolo di sincronizzazione degli AWS Service Catalog artefatti di recuperare i dettagli dall'`DescribeProvisioningArtifactAPI`, incluso l'ID di commit, fornito nell'output. `SourceRevisionInfo`
- `servicecatalog>CreateProvisioningArtifact`— Consente al ruolo di sincronizzazione degli AWS Service Catalog artefatti di creare un nuovo artefatto assegnato se viene rilevata una modifica (ad esempio, viene eseguito il commit di un git-push) al file del modello di origine nel repository esterno.
- `servicecatalog:UpdateProvisioningArtifact`— Consente al ruolo di sincronizzazione degli AWS Service Catalog artefatti di aggiornare l'artefatto fornito per un prodotto connesso o sincronizzato.
- `codeconnections:UseConnection`— Consente al ruolo di sincronizzazione degli AWS Service Catalog artefatti di utilizzare la connessione esistente per aggiornare e sincronizzare un prodotto.
- `cloudformation:ValidateTemplate`— Consente al ruolo di AWS Service Catalog artifact sync (accesso limitato) di AWS CloudFormation convalidare il formato del modello utilizzato nel repository esterno e verificare se è in grado di supportare il modello. CloudFormation

AWS politica gestita: **AWSServiceCatalogOrgsDataSyncServiceRolePolicy**

AWS Service Catalog allega questa politica al ruolo `AWSServiceRoleForServiceCatalogOrgsDataSync` collegato al servizio (SLR), consentendone AWS Service Catalog la sincronizzazione con. AWS Organizations

Questa politica concede autorizzazioni che consentono un accesso limitato alle AWS Service Catalog azioni (ad esempio, chiamate API) e ad altre AWS azioni di servizio da cui dipende. AWS Service Catalog

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `organizations`— Consente al ruolo di sincronizzazione AWS Service Catalog dei dati l'accesso limitato al AWS Organizations pubblico. APIs

Visualizza la politica: [AWSServiceCatalogOrgsDataSyncServiceRolePolicy](#).

Dettagli del ruolo collegato al servizio

AWS Service Catalog utilizza i dettagli di autorizzazione di cui sopra per il ruolo `AWSServiceRoleForServiceCatalogOrgsDataSync` collegato al servizio che viene creato quando un utente abilita l'accesso AWS Organizations condiviso al portafoglio o crea una condivisione di portafoglio. È possibile modificare questa politica utilizzando la AWS CLI, l' AWS API o tramite la AWS Service Catalog console. Per ulteriori informazioni su come creare, modificare ed eliminare i ruoli collegati ai servizi, consulta [Using service-linked roles \(\) for SLRs AWS Service Catalog](#)

Le autorizzazioni incluse nel ruolo `AWSServiceRoleForServiceCatalogOrgsDataSync` collegato al servizio consentono di eseguire le seguenti azioni AWS Service Catalog per conto del cliente.

- `organizations:DescribeAccount`— Consente al ruolo AWS Service Catalog Organizations Data Sync AWS Organizations di recuperare informazioni relative all'account specificato.
- `organizations:DescribeOrganization`— Consente al ruolo AWS Service Catalog Organizations Data Sync di recuperare informazioni sull'organizzazione a cui appartiene l'account dell'utente.

- `organizations:ListAccounts`— Consente al ruolo AWS Service Catalog Organizations Data Sync di elencare gli account nell'organizzazione dell'utente.
- `organizations:ListChildren`— Consente al ruolo AWS Service Catalog Organizations Data Sync di elencare tutte le unità organizzative (UOs) o gli account contenuti nell'unità organizzativa principale o principale specificata.
- `organizations:ListParents`— Consente al ruolo AWS Service Catalog Organizations Data Sync di elencare la radice o OUs quella che funge da genitore diretto dell'unità organizzativa o dell'account figlio specificato.
- `organizations:ListAWSServiceAccessForOrganization`— Consente al ruolo AWS Service Catalog Organizations Data Sync di recuperare un elenco dei AWS servizi che l'utente ha abilitato a integrare con la propria organizzazione.

Politiche obsolete

Di seguito sono elencate le policy gestite obsolete:

- `ServiceCatalogAdminFullAccess`— Usa invece. `AWSServiceCatalogAdminFullAccess`
- `ServiceCatalogAdminReadOnlyAccess`— Usa `AWSServiceCatalogAdminReadOnlyAccess` invece.
- `ServiceCatalogEndUserFullAccess`— Usa `AWSServiceCatalogEndUserFullAccess` invece.
- `ServiceCatalogEndUserAccess`— Usa `AWSServiceCatalogEndUserReadOnlyAccess` invece.

Utilizza la procedura seguente per accertarti che agli amministratori e agli utenti finali siano concesse le autorizzazioni mediante le policy correnti.

Per migrare dalle policy obsolete alle policy attuali, consulta [Aggiungere e rimuovere le autorizzazioni di identità IAM](#) nella Guida per l'utente AWS Identity and Access Management

AppRegistry aggiornamenti alle politiche gestite AWS

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite AppRegistry da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei AppRegistry documenti.

| Modifica | Descrizione | Data |
|--|---|----------------|
| AWSServiceCatalogSyncServiceRolePolicy — Aggiorna la politica gestita | AWS Service Catalog ha aggiornato la <code>AWSServiceCatalogSyncServiceRolePolicy</code> politica per <code>codestar-connections</code> modificarla <code>connections</code> . | 7 maggio 2024 |
| AWSServiceCatalogAdminFullAccess — Aggiorna la politica gestita | AWS Service Catalog ha aggiornato la <code>AWSServiceCatalogAdminFullAccess</code> politica per includere le autorizzazioni necessarie all' AWS Service Catalog amministratore per creare il ruolo <code>AWSServiceRoleForServiceCatalogOrgsDataSync</code> collegato al servizio (SLR) nel proprio account. | 14 aprile 2023 |
| AWSServiceCatalogOrgsDataSyncServiceRolePolicy — Nuova politica gestita | AWS Service Catalog ha aggiunto il <code>AWSServiceCatalogOrgsDataSyncServiceRolePolicy</code> , che è collegato al ruolo <code>AWSServiceRoleForServiceCatalogOrgsDataSync</code> collegato al servizio (SLR), che consente la sincronizzazione AWS Service Catalog con. AWS Organizations Questa politica consente un accesso limitato alle AWS Service Catalog | 14 aprile 2023 |

| Modifica | Descrizione | Data |
|---|---|------------------|
| | azioni (ad esempio, chiamate API) e ad altre azioni di AWS servizio da cui AWS Service Catalog dipende. | |
| AWSServiceCatalogAdminFullAccess — Aggiorna la politica gestita | AWS Service Catalog ha aggiornato la <code>AWSServiceCatalogAdminFullAccess</code> politica per includere tutte le autorizzazioni per l'AWS Service Catalog amministratore e creare compatibilità con AppRegistry. | 12 gennaio 2023 |
| AWSServiceCatalogSyncServiceRolePolicy — Nuova politica gestita | AWS Service Catalog ha aggiunto la <code>AWSServiceCatalogSyncServiceRolePolicy</code> policy, che è allegata al ruolo <code>AWSServiceRoleForServiceCatalogSync</code> collegato al servizio (SLR). Questa politica consente di AWS Service Catalog sincronizzare i modelli in un archivio esterno con i prodotti. AWS Service Catalog | 18 novembre 2022 |

| Modifica | Descrizione | Data |
|---|--|------------------|
| AWSServiceRoleForServiceCatalogSync — Nuovo ruolo collegato al servizio | AWS Service Catalog ha aggiunto il ruolo <code>AWSServiceRoleForServiceCatalogSync</code> collegato al servizio (SLR). Questo ruolo è necessario per AWS Service Catalog utilizzare <code>CodeConnections</code> e creare, aggiornare e descrivere AWS Service Catalog Provisioning Artifacts per un prodotto. | 18 novembre 2022 |

| Modifica | Descrizione | Data |
|--|---|--------------------------|
| <p>AWSServiceCatalogAdminFullAccess— Politica gestita aggiornata</p> | <p>AWS Service Catalog ha aggiornato la <code>AWSServiceCatalogAdminFullAccess</code> politica per includere tutte le autorizzazioni richieste per un AWS Service Catalog amministratore. La politica identifica le azioni specifiche che l'amministratore può intraprendere su tutte AWS Service Catalog le risorse, come creare, descrivere, eliminare e altro. Inoltre, la politica è stata modificata per supportare una funzionalità lanciata di recente, Attribute Based Access Control (ABAC) for AWS Service Catalog. ABAC consente di utilizzare la <code>AWSServiceCatalogAdminFullAccess</code> politica come modello per consentire o negare azioni sulle AWS Service Catalog risorse basate sui tag. Per ulteriori informazioni su ABAC, consulta A cosa serve ABAC in <code>AWS Identity and Access Management</code></p> | <p>30 settembre 2022</p> |
| <p>AppRegistry ha iniziato a tenere traccia delle modifiche</p> | <p>AppRegistry ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.</p> | <p>15 settembre 2022</p> |

Utilizzo di ruoli collegati ai servizi per AWS Service Catalog

AWS Service Catalog utilizza ruoli collegati ai [servizi AWS Identity and Access Management](#) (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. AWS Service Catalog I ruoli collegati ai servizi sono predefiniti AWS Service Catalog e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato al servizio semplifica la configurazione AWS Service Catalog perché non è necessario aggiungere manualmente le autorizzazioni necessarie. AWS Service Catalog definisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli. AWS Service Catalog Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato al servizio solo dopo avere eliminato le risorse correlate. In questo modo proteggi AWS Service Catalog le tue risorse perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta [AWS Servizi compatibili con IAM](#) e cerca i servizi con Sì nella colonna Ruoli collegati ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni del ruolo collegato ai servizi per **AWSServiceRoleForServiceCatalogSync**

AWS Service Catalog può utilizzare il ruolo collegato al servizio denominato **AWSServiceRoleForServiceCatalogSync**: questo ruolo collegato al servizio è necessario per utilizzare CodeConnections e creare, aggiornare e AWS Service Catalog descrivere gli artefatti di provisioning per un prodotto. AWS Service Catalog

Ai fini dell'assunzione del ruolo, il ruolo collegato al servizio

AWSServiceRoleForServiceCatalogSync considera attendibili i seguenti servizi:

- `sync.servicecatalog.amazonaws.com`

La politica di autorizzazione dei ruoli denominata

AWSServiceCatalogSyncServiceRolePolicy consente di completare le seguenti azioni sulle AWS Service Catalog risorse specificate:

- Operazione: `Connection` su `CodeConnections`
- Azione: `Create`, `Update`, and `Describe` attiva `ProvisioningArtifact` per un prodotto AWS Service Catalog

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio è necessario configurare le relative autorizzazioni. Per ulteriori informazioni, consulta [Autorizzazioni del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Creazione del ruolo collegato ai servizi **`AWSServiceRoleForServiceCatalogSync`**

Non è necessario creare manualmente il ruolo `AWSServiceRoleForServiceCatalogSync` collegato al servizio. AWS Service Catalog crea automaticamente il ruolo collegato al servizio quando lo stabilisci `CodeConnections` nell' Console di gestione AWS API AWS CLI. AWS

Important

Questo ruolo collegato al servizio può apparire nell'account, se è stata completata un'operazione in un altro servizio che utilizza le caratteristiche supportate da questo ruolo. Inoltre, se utilizzavi il AWS Service Catalog servizio prima del 18 novembre 2022, quando ha iniziato a supportare i ruoli collegati al servizio, hai AWS Service Catalog creato il `AWSServiceRoleForServiceCatalogSync` ruolo nel tuo account. Per ulteriori informazioni, consulta [Un nuovo ruolo è apparso nel mio account IAM](#).

Se elimini questo ruolo collegato al servizio, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Una volta stabilito `CodeConnections`, AWS Service Catalog crea nuovamente il ruolo collegato al servizio per te.

Puoi anche utilizzare la console IAM per creare un ruolo collegato al servizio con lo use case sincronizzato AWS Service Catalog Products. Nella AWS CLI o nell' AWS API, crea un ruolo collegato al servizio con il nome del servizio. `sync.servicecatalog.amazonaws.com` Per ulteriori informazioni, consulta [Creazione di un ruolo collegato ai servizi](#) nella Guida per l'utente IAM. Se elimini il ruolo collegato ai servizi, è possibile utilizzare lo stesso processo per crearlo nuovamente.

Autorizzazioni del ruolo collegato ai servizi per **AWSServiceRoleForServiceCatalogOrgsDataSync**

AWS Service Catalog può utilizzare il ruolo collegato al servizio denominato **AWSServiceRoleForServiceCatalogOrgsDataSync**: questo ruolo collegato al servizio è necessario per consentire alle AWS Service Catalog organizzazioni di rimanere sincronizzate con AWS Organizations

Ai fini dell'assunzione del ruolo, il ruolo collegato al servizio **AWSServiceRoleForServiceCatalogOrgsDataSync** considera attendibili i seguenti servizi:

- `orgsdatasync.servicecatalog.amazonaws.com`

[Il ruolo **AWSServiceRoleForServiceCatalogOrgsDataSync** collegato al servizio richiede l'utilizzo della seguente politica di attendibilità oltre alla politica gestita: **AWSServiceCatalogOrgsDataSyncServiceRolePolicy**](#)

JSON

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

La politica di autorizzazione dei ruoli denominata **AWSServiceCatalogOrgsDataSyncServiceRolePolicy** consente di AWS Service Catalog completare le seguenti azioni sulle risorse specificate:

- Azione: `DescribeAccount`, `DescribeOrganization` e `ListAWSServiceAccessForOrganization` su `Organizations` accounts
- Azione: `ListAccounts`, `ListChildren` e `ListParent` su `Organizations` accounts

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio è necessario configurare le relative autorizzazioni. Per ulteriori informazioni, consulta [Autorizzazioni del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Creazione del ruolo collegato ai servizi **AWSServiceRoleForServiceCatalogOrgsDataSync**

Non è necessario creare manualmente il ruolo collegato al `AWSServiceRoleForServiceCatalogOrgsDataSync` servizio. AWS Service Catalog considera la vostra azione di attivazione [Condivisione con AWS Organizations](#) o [Condivisione di un portafoglio](#) autorizzazione AWS Service Catalog alla creazione di una reflex in background per vostro conto.

AWS Service Catalog crea automaticamente il ruolo collegato al servizio quando lo richiedi `EnableAWSOrganizationsAccess` o `CreatePortfolioShare` nella Console di gestione AWS, la o l' AWS CLI API. AWS

Important

Questo ruolo collegato ai servizi può apparire nell'account se è stata completata un'operazione in un altro servizio che utilizza le funzionalità supportate dal ruolo. Per ulteriori informazioni, consulta [Un nuovo ruolo è apparso nel mio account IAM](#).

Se elimini questo ruolo collegato al servizio, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando richiedi `EnableAWSOrganizationsAccess` o `CreatePortfolioShare`, AWS Service Catalog crea nuovamente il ruolo collegato al servizio per te.

Modifica di un ruolo collegato al servizio per AWS Service Catalog

AWS Service Catalog non consente di modificare i ruoli `AWSServiceRoleForServiceCatalogSync` o i ruoli collegati al `AWSServiceRoleForServiceCatalogOrgsDataSync` servizio. Dopo avere creato un ruolo collegato al servizio, non sarà possibile modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato al servizio](#) nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per AWS Service Catalog

Puoi utilizzare la console IAM, la AWS CLI o l' AWS API per eliminare manualmente la `AWSServiceRoleForServiceCatalogSync` o `AWSServiceRoleForServiceCatalogOrgsDataSync` la SLR. Per fare ciò, devi prima rimuovere manualmente tutte le risorse che utilizzano il ruolo collegato al servizio (ad esempio, tutti AWS Service Catalog i prodotti sincronizzati con un repository esterno), quindi il ruolo collegato al servizio può essere eliminato manualmente.

AWS Service Catalog Aree supportate per i ruoli collegati ai servizi

AWS Service Catalog supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta [Regioni ed endpoint di AWS](#).

| Nome della Regione | Identità della Regione | Support in AWS Service Catalog |
|---|------------------------|--------------------------------|
| Stati Uniti orientali (Virginia settentrionale) | us-east-1 | Sì |
| Stati Uniti orientali (Ohio) | us-east-2 | Sì |
| Stati Uniti occidentali (California settentrionale) | us-west-1 | Sì |
| Stati Uniti occidentali (Oregon) | us-west-2 | Sì |
| Africa (Città del Capo) | af-south-1 | Sì |
| Asia Pacific (Hong Kong) | ap-east-1 | Sì |
| Asia Pacifico (Giacarta) | ap-southeast-3 | Sì |
| Asia Pacifico (Mumbai) | ap-south-1 | Sì |
| Asia Pacifico (Osaka) | ap-northeast-3 | Sì |
| Asia Pacifico (Seoul) | ap-northeast-2 | Sì |
| Asia Pacifico (Singapore) | ap-southeast-1 | Sì |

| Nome della Regione | Identità della Regione | Support in AWS Service Catalog |
|--|------------------------|--------------------------------|
| Asia Pacifico (Sydney) | ap-southeast-2 | Sì |
| Asia Pacifico (Tokyo) | ap-northeast-1 | Sì |
| Canada (Centrale) | ca-central-1 | Sì |
| Europa (Francoforte) | eu-central-1 | Sì |
| Europa (Irlanda) | eu-west-1 | Sì |
| Europa (Londra) | eu-west-2 | Sì |
| Europa (Milan) | eu-south-1 | Sì |
| Europa (Parigi) | eu-west-3 | Sì |
| Europa (Stoccolma) | eu-north-1 | Sì |
| Medio Oriente (Bahrein) | me-south-1 | Sì |
| Sud America (San Paolo) | sa-east-1 | Sì |
| AWS GovCloud (Stati Uniti orientali) | us-gov-east-1 | No |
| AWS GovCloud (Stati Uniti occidentali) | us-gov-west-1 | No |

Risoluzione dei problemi di AWS Service Catalog identità e accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con AWS Service Catalog un IAM.

Argomenti

- [Non sono autorizzato a eseguire alcuna azione in AWS Service Catalog](#)
- [Non sono autorizzato a eseguire iam:PassRole](#)
- [Voglio consentire a persone esterne al mio AWS account di accedere alle mie AWS Service Catalog risorse](#)

Non sono autorizzato a eseguire alcuna azione in AWS Service Catalog

Se ti Console di gestione AWS dice che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è colui che ti ha fornito le credenziali di accesso. L'errore di esempio seguente si verifica quando l'utente mateojackson tenta di utilizzare la console per visualizzare i dettagli su una my-example-widget risorsa fittizia ma non dispone delle autorizzazioni fittizie. `aws:GetWidget`

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

In questo caso, Mateo chiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa my-example-widget mediante l'operazione `aws:GetWidget`.

Non sono autorizzato a eseguire **iam:PassRole**

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, devi contattare il tuo amministratore per ricevere assistenza. L'amministratore è la persona da cui si sono ricevuti il nome utente e la password. Richiedi a tale persona di aggiornare le tue policy per poter passare un ruolo a AWS Service Catalog.

Alcuni AWS servizi consentono di passare un ruolo esistente a quel servizio, anziché creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente di nome marymajor tenta di utilizzare la console per eseguire un'azione in AWS Service Catalog. Tuttavia, l'operazione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere il ruolo al servizio.

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

In questo caso, Mary chiede al suo amministratore di aggiornare le sue politiche per consentirle di eseguire l'azione `iam:PassRole`.

Voglio consentire a persone esterne al mio AWS account di accedere alle mie AWS Service Catalog risorse

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per concedere alle persone l'accesso alle tue risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- [Per sapere se AWS Service Catalog supporta queste funzionalità, consulta AWS Identity and Access Management la Guida per l' AWS Service CatalogAWS Service Catalog amministratore.](#)
- Per scoprire come fornire l'accesso alle tue risorse su tutti AWS gli account di tua proprietà, consulta [Fornire l'accesso a un utente IAM in un altro AWS account di tua proprietà](#) nella Guida per l'utente IAM.
- Per scoprire come fornire l'accesso alle tue risorse ad AWS account di terze parti, consulta [Fornire l'accesso agli AWS account di proprietà di terze parti](#) nella IAM User Guide.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso a utenti autenticati esternamente \(Federazione delle identità\)](#) nella Guida per l'utente IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consulta [Differenza tra i ruoli IAM e le policy basate su risorse](#) nella Guida per l'utente IAM.

Controllo dell'accesso

un AWS Service Catalog portfolio offre agli amministratori un livello di controllo degli accessi per i gruppi di utenti finali. Gli utenti aggiunti a un portafoglio possono sfogliare e avviare tutti i prodotti. Per ulteriori informazioni, consulta [the section called "Gestione di portafogli"](#).

Vincoli

I vincoli controllano quali regole vengono applicate agli utenti finali quando si avvia un prodotto da un portafoglio specifico. Puoi utilizzarli per applicare vincoli ai prodotti allo scopo di controllare governance o costi. Per ulteriori informazioni sui vincoli, consulta [the section called "Utilizzo di vincoli"](#).

AWS Service Catalog i vincoli di avvio offrono un maggiore controllo sulle autorizzazioni necessarie a un utente finale. Quando l'amministratore crea un vincolo di avvio per un prodotto in un portafoglio, il vincolo di avvio associa un ARN di ruolo utilizzato quando gli utenti finali avviano il prodotto dal portafoglio. Utilizzando questo modello, è possibile controllare l'accesso alla AWS creazione di risorse. Per ulteriori informazioni, consulta [the section called “Vincoli di avvio di”](#).

Registrazione e monitoraggio AWS Service Catalog

AWS Service Catalog si integra con AWS CloudTrail, un servizio che acquisisce tutte le chiamate AWS Service Catalog API e consegna i file di log a un bucket Amazon S3 specificato dall'utente. Per ulteriori informazioni, consulta [AWS Service Catalog Registrazione](#) delle chiamate API con CloudTrail

Puoi anche utilizzare i vincoli di notifica per configurare le notifiche di Amazon SNS sugli eventi dello stack. Per ulteriori informazioni, consulta [the section called “Vincoli di notifica di”](#).

Convalida della conformità per AWS Service Catalog

I revisori esterni valutano la sicurezza e la conformità nell' AWS Service Catalog ambito di diversi programmi di AWS conformità, tra cui:

- 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)

Per un elenco di AWS servizi nell'ambito di programmi di conformità specifici, consulta [AWS Services in Scope by Compliance Program](#). Per informazioni generali, consulta Programmi di [AWS conformità Programmi di AWS garanzia Programmi](#) .

Puoi scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta [Downloading Reports in AWS Artifact](#).

La responsabilità di conformità dell'utente durante l'utilizzo AWS Service Catalog dipende dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce queste risorse per contribuire alla conformità:

- Guide [introduttive su sicurezza e conformità](#): queste guide all'implementazione illustrano le considerazioni relative all'architettura e forniscono i passaggi per implementare ambienti di base incentrati sulla sicurezza e la conformità. AWS
- [Whitepaper sull'architettura per la sicurezza e la conformità HIPAA](#): questo white paper descrive in che modo le aziende possono utilizzare per creare applicazioni conformi allo standard HIPAA. AWS
- [AWS Risorse per la conformità](#): questa raccolta di cartelle di lavoro e guide può essere applicata al tuo settore e alla tua area geografica.
- [AWS Config](#)— Questo AWS servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- [AWS Security Hub CSPM](#)— Questo AWS servizio offre una visione completa dello stato di sicurezza dell'utente e consente AWS di verificare la conformità agli standard e alle best practice del settore della sicurezza.

Resilienza in AWS Service Catalog

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture tradizionali a data center singolo o multiplo.

[Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta Global Infrastructure.AWS](#)

Oltre all'infrastruttura AWS globale, AWS Service Catalog offre azioni AWS Service Catalog self-service. Con le operazioni di self-service, i clienti possono ridurre la manutenzione amministrativa e la formazione degli utenti finali, rispettando le misure di conformità e sicurezza. Con le operazioni di self-service, come amministratore puoi consentire agli utenti finali di eseguire le attività operative, come backup e ripristino, risolvere i problemi, eseguire comandi approvati e richiedere le autorizzazioni in AWS Service Catalog. Per ulteriori informazioni, consulta [the section called "Utilizzo delle operazioni di servizio"](#).

Sicurezza dell'infrastruttura in AWS Service Catalog

In quanto servizio gestito, AWS Service Catalog è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta [AWS Cloud Security](#). Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Utilizzate chiamate API AWS pubblicate per accedere AWS Service Catalog attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Con AWS Service Catalog, puoi controllare le regioni in cui sono archiviati i dati. I portafogli e i prodotti sono disponibili solo nelle regioni in cui li hai resi disponibili. È possibile utilizzare l'API `CopyProduct` per copiare un prodotto in un'altra regione.

Migliori pratiche di sicurezza per AWS Service Catalog

AWS Service Catalog fornisce una serie di funzionalità di sicurezza da considerare durante lo sviluppo e l'implementazione delle proprie politiche di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste best practice potrebbero non essere appropriate o sufficienti per l'ambiente, sono da considerare come considerazioni utili anziché prescrizioni.

Puoi definire regole che limitano i valori dei parametri che un utente immette quando lancia un prodotto. Tali regole sono dette vincoli di modello, perché pongono dei limiti sul modo in cui viene distribuito il modello CloudFormation del prodotto in questione. Devi utilizzare un semplice editor per creare i vincoli di modello, poi applicarli ai singoli prodotti.

AWS Service Catalog applica dei vincoli quando fornisce un nuovo prodotto o aggiorna un prodotto già in uso. Viene sempre applicato il vincolo più restrittivo fra tutti quelli applicati al portafoglio e al prodotto. Ad esempio, considera uno scenario in cui il prodotto consente il lancio di tutte le istanze Amazon EC2 e il portafoglio presenta due vincoli: uno che consente il lancio di tutte le istanze EC2 di tipo non GPU e uno che consente il lancio solo di istanze EC2 t1.micro e m1.small. Per questo esempio, applica il secondo vincolo più restrittivo (t1.micro e m1.small). AWS Service Catalog

Puoi limitare l'accesso degli utenti finali alle AWS risorse quando colleghi una policy IAM a un ruolo di lancio. È quindi necessario AWS Service Catalog creare un vincolo di lancio per utilizzare il ruolo all'avvio del prodotto.

[Per ulteriori informazioni sulle politiche gestite per AWS Service Catalog, consulta AWS Managed Policies for. AWS Service Catalog](#)

Gestione di cataloghi

AWS Service Catalog fornisce un'interfaccia per la gestione di portafogli, prodotti e vincoli da una console di amministrazione.

Note

Per eseguire qualsiasi operazione in questa sezione, devi disporre di autorizzazioni di amministratore per AWS Service Catalog. Per ulteriori informazioni, consulta [Identity and Access Management in AWS Service Catalog](#).

Processi

- [Gestione di portafogli](#)
- [Gestione di prodotti](#)
- [Utilizzo dei AWS Service Catalog vincoli](#)
- [AWS Service Catalog Azioni di servizio](#)
- [Aggiungere Marketplace AWS prodotti al tuo portafoglio](#)
- [Usando CloudFormation StackSets](#)
- [Gestione dei budget](#)

Gestione di portafogli

Puoi creare, visualizzare e aggiornare i portafogli nella pagina Portfolio della console dell'amministratore. AWS Service Catalog

Processi

- [Creazione, visualizzazione ed eliminazione di portafogli](#)
- [Visualizzazione dei dettagli di un portafoglio](#)
- [Creazione ed eliminazione di portafogli](#)
- [Aggiungere prodotti](#)
- [Aggiunta di vincoli](#)
- [Concessione dell'accesso agli utenti](#)
- [Condivisione di un portafoglio](#)

- [Condivisione e importazione di portafogli](#)

Creazione, visualizzazione ed eliminazione di portafogli

La pagina Portafogli mostra un elenco dei portafogli che hai creato nella regione corrente. Utilizza questa pagina per creare nuovi portafogli, visualizzare i dettagli di un portafoglio o eliminare portafogli dal tuo account.

Per visualizzare la pagina Portfolio

1. Aprire la console Service Catalog all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Seleziona un'altra regione come necessario.
3. Se sei nuovo AWS Service Catalog, vedrai la pagina iniziale. AWS Service Catalog Selezionare Get started (Nozioni di base) per creare un portafoglio. Segui le istruzioni per creare il tuo primo portfolio, quindi procedi alla pagina Portfolio.

Durante l'utilizzo AWS Service Catalog, puoi tornare alla pagina Portfolio in qualsiasi momento; scegli Service Catalog nella barra di navigazione, quindi scegli Portfolios.

Visualizzazione dei dettagli di un portafoglio

Nella console dell' AWS Service Catalog amministratore, la pagina dei dettagli del portafoglio elenca le impostazioni per un portafoglio. Utilizzate questa pagina per gestire i prodotti del portafoglio, concedere agli utenti l'accesso ai prodotti TagOptions e applicare eventuali vincoli.

Visualizzazione della pagina Portfolio details (Dettagli portafoglio)

1. Aprire la console Service Catalog all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Scegli il portafoglio che intendi gestire.

Creazione ed eliminazione di portafogli

Utilizza la pagina Portafogli per creare ed eliminare portafogli.

Creazione di un nuovo portafoglio

1. Dal menu di navigazione a sinistra, scegli Portfolio.

2. Scegli Crea portfolio.
3. Nella pagina Crea portfolio, inserisci le informazioni richieste.
4. Scegli Crea. AWS Service Catalog crea il portfolio e visualizza i dettagli del portfolio.

Come eliminare un portafoglio

Note

È possibile eliminare solo i portafogli locali. È possibile rimuovere i portafogli importati (condivisi), ma non è possibile eliminare i portafogli importati.

Prima di poter eliminare un portfolio, è necessario rimuoverne tutti i prodotti, i vincoli, i gruppi, i ruoli, gli utenti, le azioni e. TagOptions A tale scopo, apri un portfolio per visualizzare i dettagli del portfolio. Quindi scegli una scheda per rimuoverli.

Note

Per evitare errori, rimuovi i vincoli dal portafoglio prima di rimuovere qualsiasi prodotto.

1. Dal menu di navigazione a sinistra, scegli Portfolio.
2. Seleziona il portfolio che desideri eliminare.
3. Scegli Elimina. Puoi eliminare solo i portafogli locali. Se state tentando di eliminare un portfolio importato (condiviso), il menu Azioni non è disponibile.
4. Nella finestra di conferma scegli Delete (Elimina).

Aggiungere prodotti

Puoi aggiungere prodotti a un portafoglio caricando un nuovo prodotto direttamente in un portafoglio esistente o associando un prodotto esistente dal tuo catalogo al portafoglio.

Note

Quando crei un AWS Service Catalog prodotto, puoi caricare un CloudFormation modello o un file di configurazione Terraform. Il CloudFormation modello è archiviato in un bucket

Amazon Simple Storage Service (Amazon S3) e il nome del bucket inizia con "cf-templates-». È inoltre necessario disporre dell'autorizzazione per recuperare oggetti da bucket aggiuntivi durante il provisioning di un prodotto. [Per ulteriori informazioni, consulta Creazione di prodotti.](#)

Aggiungere un nuovo prodotto

Puoi aggiungere nuovi prodotti direttamente dalla pagina dei dettagli del portafoglio. Quando crei un prodotto da questa pagina, lo AWS Service Catalog aggiunge al portafoglio attualmente selezionato.

Per aggiungere un nuovo prodotto

1. Vai alla pagina Portafogli, quindi scegli il nome del portafoglio a cui desideri aggiungere il prodotto.
2. Nella pagina dei dettagli del portfolio, espandi la sezione Prodotti, quindi scegli Carica nuovo prodotto.
3. Per Enter product details (Immetti dettagli versione), immetti quanto segue:
 - Product name (Nome prodotto) – Il nome del prodotto.
 - Descrizione del prodotto (opzionale): la descrizione del prodotto. Questa descrizione viene mostrata nell'elenco dei prodotti per aiutarti a scegliere il prodotto corretto.
 - Descrizione: la descrizione completa. Questa descrizione viene mostrata nell'elenco dei prodotti per aiutarti a scegliere il prodotto corretto.
 - Proprietario o distributore: il nome o l'indirizzo e-mail del proprietario. Le informazioni di contatto del distributore sono facoltative.
 - Fornitore (opzionale): il nome dell'editore dell'applicazione. Questo campo consente di ordinare l'elenco dei prodotti per facilitarne la ricerca.
4. Nella pagina Version details (Dettagli versione)immettere quanto segue:
 - Scegli il modello: per CloudFormation i prodotti, scegli il tuo file modello, un CloudFormation modello da un'unità locale o un URL che rimanda a un modello archiviato in Amazon S3, un modello CloudFormation Stack ARN esistente o un file modello archiviato in un repository esterno.

Per i prodotti Teraform, scegli il tuo file modello, un file di configurazione tar.gz da un'unità locale o un URL che punti a un modello archiviato in Amazon S3 o un file di configurazione tar.gz archiviato in un repository esterno.

- Nome della versione (opzionale): il nome della versione del prodotto (ad esempio, «v1», «v2beta»). Gli spazi non sono consentiti.
 - Description (Descrizione) (facoltativa) – Una descrizione della versione del prodotto, incluse le differenze rispetto alla versione precedente.
5. Per Enter support details (Immetti dettagli supporto) immetti quanto segue:
- Email contact (E-mail di contatto) (facoltativo) – L'indirizzo e-mail a cui segnalare i problemi relativi al prodotto.
 - Link di supporto (opzionale): un URL a un sito in cui gli utenti possono trovare informazioni di supporto o ticket di file. L'URL deve iniziare con `http://` o `https://`. Gli amministratori sono responsabili del mantenimento dell'accuratezza e dell'accesso alle informazioni di supporto.
 - Descrizione dell'assistenza (opzionale): una descrizione di come utilizzare il collegamento Email contact and Support.
6. Scegli Crea prodotto.

Aggiungere un prodotto esistente

Puoi aggiungere prodotti esistenti a un portafoglio da tre posizioni: elenco dei portafogli, pagina dei dettagli del portafoglio o pagina dell'elenco dei prodotti.

Per aggiungere un prodotto esistente a un portafoglio

1. Vai alla pagina Portafogli.
2. Scegli un portfolio. Quindi scegli Azioni - Aggiungi prodotto al portafoglio.
3. Scegli un prodotto, quindi scegli Aggiungi prodotto al portafoglio.

Rimuovere un prodotto da un portafoglio

Quando non desideri più utilizzare un prodotto, rimuovilo da un portafoglio. Il prodotto è ancora disponibile nel tuo catalogo dalla pagina Prodotti e puoi comunque aggiungerlo ad altri portafogli. Puoi rimuovere molteplici prodotti da un portafoglio simultaneamente.

Rimozione di un prodotto da un portafoglio

1. Vai alla pagina Portafogli, quindi scegli il portafoglio che contiene il prodotto. Si apre la pagina dei dettagli del portfolio.
2. Espandi la sezione Prodotti.
3. Scegli uno o più prodotti, quindi scegli Rimuovi.
4. Conferma la tua scelta.

Aggiunta di vincoli

È necessario aggiungere dei vincoli per controllare il modo in cui gli utenti interagiscono con i prodotti. Per ulteriori informazioni sui tipi di vincoli supportati AWS Service Catalog , consulta [Utilizzo dei AWS Service Catalog vincoli](#)

I vincoli devono essere aggiunti ai prodotti dopo essere stati inclusi in un portafoglio.

Aggiunta di un vincolo a un prodotto

1. Aprire la console Service Catalog all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Scegli Portfolios e seleziona un portfolio.
3. Nella pagina dei dettagli del portfolio, espandi la sezione Crea vincolo e scegli Aggiungi vincoli.
4. Per Prodotto, selezionate il prodotto a cui applicare il vincolo.
5. Per Tipo di vincolo, scegliete una delle seguenti opzioni:

Launch: consente di assegnare un ruolo IAM al prodotto utilizzato per fornire le risorse. AWS Per ulteriori informazioni, consulta [AWS Service Catalog Vincoli di avvio](#).

Notifica: consente di trasmettere in streaming le notifiche dei prodotti su un argomento di Amazon SNS. Per ulteriori informazioni, consulta [AWS Service Catalog Vincoli di notifica](#).

Modello: consente di limitare le opzioni disponibili per gli utenti finali al momento del lancio del prodotto. Un modello è costituito da un file di testo in formato JSON che contiene una o più regole. Le regole vengono aggiunte al CloudFormation modello utilizzato dal prodotto. Per ulteriori informazioni, consulta [Regole di vincolo di modello](#).

Stack Set: consente di configurare la distribuzione del prodotto tra account e regioni utilizzando CloudFormation StackSets. Per ulteriori informazioni, consulta [AWS Service Catalog Vincoli Stack Set](#).

Aggiornamento dei tag: consente di aggiornare i tag dopo che il prodotto è stato fornito. Per ulteriori informazioni, consulta [AWS Service Catalog Tag Update Constraints](#).

6. Scegli Continua e inserisci le informazioni richieste.

Modifica di un vincolo

1. Accedi a Console di gestione AWS e apri la console dell' AWS Service Catalog amministratore all'indirizzo <https://console.aws.amazon.com/catalog/>.
2. Scegli Portafogli e seleziona un portfolio.
3. Nella pagina dei dettagli del portfolio, espandi la sezione Crea vincolo e seleziona il vincolo da modificare.
4. Scegliete Modifica vincoli.
5. Modificate il vincolo secondo necessità e scegliete Salva.

Concessione dell'accesso agli utenti

Offri agli utenti l'accesso ai portafogli tramite gruppi o ruoli. Il modo migliore per fornire l'accesso al portafoglio a molti utenti è inserire gli utenti in un gruppo IAM e concedere l'accesso a quel gruppo. In tal modo, è possibile semplicemente aggiungere e rimuovere utenti dal gruppo per gestire l'accesso al portafoglio. Per ulteriori informazioni, consulta [Utenti e gruppi IAM](#) nella IAM User Guide.

Oltre all'accesso a un portafoglio, gli utenti devono avere accesso anche alla console dell'utente AWS Service Catalog finale. Concedi l'accesso alla console applicando le autorizzazioni in IAM. Per ulteriori informazioni, consulta [Identity and Access Management in AWS Service Catalog](#).

Se desideri condividere un portafoglio e i relativi Principal con altri account, puoi associare i nomi principali (gruppi, ruoli o utenti) al portafoglio. I nomi principali sono condivisi con il portafoglio e utilizzati negli account dei destinatari per concedere l'accesso agli utenti finali.

Concessione dell'accesso a un portafoglio a utenti o gruppi

1. Aprire la console Service Catalog all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Dal riquadro di navigazione, scegli Amministrazione, quindi scegli Portafogli.
3. Scegli un portfolio a cui desideri concedere l'accesso a gruppi, ruoli o utenti. AWS Service Catalog accede alla pagina dei dettagli del portfolio.
4. Nella pagina dei dettagli del portfolio, scegli la scheda Accesso.

5. In Accesso al portfolio, scegli Concedi l'accesso.
6. Per Tipo, scegli Nome principale, quindi seleziona il gruppo/, role/ o user/, Type. Puoi aggiungere fino a 9 nomi principali.
7. Scegli Grant Access per associare il principale al portafoglio corrente.

Rimozione dell'accesso a un portafoglio

1. Nella pagina dei dettagli del portfolio, scegli un gruppo, un ruolo o un nome utente.
2. Scegli Rimuovi accesso.

Condivisione di un portafoglio

Per consentire a un AWS Service Catalog amministratore di un altro AWS account di distribuire i tuoi prodotti agli utenti finali, condividi il tuo AWS Service Catalog portafoglio con loro utilizzando account-to-account la condivisione o AWS Organizations.

Quando condividi un portafoglio utilizzando account-to-account sharing o Organizations, condividi un riferimento di quel portafoglio. I prodotti e i vincoli nel portafoglio importato rimangono sincronizzati con le modifiche che apporti al portafoglio condiviso, ovvero il portafoglio originale che hai condiviso.

Il destinatario non può modificare i prodotti o i vincoli, ma può aggiungere AWS Identity and Access Management l'accesso per gli utenti finali.

Note

Non è possibile condividere una risorsa condivisa. Sono inclusi i portafogli che contengono un prodotto condiviso.

Account-to-account condivisione

Per completare questi passaggi, è necessario ottenere l'ID account dell' AWS account di destinazione. Puoi trovare l'ID nella pagina Il mio account all'interno Console di gestione AWS dell'account di destinazione.

Per condividere un portafoglio con un AWS account

1. Aprire la console Service Catalog all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.

2. Nel menu di navigazione a sinistra, scegli Portfolio, quindi seleziona il portfolio che desideri condividere. Nel menu Azioni, seleziona Condividi.
3. In Inserisci l'ID dell'account, inserisci l'ID dell' AWS account con cui stai condividendo. (Facoltativo) Seleziona [TagOption Condivisione](#). Quindi, scegli Condividi.
4. Invia l'URL all' AWS Service Catalog amministratore dell'account di destinazione. L'URL apre la pagina Importa portafoglio con l'ARN del portafoglio condiviso fornito automaticamente.

Importazione di un portafoglio

Se AWS Service Catalog l'amministratore di un altro AWS account condivide un portafoglio con te, importa quel portafoglio nel tuo account in modo da poterne distribuire i prodotti agli utenti finali.

Non è necessario importare un portafoglio se il portafoglio è stato condiviso tramite AWS Organizations.

Per importare il portfolio, è necessario ottenere l'ID del portafoglio dall'amministratore.

Per visualizzare tutti i portafogli importati, apri la AWS Service Catalog console all'indirizzo <https://console.aws.amazon.com/servicecatalog/>. Nella pagina Portfolio, seleziona la scheda Importati. Esaminate la tabella Portafogli importati.

Condivisione con AWS Organizations

Puoi condividere i AWS Service Catalog portafogli utilizzando AWS Organizations.

Innanzitutto, devi decidere se condividere dall'account di gestione o da un account amministratore delegato. Se non desideri condividere dal tuo account di gestione, registra un account amministratore delegato da utilizzare per la condivisione. Per ulteriori informazioni, consulta [Registrazione di un amministratore delegato](#) nella Guida per sviluppatori di CloudFormation .

Successivamente, devi decidere con chi condividere. Puoi condividere con le seguenti entità:

- Un account dell'organizzazione.
- Un'unità organizzativa (OU).
- L'organizzazione stessa. (Condivisione con tutti gli account dell'organizzazione).

Condivisione da un account di gestione

È possibile condividere un portfolio con un'organizzazione quando si utilizza la struttura organizzativa o si immette l'ID di un nodo organizzativo.

Per condividere un portfolio con un'organizzazione utilizzando la struttura organizzativa

1. Apri la AWS Service Catalog console all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Nella pagina Portafogli, seleziona il portfolio che desideri condividere. Nel menu Azioni, seleziona Condividi.
3. Seleziona AWS Organizationse filtra in base alla tua struttura organizzativa.

È possibile selezionare il nodo Root per condividere il portfolio con l'intera organizzazione, un'unità organizzativa (OU) principale, un'unità organizzativa secondaria o un AWS account all'interno dell'organizzazione.

La condivisione con un'unità organizzativa principale consente di condividere il portafoglio con tutti gli account e le unità organizzative secondarie all'interno di tale unità organizzativa principale.

È possibile selezionare Visualizza solo AWS gli account per visualizzare un elenco di tutti gli AWS account dell'organizzazione.

Per condividere un portafoglio con un'organizzazione inserendo l'ID del nodo organizzativo

1. Apri la AWS Service Catalog console all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Nella pagina Portafogli, seleziona il portfolio che desideri condividere. Nel menu Azioni, seleziona Condividi.
3. Seleziona Nodo dell'organizzazione.

Seleziona se desideri condividere con l'intera organizzazione, un AWS account all'interno dell'organizzazione o un'unità organizzativa.

Inserisci l'ID del nodo organizzativo selezionato, che puoi trovare all'interno della AWS Organizations console all'indirizzo <https://console.aws.amazon.com/organizations/>.

Condivisione da un account di amministratore delegato

L'account di gestione di un'organizzazione può registrare e annullare la registrazione di altri account come amministratori delegati dell'organizzazione.

Un amministratore delegato può condividere AWS Service Catalog le risorse della propria organizzazione allo stesso modo di un account di gestione. Sono autorizzati a creare, eliminare e condividere portafogli.

Per registrare o annullare la registrazione di un amministratore delegato, è necessario utilizzare l'API o la CLI dell'account di gestione. Per ulteriori informazioni, consulta le pagine [RegisterDelegatedAdministrator](#) e [DeregisterDelegatedAdministrator](#) nella Documentazione di riferimento dell'API AWS Organizations .

Note

Prima di poter designare un delegato, l'amministratore deve chiamare [EnableAWSOrganizationsAccess](#)

La procedura per condividere un portfolio da un account amministratore delegato è la stessa della condivisione da un account di gestione, come illustrato sopra in [the section called “Condivisione da un account di gestione”](#)

Se un membro viene annullato dalla registrazione come amministratore delegato, si verifica quanto segue:

- Le operazioni di portafoglio create da tale account vengono rimosse.
- Gli account non possono più creare nuove quote di portafoglio.

Note

Se il portafoglio e le azioni creati da un amministratore delegato non vengono rimossi dopo la cancellazione della registrazione dell'amministratore delegato, registra e annulla nuovamente la registrazione dell'amministratore delegato. Questa azione rimuove il portafoglio e le azioni creati da quell'account.

Spostamento degli account all'interno dell'organizzazione

Se trasferisci un account all'interno della tua organizzazione, i AWS Service Catalog portafogli condivisi con l'account potrebbero cambiare.

Gli account hanno accesso solo ai portafogli condivisi con l'organizzazione o l'unità organizzativa di destinazione.

Condivisione TagOptions durante la condivisione dei portafogli

In qualità di amministratore, puoi creare una condivisione da includere TagOptions. TagOptions sono coppie chiave-valore che consentono agli amministratori di:

- Definire e applicare la tassonomia per i tag.
- Definire le opzioni relative ai tag e associatele a prodotti e portafogli.
- Condividi le opzioni di tag associate a portafogli e prodotti con altri account.

Quando aggiungi o rimuovi opzioni di tag nell'account principale, la modifica appare automaticamente negli account dei destinatari. Negli account dei destinatari, quando un utente finale fornisce un prodotto TagOptions, deve scegliere i valori per i tag che diventano tag sul prodotto fornito.

Negli account dei destinatari, gli amministratori possono associare altre informazioni locali TagOptions al portafoglio importato per applicare regole di etichettatura specifiche per quell'account.

Note

Per condividere un portafoglio, è necessario l'ID dell'account del AWS consumatore. Trova l'ID AWS dell'account in *Il mio account* nella console.

Note

Se a TagOption ha un solo valore, AWS lo applica automaticamente durante il processo di provisioning.

Da condividere TagOptions quando si condividono i portafogli

1. Dal menu di navigazione a sinistra, scegli Portfolio.

2. In Portafogli locali, scegli e apri un portfolio.
3. Scegli Condividi dall'elenco qui sopra, quindi scegli il pulsante Condividi.
4. Scegli di condividere con un altro AWS account o organizzazione.
5. Inserisci il numero ID dell'account a 12 cifre, seleziona Abilita, quindi scegli Condividi.

L'account che hai condiviso viene visualizzato nella sezione Account condivisi con. Indica se TagOptions sono stati abilitati.

Puoi anche aggiornare una quota di portafoglio da includere TagOptions. Tutto TagOptions ciò che appartiene al portafoglio e al prodotto viene ora condiviso su questo account.

Per aggiornare una condivisione di portafoglio da includere TagOptions

1. Dal menu di navigazione a sinistra, scegli Portfolio.
2. In Portafoglio locale, scegli e apri un portafoglio.
3. Scegli Condividi dalla lista qui sopra.
4. In Account condivisi con, scegli un ID account, quindi scegli Azioni.
5. Seleziona Aggiorna unshare o Annulla share.

Quando selezioni Aggiorna non condividere, scegli Abilita per avviare la condivisione.

TagOptions L'account che hai condiviso viene visualizzato nella sezione Account condivisi con.

Quando selezioni Annulla condivisione, conferma che non desideri più condividere l'account.

Condivisione dei nomi principali durante la condivisione dei portafogli

In qualità di amministratore, puoi creare una condivisione di portafoglio che includa i nomi principali. I nomi principali sono nomi di gruppi, ruoli e utenti che gli amministratori possono specificare in un portfolio e quindi condividere con il portfolio. Quando condividi il portfolio, AWS Service Catalog verifica se tali nomi principali esistono già. Se esistono, associa AWS Service Catalog automaticamente gli IAM Principal corrispondenti al portafoglio condiviso per concedere l'accesso agli utenti.

Note

Quando associ un principale a un portafoglio, può verificarsi una potenziale escalation di privilegi quando tale portafoglio viene condiviso successivamente con altri account. Per un

utente in un account destinatario che non è un AWS Service Catalog amministratore, ma ha comunque la possibilità di creare Principal (Utenti/Ruoli), tale utente può creare un Principal IAM che corrisponda a un'associazione di nomi principali per il portafoglio. Anche se questo utente potrebbe non sapere a quali nomi principali sono associati AWS Service Catalog, potrebbe essere in grado di indovinare l'utente. Se questo potenziale percorso di escalation è fonte di preoccupazione, AWS Service Catalog consiglia di utilizzare `PrincipalType` `as. IAM`. Con questa configurazione, `PrincipalARN` deve esistere già nell'account del destinatario prima dell'associazione.

Quando aggiungi o rimuovi i nomi principali nell'account principale, applica AWS Service Catalog automaticamente tali modifiche nell'account del destinatario. Gli utenti dell'account destinatario possono quindi eseguire attività in base al loro ruolo:

- Gli utenti finali possono fornire, aggiornare e terminare il prodotto del portafoglio.
- Gli amministratori possono associare ulteriori IAM Principal al portafoglio importato per concedere l'accesso agli utenti finali specifici di quell'account.

Note

La condivisione dei nomi principali è disponibile solo per. AWS Organizations

Per condividere i nomi principali durante la condivisione dei portafogli

1. Dal menu di navigazione a sinistra, scegli Portfolio.
2. In Portafogli locali, scegli il portafoglio che desideri condividere.
3. Nel menu Azioni, scegli Condividi.
4. Seleziona un'organizzazione in AWS Organizations.
5. Seleziona la radice dell'intera organizzazione, un'unità organizzativa (OU) o un membro dell'organizzazione.
6. Nelle impostazioni di condivisione, abilita l'opzione di condivisione principale.

Puoi anche aggiornare una condivisione di portafoglio per includere la condivisione del nome principale. In questo modo tutti i nomi principali che appartengono a quel portafoglio vengono condivisi con l'account del destinatario.

Per aggiornare una condivisione di portafoglio per abilitare o disabilitare i nomi principali

1. Dal menu di navigazione a sinistra, scegli Portfolio.
2. In Portafoglio locale, scegli il portafoglio che desideri aggiornare.
3. Scegli la scheda Condividi.
4. Seleziona la condivisione che desideri aggiornare, quindi scegli Condividi.
5. Scegli Aggiorna condivisione, quindi scegli Abilita per avviare la condivisione principale. AWS Service Catalog quindi condivide i nomi principali negli account dei destinatari.

Disabilita la condivisione dei principali se desideri interrompere la condivisione dei nomi principali con gli account dei destinatari.

Utilizzo di caratteri jolly quando si condividono i nomi principali

AWS Service Catalog supporta la concessione dell'accesso al portafoglio ai nomi dei principali IAM (utente, gruppo o ruolo) con caratteri jolly, come '*' o '?'. L'utilizzo di pattern wildcard consente di coprire più nomi principali IAM contemporaneamente. Il percorso ARN e il nome principale consentono un numero illimitato di caratteri jolly.

Esempi di un ARN con caratteri jolly accettabile:

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

Esempi di un ARN con caratteri jolly non accettabile:

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

Nel formato IAM Principal ARN (**arn:partition:iam::resource-type/resource-path/resource-name**), i valori validi includono user/, group/ o role/. Il «?» e «*» sono consentiti solo dopo il tipo di risorsa nel segmento resource-id. Puoi usare caratteri speciali ovunque all'interno del resource-id.

Il carattere «*» corrisponde anche al carattere «/», permettendo la formazione di percorsi all'interno del resource-id. Esempio:

arn:aws:iam::role/*/ResourceName_? corrisponde a entrambi e. **arn:aws:iam::role/pathA/pathB/ResourceName_1** **arn:aws:iam::role/pathA/ResourceName_1**

Condivisione e importazione di portafogli

Per rendere AWS Service Catalog i tuoi prodotti disponibili a utenti che non fanno parte della tua organizzazione Account AWS, ad esempio utenti che appartengono ad altre organizzazioni o ad altri Account AWS membri della tua organizzazione, condividi i tuoi portafogli con loro. È possibile condividere in diversi modi, tra cui la account-to-account condivisione, la condivisione organizzativa e la distribuzione dei cataloghi utilizzando set di pile.

Prima di condividere prodotti e portafogli con altri account, devi decidere se condividere un riferimento del catalogo o distribuire una copia del catalogo in ciascun account del destinatario. Ti ricordiamo che se distribuisi una copia, devi ridistribuirla se ci sono aggiornamenti che desideri propagare agli account dei destinatari.

Puoi utilizzare i set di stack per distribuire il catalogo su più account contemporaneamente. Se desideri condividere un riferimento (una versione importata del tuo portfolio che rimane sincronizzata con l'originale), puoi utilizzare la account-to-account condivisione o la condivisione utilizzando AWS Organizations

Per utilizzare i set di stack per distribuire una copia del catalogo, consulta [Come configurare un catalogo multiregionale e multi-account di prodotti standard aziendali](#). AWS Service Catalog

Quando condividi un portafoglio utilizzando account-to-account la condivisione o AWS Organizations, consenti AWS Service Catalog all'amministratore di un altro AWS account di importare il tuo portafoglio nel proprio account e distribuire i prodotti agli utenti finali di quell'account.

Questo portafoglio importato non è una copia indipendente. I prodotti e i vincoli nel portafoglio importato rimangono sincronizzati con le modifiche che apporti al portafoglio condiviso, ovvero il portafoglio originale che hai condiviso. L'amministratore destinatario, l'amministratore con cui condividi un portafoglio, non può modificare i prodotti o i vincoli, ma può aggiungere l'accesso AWS Identity and Access Management (IAM) per gli utenti finali. Per ulteriori informazioni, consulta [Concessione dell'accesso agli utenti](#).

L'amministratore destinatario può distribuire i prodotti agli utenti finali che appartengono al proprio AWS account nei seguenti modi:

- Aggiungendo utenti, gruppi e ruoli al portfolio importato.
- Aggiungendo prodotti dal portafoglio importato a un portafoglio locale, un portafoglio separato creato dall'amministratore destinatario e che appartiene al suo AWS account. L'amministratore destinatario aggiunge quindi utenti, gruppi e ruoli a quel portafoglio locale. Tutti i vincoli originariamente applicati ai prodotti del portafoglio condiviso sono presenti anche nel portafoglio locale. L'amministratore locale del destinatario del portafoglio può aggiungere ulteriori vincoli, ma non può rimuovere i vincoli originariamente importati dal portafoglio condiviso.

Quando aggiungi prodotti o vincoli al portafoglio condiviso o li rimuovi dal quel portafoglio, la modifica viene propagata a tutte le istanze importate del portafoglio. Ad esempio, se rimuovi un prodotto dal portafoglio condiviso, quel prodotto viene rimosso anche dal portafoglio importato. Viene inoltre rimosso da tutti i portafogli locali a cui il prodotto importato è stato aggiunto. Se un utente finale avvia un prodotto prima della rimozione, il prodotto con provisioning dell'utente finale continua a essere eseguito, ma il prodotto non è più disponibile per avvii successivi.

Se applichi un vincolo di avvio a un prodotto in un portafoglio condiviso, viene propagato a tutte le istanze importate del prodotto. Per ignorare questo vincolo di avvio, l'amministratore destinatario aggiunge il prodotto a un portafoglio locale e quindi applica un altro vincolo di avvio al prodotto. Il vincolo di avvio applicato imposta un ruolo di avvio per il prodotto.

Un ruolo di lancio è un ruolo IAM AWS Service Catalog utilizzato per fornire AWS risorse (come EC2 istanze Amazon o database Amazon RDS) quando un utente finale lancia il prodotto. In qualità di amministratore, puoi scegliere di designare un ruolo di lancio specifico (ARN) o un nome di ruolo locale. Se si utilizza il ruolo ARN, il ruolo verrà utilizzato anche se l'utente finale appartiene a un AWS account diverso da quello che possiede il ruolo di avvio. Se si utilizza un nome di ruolo locale, viene utilizzato il ruolo IAM con quel nome nell'account dell'utente finale.

Per ulteriori informazioni sui vincoli e i ruoli di avvio, consulta [AWS Service Catalog Vincoli di avvio](#). L' AWS account proprietario del ruolo di lancio fornisce le AWS risorse e a tale account vengono addebitati i costi di utilizzo di tali risorse. Per ulteriori informazioni, consultare [AWS Service Catalog Prezzi](#).

Questo video mostra come condividere portafogli tra account in AWS Service Catalog

[Condividi \(https://www.youtube.com/embed/BVSoHYOppjk% 22% 3EShare\) portafogli tra conti in.](https://www.youtube.com/embed/BVSoHYOppjk%22%3EShare)
AWS Service Catalog

Note

Non puoi condividere nuovamente i prodotti di un portafoglio importato o condiviso.

Note

Le importazioni di portafoglio devono avvenire nella stessa area tra gli account di gestione e quelli dipendenti.

Relazione tra portafogli condivisi e importati

Questa tabella riassume la relazione tra un portafoglio importato e un portafoglio condiviso e le azioni che un amministratore che importa un portafoglio può e non può intraprendere con quel portafoglio e i prodotti in esso contenuti.

| Elemento di portafoglio condiviso | Relazione con portafoglio importato | L'amministratore di destinazione può | L'amministratore di destinazione non può |
|-----------------------------------|--|--|---|
| Prodotti e versioni di prodotto | Ereditati. Se il creatore del portafoglio aggiunge prodotti al portafoglio condiviso o ne rimuove dallo stesso, la modifica viene propagata al portafoglio importato. | Aggiungere prodotti importati a portafogli locali. I prodotti rimangono sincronizzati con il portafoglio condiviso. | Caricare o aggiungere prodotti al portafoglio importato o rimuovere prodotti dal portafoglio importato. |
| Vincoli di avvio | Ereditati. Se il creatore del portafoglio aggiunge o rimuove vincoli di lancio da un prodotto condiviso, la modifica | In un portafoglio locale, l'amministratore può applicare vincoli di lancio che influiscono sul lancio locale del prodotto. | Aggiungere vincoli di avvio al portafoglio importato o rimuoverli e dallo stesso. |

| Elemento di portafoglio condiviso | Relazione con portafoglio importato | L'amministratore di destinazione può | L'amministratore di destinazione non può |
|-----------------------------------|---|---|---|
| | <p>si propaga a tutte le istanze importate del prodotto.</p> <p>Se l'amministratore destinatario aggiunge un prodotto importato al proprio portafoglio locale, tale vincolo di lancio importato non viene trasferito al portafoglio condiviso.</p> | | |
| Vincoli di modello | <p>Ereditati.</p> <p>Se il creatore del portafoglio aggiunge vincoli di modello a un prodotto condiviso o ne rimuove dallo stesso, la modifica viene propagata a tutte le istanze importate del prodotto.</p> <p>Se l'amministratore destinatario aggiunge un prodotto importato a un portafoglio locale, i vincoli del modello importato non vengono trasferiti al portafoglio locale.</p> | In un portfolio locale, l'amministratore può aggiungere vincoli di modello che limitano il prodotto locale. | Rimuovere i vincoli di modello importati. |

| Elemento di portafoglio condiviso | Relazione con portafoglio importato | L'amministratore di destinazione può | L'amministratore di destinazione non può |
|-----------------------------------|-------------------------------------|--|--|
| Utenti, gruppi e ruoli | Non ereditati. | Aggiungi utenti, gruppi e ruoli presenti nell'account dell'amministratore. AWS | Non applicabile. |

Gestione di prodotti

Puoi creare prodotti, aggiornare i prodotti creando una nuova versione basata su un modello aggiornato e raggruppare i prodotti in portafogli per distribuirli agli utenti.

Le nuove versioni dei prodotti vengono propagate a tutti gli utenti che hanno accesso al prodotto tramite un portafoglio. Quando distribuisce un aggiornamento, gli utenti finali possono aggiornare i prodotti forniti esistenti.

Processi

- [Visualizzazione della pagina dei prodotti](#)
- [Creazione di prodotti](#)
- [Aggiungere prodotti ai portafogli](#)
- [Aggiornamento dei prodotti](#)
- [Sincronizzazione dei prodotti con i file modello di GitHub GitHub Enterprise o Bitbucket](#)
- [Eliminazione di prodotti](#)
- [Gestione delle versioni](#)

Visualizzazione della pagina dei prodotti

È possibile gestire i prodotti dalla pagina con l'elenco dei prodotti nella console di AWS Service Catalog amministrazione.

Per visualizzare la pagina con l'elenco dei prodotti

1. Aprire la console Service Catalog all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Scegli Elenco prodotti.

Creazione di prodotti

Puoi creare prodotti dalla pagina Prodotti nella console dell' AWS Service Catalog amministratore.

Note

La creazione di prodotti Terraform richiede una configurazione aggiuntiva, tra cui un motore di provisioning Terraform e un ruolo di lancio. Per ulteriori informazioni, consulta. [Guida introduttiva a un prodotto Terraform](#)

Per creare un nuovo AWS Service Catalog prodotto

1. Vai alla pagina con l'elenco dei prodotti.
2. Scegli Crea prodotto, quindi scegli Crea prodotto.
3. Dettagli del prodotto: ti consente di scegliere il tipo di prodotto che desideri creare. AWS Service Catalog supporta CloudFormation i tipi di prodotto Terraform Cloud ed External (supporta Terraform Community Edition). I dettagli del prodotto contengono anche i metadati che appaiono quando cerchi e visualizzi i prodotti in un elenco o in una pagina prodotto. Immetti i seguenti dati:
 - Product name (Nome prodotto) – Il nome del prodotto.
 - Descrizione del prodotto: la descrizione viene visualizzata nell'elenco dei prodotti per aiutarti a scegliere il prodotto corretto.
 - Proprietario: la persona o l'organizzazione che pubblica questo prodotto. Il proprietario potrebbe essere il nome dell'organizzazione IT o l'amministratore.
 - Distributore (opzionale): il nome dell'editore dell'applicazione. Questo campo consente di ordinare l'elenco dei prodotti per facilitarne la ricerca.
4. I dettagli sulla versione consentono di aggiungere il file modello e creare il prodotto. Immetti i seguenti dati:
 - Scegli il metodo: esistono quattro modi per aggiungere un file modello.
 - Usa un file modello locale: carica un CloudFormation modello o un file di configurazione Terraform tar.gz da un'unità locale.
 - Usa un URL Amazon S3: specifica un URL che punti a un CloudFormation modello o a un file di configurazione Terraform tar.gz archiviato in Amazon S3. Se specifichi un URL Amazon S3, deve iniziare con. `https://`

- Usa un repository esterno: specifica il tuo repository di GitHub codice, GitHub Enterprise o Bitbucket. AWS Service Catalog consente di sincronizzare i prodotti con i file modello. Per i prodotti Terraform, il formato di file modello deve essere un singolo file archiviato in Tar e compresso in Gzip.
 - Usa uno CloudFormation stack esistente: inserisci l'ARN per uno CloudFormation stack esistente. Questo metodo non supporta Terraform Cloud o prodotti esterni.
 - Nome della versione (opzionale): il nome della versione del prodotto (ad esempio, «v1», «v2beta»). Gli spazi non sono consentiti.
 - Descrizione (opzionale): una descrizione della versione del prodotto, incluso il modo in cui questa versione si differenzia dalle altre versioni.
 - Guida: gestita nella scheda delle versioni in una pagina dei dettagli del prodotto. Quando viene creata una versione del prodotto, durante il flusso di lavoro di creazione del prodotto, le linee guida per quella versione sono impostate come predefinite. [Per ulteriori informazioni sulle linee guida, consulta Gestione delle versioni.](#)
5. Support Details identifica l'organizzazione all'interno dell'azienda e fornisce un punto di contatto per l'assistenza. Immetti i seguenti dati:
- Email contact (E-mail di contatto) (facoltativo) – L'indirizzo e-mail a cui segnalare i problemi relativi al prodotto.
 - Link di supporto (opzionale): un URL a un sito in cui gli utenti possono trovare informazioni di supporto o ticket di file. L'URL deve iniziare con `http://` o `https://`. Gli amministratori sono responsabili del mantenimento dell'accuratezza e dell'accesso alle informazioni di supporto.
 - Descrizione dell'assistenza (opzionale): una descrizione di come utilizzare il collegamento Email contact and Support.
6. Gestione dei tag (opzionale): oltre a utilizzare i tag per classificare le risorse, puoi utilizzarli anche per autenticare le autorizzazioni necessarie per creare questa risorsa.
7. Crea prodotto: dopo aver completato il modulo, seleziona Crea prodotto. Dopo alcuni secondi, il prodotto viene visualizzato nella pagina con l'elenco dei prodotti. È possibile che sia necessario aggiornare il browser per visualizzare il prodotto.

È inoltre possibile utilizzarlo CodePipeline per creare e configurare una pipeline in cui distribuire il modello di prodotto AWS Service Catalog e apportare le modifiche apportate nell'archivio di origine. Per ulteriori informazioni, consulta [Tutorial: Create a pipeline](#) that deploys to. AWS Service Catalog

È possibile definire le proprietà dei parametri nel modello CloudFormation o nel modello Terraform e applicare tali regole durante il provisioning. Queste proprietà possono definire la lunghezza minima e massima, i valori minimo e massimo, i valori consentiti e un'espressione regolare per il valore. AWS Service Catalog emette un avviso durante il provisioning se il valore fornito non aderisce alla proprietà del parametro. Per ulteriori informazioni sulle proprietà dei parametri, vedere [Parametri nella Guida](#) per l'CloudFormation utente.

Risoluzione dei problemi

È necessario disporre dell'autorizzazione per recuperare oggetti dai bucket Amazon S3. Altrimenti, potresti riscontrare il seguente errore durante l'avvio o l'aggiornamento di un prodotto.

Error: failed to process product version s3 access denied exception

Se visualizzi questo messaggio, assicurati di disporre dell'autorizzazione per recuperare oggetti dai seguenti bucket:

- Il bucket in cui è archiviato il modello di artefatto di provisioning.
- Il bucket che inizia con "cf-templates-*" e dove memorizza il modello di artefatto di provisioning. AWS Service Catalog
- Il bucket interno che inizia con "sc-*" e dove memorizza i metadati. AWS Service Catalog Non sarai in grado di vedere questo bucket dal tuo account.

La seguente politica di esempio mostra le autorizzazioni minime necessarie per recuperare oggetti dai bucket menzionati in precedenza.

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

Aggiungere prodotti ai portafogli

Puoi aggiungere prodotti a qualsiasi numero di portafogli. Quando un prodotto viene aggiornato, tutti i portafogli (compresi i portafogli condivisi) che contengono il prodotto ricevono automaticamente la nuova versione.

Aggiunta di un prodotto dal catalogo a un portafoglio

1. Vai alla pagina con l'elenco dei prodotti.
2. Seleziona un prodotto, quindi scegli Azioni. Dal menu a discesa, scegli Aggiungi prodotto al portafoglio. Verrai indirizzato alla pagina Aggiungi ***name-of-product*** al portfolio.
3. Scegli un portfolio, quindi scegli Aggiungi prodotto al portafoglio.

Quando si aggiunge un prodotto Terraform a un portafoglio, il prodotto richiede un vincolo di lancio. Devi selezionare un ruolo IAM dal tuo account, inserire un ARN del ruolo IAM o inserire un nome di ruolo. Se specifichi un nome di ruolo e se un account utilizza il vincolo di avvio, l'account utilizza quel nome per il ruolo IAM. Ciò consente ai vincoli relativi al ruolo di avvio di essere indipendenti dall'account, garantendo la possibilità di creare meno risorse per account condiviso. Per dettagli e istruzioni, consulta [Passaggio 6: aggiungi un vincolo di lancio al tuo prodotto Terraform](#)

Un portafoglio può contenere numerosi prodotti che sono una combinazione di tipi di prodotti Terraform CloudFormation e diversi.

Aggiornamento dei prodotti

Quando aggiorni il modello di un prodotto, crei una nuova versione del prodotto. Le nuove versioni del prodotto sono automaticamente disponibili per tutti gli utenti che hanno accesso a un portafoglio contenente il prodotto.

Note

Quando si aggiorna un prodotto esistente, non è possibile modificare il tipo di prodotto (CloudFormation o Terraform). Ad esempio, se aggiorni un CloudFormation prodotto, non puoi sostituire il CloudFormation modello esistente con un file di configurazione Terraform tar.gz. È necessario aggiornare il file CloudFormation modello esistente con un nuovo file CloudFormation modello.

Gli utenti finali che attualmente utilizzano un prodotto fornito della versione precedente del prodotto possono aggiornare il prodotto fornito alla nuova versione. Quando è disponibile una nuova versione di un prodotto, gli utenti possono utilizzare il comando Update provisioned product nell'elenco dei prodotti Provisioned o nelle pagine dei dettagli del prodotto Provisioned.

Prima di creare una nuova versione di un prodotto, AWS Service Catalog consiglia di testare gli aggiornamenti del prodotto nel CloudFormation o nel motore Terraform per assicurarsi che funzionino correttamente.

Creazione di una nuova versione di un prodotto

1. Vai alla pagina con l'elenco dei prodotti.
2. Scegli il prodotto che desideri aggiornare. Verrai indirizzato alla pagina dei dettagli del prodotto.
3. Nella pagina dei dettagli del prodotto, espandi la scheda Versioni, quindi scegli Crea nuova versione.
4. In Dettagli della versione, procedi come segue:

- Scegli modello: esistono quattro modi per aggiungere un file modello.

Usa un file modello locale: carica un CloudFormation modello o un file di configurazione Terraform tar.gz da un'unità locale.

Usa un URL Amazon S3: specifica un URL che punti a un CloudFormation modello o a un file di configurazione Terraform tar.gz archiviato in Amazon S3. Se specifichi un URL Amazon S3, deve iniziare con https://.

Usa un repository esterno: specifica il tuo repository di GitHub codice, GitHub Enterprise o Bitbucket. AWS Service Catalog consente di sincronizzare i prodotti con i file modello. Per i prodotti Terraform, il formato di file modello deve essere un singolo file archiviato in Tar e compresso in Gzip.

Usa uno CloudFormation stack esistente: inserisci l'ARN per uno CloudFormation stack esistente. Questo metodo non supporta Terraform Cloud o prodotti esterni.

- Titolo della versione: il nome della versione del prodotto (ad esempio «v1», «v2beta»). Gli spazi non sono consentiti.
- Descrizione (opzionale): una descrizione della versione del prodotto, incluso il modo in cui questa versione si differenzia dalla versione precedente.

5. Scegli Crea versione del prodotto.

Puoi anche utilizzarla CodePipeline per creare e configurare una pipeline in cui distribuire il modello di prodotto e inserire AWS Service Catalog le modifiche nel tuo repository di origine. Per ulteriori informazioni, consulta [Tutorial: Create a pipeline](#) that deploys to. AWS Service Catalog

Sincronizzazione dei prodotti con i file modello di GitHub GitHub Enterprise o Bitbucket

AWS Service Catalog consente di sincronizzare i prodotti con i file modello gestiti tramite un provider di repository esterno. AWS Service Catalog si riferisce ai prodotti con questo tipo di connessione modello come prodotti sincronizzati con Git. Le opzioni di repository includono Enterprise o GitHub Bitbucket GitHub . Dopo aver autorizzato il tuo account Account AWS con un account di repository esterno, puoi creare nuovi AWS Service Catalog prodotti o aggiornare i prodotti esistenti per la sincronizzazione con un file modello nel repository. Quando vengono apportate modifiche al file modello e salvate nel repository (ad esempio, utilizzando git-push), rileva AWS Service Catalog automaticamente le modifiche e crea una nuova versione del prodotto (artefatto).

Argomenti

- [Autorizzazioni necessarie per sincronizzare i prodotti con file modello esterni](#)
- [Crea una connessione all'account](#)
- [Visualizzazione delle connessioni di prodotti sincronizzate con Git](#)
- [Aggiornamento delle connessioni dei prodotti sincronizzate con Git](#)
- [Eliminazione delle connessioni di prodotti sincronizzate con Git](#)
- [Sincronizzazione dei prodotti Terraform con i file modello di GitHub GitHub Enterprise o Bitbucket](#)
- [Regione AWS supporto per prodotti sincronizzati con Git](#)

Autorizzazioni necessarie per sincronizzare i prodotti con file modello esterni

È possibile utilizzare la seguente politica AWS Identity and Access Management (IAM) come modello per consentire agli AWS Service Catalog amministratori di sincronizzare i prodotti con i file modello da un repository esterno. Questa politica include le autorizzazioni richieste da entrambi e. CodeConnections AWS Service Catalog AWS Service Catalog consiglia di copiare il modello di policy riportato di seguito e di utilizzare anche la [policy AWS Service CatalogAWSServiceCatalogAdminFullAccess gestita](#) quando si abilitano prodotti sincronizzati con il repository.

JSON

```

{
  "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"
        }
      }
    }
  ]
}

```

Crea una connessione all'account

Prima di sincronizzare un file modello con un AWS Service Catalog prodotto, devi creare e autorizzare una connessione unica. account-to-account Questa connessione viene utilizzata per specificare i dettagli del repository contenente il file modello desiderato. È possibile creare una connessione utilizzando la AWS Service Catalog console, la CodeConnections console AWS Command Line Interface (CLI) o. CodeConnections APIs

Dopo aver stabilito una connessione, puoi utilizzare la AWS Service Catalog console, l' AWS Service Catalog API o la CLI per creare un prodotto sincronizzato AWS Service Catalog . AWS Service Catalog gli amministratori possono creare nuovi AWS Service Catalog prodotti o aggiornare quelli esistenti sulla base di un file modello in un repository e in una filiale. Se viene salvata una modifica nel repository, rileva AWS Service Catalog automaticamente la modifica e crea una nuova versione del prodotto. Le versioni precedenti del prodotto vengono mantenute fino al limite di versioni prescritto e viene assegnato uno stato obsoleto.

Inoltre, crea AWS Service Catalog automaticamente un ruolo collegato al servizio (SLR) dopo la creazione della connessione. Questa SLR consente di AWS Service Catalog rilevare eventuali modifiche al file modello salvate nel repository. La SLR consente inoltre di AWS Service Catalog creare automaticamente nuove versioni di prodotto per prodotti sincronizzati. [Per ulteriori informazioni sulle autorizzazioni e sulle funzionalità SLR, consulta Ruoli collegati al servizio per. AWS Service Catalog](#)

Per creare un nuovo prodotto sincronizzato con Git

1. Nel pannello di navigazione a sinistra, scegli Elenco prodotti, quindi scegli Crea prodotto.
2. Inserisci i dettagli del prodotto.
3. In Dettagli sulla versione, scegli Specificare il repository di codice utilizzando un AWS CodeStar provider, quindi scegli il link Crea una nuova AWS CodeStar connessione.
4. Dopo aver creato la connessione, aggiorna l'elenco delle connessioni, quindi seleziona la nuova connessione. Specificate i dettagli del repository, inclusi il repository, il ramo e il percorso del file del modello.

Per informazioni sull'utilizzo di un file di configurazione Terraform, vedere. [Sincronizzazione dei prodotti Terraform con i file modello di GitHub GitHub Enterprise o Bitbucket](#)

- a. (Facoltativo quando si crea una nuova risorsa di AWS Service Catalog prodotto) Nella sezione Dettagli del supporto, aggiungi i metadati per il prodotto.

- b. (Facoltativo quando si crea una nuova risorsa di AWS Service Catalog prodotto) Nella sezione Tag, scegli Aggiungi nuovo tag e inserisci le coppie Chiave e Valore.
5. Scegli Crea nuovo prodotto.

Per creare più prodotti sincronizzati con Git

1. Nel pannello di navigazione a sinistra della AWS Service Catalog console, scegli Elenco prodotti, quindi scegli Crea più prodotti gestiti da git.
2. Inserisci i dettagli comuni del prodotto.
3. In Dettagli del repository esterno, seleziona una AWS CodeStar connessione, quindi specifica il repository e il ramo.
4. Nel riquadro Aggiungi prodotti, inserisci il percorso del file del modello e il nome del prodotto. Scegli Aggiungi nuovo articolo e continua ad aggiungere prodotti come desideri.
5. Dopo aver aggiunto tutti i prodotti desiderati, scegli Creazione in blocco.

Per connettere un AWS Service Catalog prodotto esistente a un archivio esterno

1. Nel pannello di navigazione a sinistra della AWS Service Catalog console, scegli Elenco prodotti, quindi scegli Connetti i prodotti a un repository esterno.
2. Nella pagina Seleziona prodotti, seleziona i prodotti che desideri connettere a un repository esterno, quindi scegli Avanti.
3. Nella pagina Specificare i dettagli dell'origine, seleziona una AWS CodeStar connessione esistente, quindi specifica il repository, il ramo e il percorso del file modello.
4. Scegli Next (Successivo).
5. Nella pagina Rivedi e invia, verifica i dettagli della connessione, quindi scegli Connetti i prodotti a un repository esterno.

Visualizzazione delle connessioni di prodotti sincronizzate con Git

Puoi utilizzare la AWS Service Catalog console, l'API o visualizzare i dettagli di connessione AWS CLI al repository. Per AWS Service Catalog i prodotti collegati a un file modello, puoi recuperare le informazioni sulla connessione al repository e sull'ultima volta in cui il modello è stato sincronizzato con il prodotto dallo stato dell'ultima sincronizzazione.

Note

È possibile visualizzare le informazioni del repository e lo stato dell'ultima sincronizzazione a livello di prodotto. Gli utenti devono disporre delle autorizzazioni IAM CodeConnections APIs per visualizzare i dettagli del repository. Consulta [Autorizzazioni richieste per sincronizzare i AWS Service Catalog prodotti con i file modello](#) per ulteriori informazioni sulla politica richiesta per queste autorizzazioni IAM.

Per visualizzare i dettagli della connessione e del repository utilizzando Console di gestione AWS

1. Nel pannello di navigazione a sinistra, scegli Elenco prodotti.
2. Seleziona il prodotto dall'elenco.
3. Nella pagina Prodotto, accedi alla sezione Dettagli sull'origine del prodotto.
4. Per visualizzare l'ID di revisione di origine per una versione del prodotto, scegli il link Ultima versione creata. La sezione Dettagli della versione mostra l'ID di revisione di origine.

Per visualizzare i dettagli della connessione e del repository utilizzando AWS CLI

Da AWS CLI, esegui i seguenti comandi:

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

```
$ aws servicecatalog describe-provisioning-artifact
```

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

```
$ aws servicecatalog list-provisioning-artifacts
```

Aggiornamento delle connessioni dei prodotti sincronizzate con Git

Puoi aggiornare le connessioni degli account esistenti e i prodotti sincronizzati con Git utilizzando la AWS Service Catalog console, AWS Service Catalog l'API o. AWS CLI

Per informazioni su come collegare un AWS Service Catalog prodotto esistente a un file modello, consulta [Creazione di nuove connessioni di prodotto sincronizzate con Git](#).

Per aggiornare i prodotti esistenti ai prodotti sincronizzati con Git

1. Nel pannello di navigazione a sinistra, scegli **Elenco prodotti**, quindi scegli una delle seguenti opzioni:
 - Per aggiornare un singolo prodotto, seleziona il prodotto, vai alla sezione **Dettagli sull'origine del prodotto**, quindi scegli **Modifica dettagli**.
 - Per aggiornare più prodotti, scegli **Connetti prodotti a un repository esterno**, seleziona fino a dieci prodotti, quindi scegli **Avanti**.
2. Nella sezione **Dettagli sull'origine del prodotto**, esegui i seguenti aggiornamenti:
 - Specificare la connessione.
 - Specificare il repository.
 - Specificare il ramo.
 - Assegna un nome al file modello.
3. Scegli **Save changes (Salva modifiche)**.

Note

Per i prodotti non ancora collegati a un archivio esterno, puoi utilizzare l'opzione **Connetti a un archivio esterno** visualizzata nell'avviso nella parte superiore della pagina di informazioni sul prodotto dopo aver selezionato il prodotto.

Puoi anche utilizzare la **AWS Service Catalog console** o **AWS CLI**

- **Connect** un **AWS Service Catalog** prodotto esistente a un file modello in un repository esterno
- **Aggiorna** i metadati del prodotto, inclusi il nome, la descrizione e i tag del prodotto.
- **Riconfigura** (aggiorna la sincronizzazione per utilizzare una fonte di repository diversa) una connessione per un prodotto precedentemente connesso. **AWS Service Catalog**

Per aggiornare i dettagli della connessione e del repository utilizzando la console **AWS Service Catalog**

1. Nel pannello di navigazione a sinistra della **AWS Service Catalog console**, scegli **Elenco prodotti**, quindi seleziona un prodotto attualmente connesso a un repository esterno.

2. Nella sezione Dettagli sull'origine del prodotto, scegli Modifica l'origine del prodotto.
3. Nella sezione Dettagli sull'origine del prodotto, specifica il nuovo repository desiderato.
4. Scegli Save changes (Salva modifiche).

Per aggiornare i dettagli della connessione e del repository utilizzando AWS CLI

Dal AWS CLI comando esegui il `$ aws servicecatalog update-provisioning-artifact` comando `$ aws servicecatalog update-product and`.

Eliminazione delle connessioni di prodotti sincronizzate con Git

Puoi eliminare una connessione tra un AWS Service Catalog prodotto e un file modello utilizzando la AWS Service Catalog console, l'API o. CodeConnections AWS CLI Quando disconnetti un prodotto da un file modello, il AWS Service Catalog prodotto sincronizzato passa a un prodotto gestito regolarmente. Dopo aver disconnesso il prodotto, se il file modello viene modificato e salvato nell'archivio precedentemente connesso, le modifiche non vengono riflesse. Per ricollegare un AWS Service Catalog prodotto a un file modello in un repository esterno, consulta [Aggiornamento delle connessioni](#) e dei prodotti sincronizzati. AWS Service Catalog

Per disconnettere un prodotto sincronizzato con Git utilizzando la console AWS Service Catalog

1. Nella Console di gestione AWS, scegli Elenco prodotti dal pannello di navigazione a sinistra.
2. Seleziona un prodotto dall'elenco.
3. Nella pagina Prodotto, accedi alla sezione Dettagli sull'origine del prodotto.
4. Scegli Disconnetti.
5. Conferma l'azione, quindi scegli Disconnetti.

Per disconnettere un prodotto sincronizzato con Git utilizzando AWS CLI

Da, esegui il comando. AWS CLI `$ aws servicecatalog update-product`
Nell'`ConnectionParametersinput`, rimuovi la connessione specificata.

Per eliminare una connessione utilizzando l' CodeConnections API o AWS CLI

Nell' CodeConnections API o AWS CLI, esegui il `$ aws codestar-connections delete-connection` comando.

Sincronizzazione dei prodotti Terraform con i file modello di GitHub GitHub Enterprise o Bitbucket

Quando si crea un prodotto sincronizzato con Git utilizzando un file di configurazione Terraform, il percorso del file accetta solo il formato tar.gz. I formati delle cartelle Terraform non sono accettati nel percorso del file.

Regione AWS supporto per prodotti sincronizzati con Git

AWS Service Catalog supporta prodotti sincronizzati con Git come indicato nella tabella Regioni AWS seguente.

| Regione AWS nome | Regione AWS identità | Support per prodotti sincronizzati con Git |
|---|----------------------|--|
| Stati Uniti orientali (Virginia settentrionale) | us-east-1 | Sì |
| Stati Uniti orientali (Ohio) | us-east-2 | Sì |
| Stati Uniti occidentali (California settentrionale) | us-west-1 | Sì |
| Stati Uniti occidentali (Oregon) | us-west-2 | Sì |
| Africa (Città del Capo) | af-south-1 | No |
| Asia Pacific (Hong Kong) | ap-east-1 | No |
| Asia Pacifico (Giacarta) | ap-southeast-3 | No |
| Asia Pacifico (Mumbai) | ap-south-1 | Sì |
| Asia Pacifico (Osaka) | ap-northeast-3 | No |
| Asia Pacific (Seoul) | ap-northeast-2 | Sì |
| Asia Pacifico (Singapore) | ap-southeast-1 | Sì |
| Asia Pacifico (Sydney) | ap-southeast-2 | Sì |

| Regione AWS nome | Regione AWS identità | Support per prodotti sincronizzati con Git |
|--|----------------------|--|
| Asia Pacifico (Tokyo) | ap-northeast-1 | Sì |
| Canada (Centrale) | ca-central-1 | Sì |
| Europa (Francoforte) | eu-central-1 | Sì |
| Europa (Irlanda) | eu-west-1 | Sì |
| Europa (Londra) | eu-west-2 | Sì |
| Europe (Milan) | eu-south-1 | No |
| Europa (Parigi) | eu-west-3 | Sì |
| Europa (Stoccolma) | eu-north-1 | Sì |
| Medio Oriente (Bahrein) | me-south-1 | No |
| Sud America (San Paolo) | sa-east-1 | Sì |
| AWS GovCloud (Stati Uniti orientali) | us-gov-east-1 | No |
| AWS GovCloud (Stati Uniti occidentali) | us-gov-west-1 | No |

Eliminazione di prodotti

Quando elimini un prodotto, AWS Service Catalog rimuove tutte le versioni del prodotto da ogni portafoglio contenente il prodotto.

AWS Service Catalog consente di eliminare un prodotto utilizzando la AWS Service Catalog console o AWS CLI. Per eliminare correttamente un prodotto, è necessario innanzitutto dissociare tutte le risorse associate al prodotto. Esempi di associazioni di risorse di prodotto includono associazioni di portafoglio TagOptions, budget e Service Actions.

Important

Non è possibile ripristinare un prodotto dopo che è stato eliminato.

Per eliminare un prodotto utilizzando la AWS Service Catalog console

1. Vai alla pagina Portafogli e seleziona il portfolio contenente il prodotto che desideri eliminare.
2. Seleziona il prodotto che desideri eliminare, quindi scegli Elimina nella parte superiore destra del riquadro del prodotto.
3. Per i prodotti senza risorse associate, conferma il prodotto che desideri eliminare inserendo delete nella casella di testo, quindi scegli Elimina.

Per i prodotti con risorse associate, continua con il passaggio 4.

4. Nella finestra Elimina prodotto, esamina la tabella Associazioni, che mostra tutte le risorse associate al prodotto. AWS Service Catalog tenta di dissociare queste risorse quando si elimina il prodotto.
5. Conferma di voler eliminare il prodotto e rimuovere tutte le risorse associate inserendo delete nella casella di testo.
6. Scegli Dissocia ed elimina.

Se non AWS Service Catalog è possibile dissociare tutte le risorse del prodotto, il prodotto non viene eliminato. La finestra Elimina prodotto mostra il numero di disassociazioni non riuscite e una descrizione per ogni errore. Per ulteriori informazioni sulla risoluzione delle disassociazioni di risorse non riuscite durante l'eliminazione di un prodotto, vedere Risoluzione delle disassociazioni di risorse non riuscite durante l'eliminazione di un prodotto di seguito.

Argomenti

- [Eliminazione di prodotti utilizzando il AWS CLI](#)
- [Risoluzione delle disassociazioni di risorse non riuscite durante l'eliminazione di un prodotto](#)

Eliminazione di prodotti utilizzando il AWS CLI

AWS Service Catalog ti consente di utilizzare il [AWS Command Line Interface](#)(AWS CLI) per eliminare prodotti dal tuo portafoglio. AWS CLI È uno strumento open source che consente di interagire con i AWS servizi utilizzando i comandi nella shell della riga di comando. La funzione AWS Service Catalog force-delete richiede un [AWS CLI alias](#), che è una scorciatoia che è possibile creare AWS CLI per abbreviare i comandi o gli script che si utilizzano di frequente.

Prerequisiti

- Installa e configura la AWS CLI. [Per ulteriori informazioni, vedere Installazione o aggiornamento della versione più recente di e Nozioni di base sulla configurazione. AWS CLI](#) Usa una AWS CLI versione minima di 1.11.24 o 2.0.0.
- L'alias CLI di eliminazione del prodotto richiede un terminale compatibile con bash e il processore JSON a riga di comando JQ. [Per ulteriori informazioni sull'installazione del processore JSON a riga di comando, consulta Download jq.](#)
- Crea un AWS CLI alias per le chiamate Disassociation API in batch, che ti consente di eliminare un prodotto con un solo comando.

Per eliminare correttamente un prodotto, devi prima dissociare tutte le risorse associate al prodotto. Esempi di associazioni di risorse di prodotto includono associazioni di portafoglio, budget, opzioni di tag e azioni di servizio. Quando si utilizza la CLI per eliminare un prodotto, l'`force-delete-productalias` CLI consente di chiamare l'`DisassociateAPI` per dissociare tutte le risorse che potrebbero impedire l'API. `DeleteProduct` In questo modo si evita una chiamata separata per le disassociazioni individuali.

Note

I percorsi dei file illustrati nelle procedure seguenti possono variare a seconda del sistema operativo utilizzato per eseguire queste azioni.

Creazione di un AWS CLI alias per eliminare i prodotti AWS Service Catalog

Quando si utilizza AWS CLI per eliminare un AWS Service Catalog prodotto, l'`force-delete-productalias` CLI consente di chiamare l'`DisassociateAPI` per dissociare tutte le risorse che potrebbero impedire la chiamata. `DeleteProduct`

Crea un **alias** file nella tua cartella di configurazione AWS CLI

1. Nella AWS CLI console, accedi alla cartella di configurazione. Per impostazione predefinita, il percorso della cartella di configurazione è `~/ .aws/` su Linux e macOS o `%USERPROFILE% \ .aws\` su Windows.
2. Crea una sottocartella denominata `cli` utilizzando la navigazione dei file o inserendo il seguente comando nel tuo terminale preferito:

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

Il percorso predefinito della `cli` cartella risultante è `~/.aws/cli/` su Linux e macOS o `%USERPROFILE%\cli` su Windows.

3. Nella nuova `cli` cartella, create un file di testo denominato `alias` senza estensione. È possibile creare il `alias` file utilizzando la navigazione dei file o inserendo il seguente comando nel terminale preferito:

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

4. Inserisci `[toplevel]` sulla prima riga.
5. Salvare il file.

Successivamente, puoi aggiungere l' `force-delete-productalias` al tuo `alias` file incollando manualmente lo script di `alias` nel file o utilizzando un comando nella finestra del terminale.

Aggiungi manualmente l' `force-delete-productalias` al tuo file **alias**

1. Nella AWS CLI console, accedi alla cartella di AWS CLI configurazione e apri il `alias` file.
2. Inserisci il seguente `alias` di codice nel file, sotto la `[toplevel]` riga:

```
[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. Salvare il file.

Usa la finestra del terminale per aggiungere l' `force-delete-productalias` al tuo file **alias**

1. Apri la finestra del terminale ed esegui il seguente comando

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

2. Incolla lo script di alias nella finestra del terminale, quindi premi CTRL+D per uscire dal comando. `cat`

Chiama l' `force-delete-productalias`

1. Nella finestra del terminale, esegui il comando seguente per richiamare l'alias di eliminazione del prodotto

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

L'esempio seguente mostra il comando `force-delete-product alias` e la risposta risultante

```
$ 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. Inserisci `y` per confermare che desideri eliminare il prodotto.

Dopo aver eliminato con successo il prodotto, la finestra del terminale visualizza i seguenti risultati

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

Risorse aggiuntive

Per ulteriori informazioni sull' AWS CLI utilizzo degli alias e sull'eliminazione AWS Service Catalog dei prodotti, consulta le seguenti risorse:

- [Creazione e utilizzo di AWS CLI alias](#) nella guida per l'AWS Command Line Interface utente (CLI).
- AWS CLI repository di [alias repository git](#).
- [Eliminazione di prodotti. AWS Service Catalog](#)
- [AWS re:Invent 2016: The Effective User on. AWS CLI YouTube](#)

Risoluzione delle disassociazioni di risorse non riuscite durante l'eliminazione di un prodotto

Se il tuo precedente tentativo di [eliminare un prodotto](#) non è riuscito a causa di eccezioni relative alla dissociazione delle risorse, consulta l'elenco delle eccezioni e delle relative risoluzioni riportato di seguito.

Note

Se hai chiuso la finestra Eliminazione dei prodotti prima di ricevere il messaggio di dissociazione delle risorse non riuscita, puoi seguire i passaggi da uno a tre della sezione Elimina un prodotto precedente per aprire nuovamente la finestra.

Per risolvere una disassociazione delle risorse non riuscita

Nella finestra Elimina prodotto, esamina la colonna Stato della tabella Associazioni. Identifica l'eccezione di dissociazione delle risorse non riuscita e le risoluzioni suggerite:

| Tipo di eccezione di stato | Causa | Risoluzione |
|--|---|---|
| Prodotto prod-**** | AWS Service Catalog non è stato possibile eliminare il prodotto perché al prodotto sono ancora associati dei budget TagOptions, almeno uno alle azioni ProvisioningArtifact associate, il prodotto è ancora assegnato a un portfolio, il prodotto ha utenti o il prodotto ha dei vincoli. | Tenta di eliminare nuovamente il prodotto. |
| Utente: non username è autorizzato a eseguire: | L'utente che tenta di eliminare il prodotto non dispone delle autorizzazioni necessari e per dissociare le risorse del prodotto. | AWS Service Catalog consiglia di contattare l'amministratore dell'account per ulteriori informazioni sulla dissociazione delle risorse del prodotto, per le quali attualmente non si dispone delle autorizzazioni necessarie. |

Gestione delle versioni

Quando si crea un prodotto, è possibile assegnare le versioni del prodotto e aggiornarle in qualsiasi momento.

Le versioni hanno un CloudFormation modello, un titolo, una descrizione, uno stato e una guida.

Stato della versione

Una versione può avere uno dei tre stati:

- **Attiva** - Una versione attiva viene visualizzata nell'elenco delle versioni e consente agli utenti di avviarla.
- **Inattiva** - Una versione inattiva è nascosta nell'elenco delle versioni. I prodotti con provisioning esistenti lanciati da questa versione non saranno interessati.
- **Eliminata**: una versione eliminata viene rimossa dall'elenco delle versioni. L'eliminazione di una versione non può essere annullata.

Indicazioni sulla versione

È possibile impostare le indicazioni sulla versione per fornire informazioni agli utenti finali sulla versione del prodotto. Le indicazioni sulla versione riguardano solo le versioni attive del prodotto.

Ci sono due opzioni per le indicazioni sulla versione:

- **Nessuna**: per impostazione predefinita, le versioni del prodotto non dispongono di alcuna guida. Gli utenti finali possono utilizzare tale versione per aggiornare e lanciare i prodotti forniti.
- **Obsoleto**: gli utenti non possono lanciare nuovi prodotti forniti utilizzando una versione del prodotto obsoleta. Se un prodotto con provisioning p lanciato in precedenza utilizza una versione ormai obsoleta, gli utenti possono aggiornare quel prodotto fornito solo utilizzando la versione esistente o una nuova versione.

Aggiornamento delle versioni

Quando si crea un prodotto, si assegnano le versioni del prodotto e si può anche aggiornare una versione in qualsiasi momento. Per ulteriori informazioni sulla creazione di un prodotto, consultare [Creazione di prodotti](#).

Per aggiornare la versione di un prodotto

1. Nella console, scegli Prodotti. AWS Service Catalog
2. Dall'elenco dei prodotti, scegliere il prodotto di cui si desidera aggiornare la versione.
3. Nella pagina Product details (Dettagli prodotto) scegliere la scheda Versions (Versioni), quindi scegliere la versione che desideri aggiornare.
4. Nella pagina Version details (Dettagli versione) modificare la versione del prodotto, quindi scegliere Save changes (Salva modifiche).

Utilizzo dei AWS Service Catalog vincoli

Applica vincoli per controllare le regole applicate a un prodotto in un portafoglio specifico quando gli utenti finali lo avviano. Quando gli utenti finali avviano il prodotto, vedranno le regole applicate utilizzando i vincoli. Puoi applicare vincoli a un prodotto una volta inserito in un portafoglio. I vincoli sono attivi non appena li crei e vengono applicati a tutte le versioni correnti di un prodotto che non sono state lanciate.

Vincoli

- [AWS Service Catalog Vincoli di avvio](#)
- [AWS Service Catalog Vincoli di notifica](#)
- [AWS Service Catalog Vincoli di aggiornamento dei tag](#)
- [AWS Service Catalog Vincoli Stack Set](#)
- [AWS Service Catalog Vincoli del modello](#)

AWS Service Catalog Vincoli di avvio

Un vincolo di lancio specifica il ruolo AWS Identity and Access Management (IAM) da AWS Service Catalog assumere quando un utente finale avvia, aggiorna o chiude un prodotto. Un ruolo IAM è una raccolta di autorizzazioni che un utente o un servizio può assumere temporaneamente per utilizzare i AWS servizi. AWS Per un esempio introduttivo, vedi:

- CloudFormation tipo di prodotto: [Passaggio 6: aggiungere un vincolo di avvio per assegnare un ruolo IAM](#)
- Tipo di prodotto Terraform Open Source o Terraform Cloud: [Fase 5: Creare ruoli di lancio](#)

I vincoli di lancio si applicano ai prodotti del portafoglio (associazione prodotto-portafoglio). I vincoli di lancio non si applicano a livello di portafoglio o a un prodotto in tutti i portafogli. Per associare un vincolo di avvio a tutti i prodotti in un portafoglio, devi applicare il vincolo di avvio a ogni prodotto individualmente.

Senza vincoli di lancio, gli utenti finali devono lanciare e gestire i prodotti utilizzando le proprie credenziali IAM. A tal fine, devono disporre delle autorizzazioni per AWS i servizi CloudFormation utilizzati dai prodotti e. AWS Service Catalog Utilizzando un ruolo di avvio, puoi invece limitare le autorizzazioni degli utenti finali al minimo richiesto per quel prodotto. Per ulteriori informazioni sulle autorizzazioni per utenti finali, consulta [Identity and Access Management in AWS Service Catalog](#).

Per creare e assegnare ruoli IAM, devi disporre delle seguenti autorizzazioni amministrative IAM:

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

Configurazione di un ruolo di avvio

Il ruolo IAM che assegna a un prodotto come vincolo di lancio deve disporre delle autorizzazioni per utilizzare quanto segue:

Per i prodotti Cloudformation

- La policy gestita di `arn:aws:iam::aws:policy/AWSCloudFormationFullAccess` CloudFormation
- Servizi inclusi nel AWS CloudFormation modello del prodotto
- Accesso in lettura al AWS CloudFormation modello in un bucket Amazon S3 di proprietà del servizio.

Per i prodotti Terraform

- Servizi nel modello Amazon S3 per il prodotto
- Accesso in lettura al modello Amazon S3 in un bucket Amazon S3 di proprietà del servizio.

- `resource-groups:Tagger` per il tagging in un'istanza Amazon EC2 (assunto dal motore di provisioning Terraform durante l'esecuzione delle operazioni di provisioning)
- `resource-groups:CreateGroup` per l'etichettatura dei gruppi di risorse (presupposto per creare gruppi di risorse e AWS Service Catalog assegnare tag)

La politica di fiducia del ruolo IAM deve consentire di AWS Service Catalog assumere il ruolo. Nella procedura riportata di seguito, la politica di fiducia verrà impostata automaticamente quando si seleziona AWS Service Catalog come tipo di ruolo. Se non utilizzi la console, consulta la sezione [Creazione di politiche di fiducia per AWS i servizi che assumono ruoli in Come usare le politiche di fiducia con i ruoli IAM](#).

Note

Le autorizzazioni `servicecatalog:ProvisionProduct`, `servicecatalog:TerminateProvisionedProduct` e `servicecatalog:UpdateProvisionedProduct` non possono essere assegnate in un ruolo di avvio. È necessario utilizzare i ruoli IAM, come illustrato nei passaggi delle policy in linea nella sezione [Concedere autorizzazioni agli utenti AWS Service Catalog finali](#).

Note

Per visualizzare i prodotti e le risorse CloudFormation forniti nella AWS Service Catalog console, gli utenti finali devono avere accesso in lettura. CloudFormation La visualizzazione dei prodotti e delle risorse forniti nella console non utilizza il ruolo di avvio.

Creazione di un ruolo di avvio

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.

I prodotti Terraform richiedono configurazioni aggiuntive dei ruoli di lancio. Per ulteriori informazioni, consulta la [Fase 5: Creare ruoli di lancio](#) in Getting Started with a Terraform Open Source.

2. Scegli Ruoli.
3. Scegli Crea nuovo ruolo.
4. Immettere un nome di ruolo e scegliere Next Step (Fase successiva).

5. In Ruoli AWS di servizio accanto a AWS Service Catalog, scegli **Seleziona**.
6. Nella pagina **Attach Policy (Associa policy)**, scegliere **Next Step (Fase successiva)**.
7. Per creare il ruolo, scegliere **Create Role (Crea ruolo)**.

Associazione di una policy a un nuovo ruolo

1. Scegli il ruolo che hai creato per visualizzare la pagina dei dettagli del ruolo.
2. Scegliere la scheda **Permissions (Autorizzazioni)** ed espandere la sezione **Inline Policies (Policy inline)**. Quindi, scegliere **click here (fai clic qui)**.
3. Scegliere **Custom Policy (Policy personalizzata)** quindi **Select (Seleziona)**.
4. Immettere un nome per la policy, quindi incollare quanto segue nell'editor **Policy Document (Documento policy)**:

```

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

```

Note

Quando configuri un ruolo di avvio per un vincolo di avvio, devi usare questa stringa:
"s3:ExistingObjectTag/servicecatalog:provisioning":"true"

5. Aggiungi una riga alla politica per ogni servizio aggiuntivo utilizzato dal prodotto. Ad esempio, per aggiungere l'autorizzazione per Amazon Relational Database Service (Amazon RDS), inserisci una virgola alla fine dell'ultima riga **Action** dell'elenco, quindi aggiungi la seguente riga:

```
"rds:*"
```

6. Scegli Apply Policy (Applica policy).

Applicazione di un vincolo di avvio

Dopo aver configurato il ruolo di lancio, assegna il ruolo al prodotto come vincolo di lancio. Questa azione indica AWS Service Catalog di assumere il ruolo quando un utente finale avvia il prodotto.

Assegnazione del ruolo a un prodotto

1. Aprire la console Service Catalog all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Scegliere il portafoglio che contiene il prodotto.
3. Scegliere la scheda Vincoli, quindi Crea vincolo.
4. Scegliere il prodotto da Product (Prodotto), quindi scegliere Launch (Avvia) sotto Constraint type (Tipo di vincolo). Scegli Continua.
5. Nella sezione Launch constraint, puoi selezionare un ruolo IAM dal tuo account e inserire un ARN del ruolo IAM oppure inserire il nome del ruolo.

Se specifichi il nome del ruolo e se un account utilizza il vincolo di avvio, l'account utilizza quel nome per il ruolo IAM. Questo approccio consente ai vincoli del ruolo di avvio di essere indipendenti dall'account, in modo da poter creare meno risorse per account condiviso.

Note

Il nome del ruolo specificato deve esistere nell'account che ha creato il vincolo di avvio e nell'account dell'utente che lancia un prodotto con questo vincolo di avvio.

6. Dopo aver specificato il ruolo IAM, scegliere Crea.

Aggiungere Confused Deputy a Launch Constraint

AWS Service Catalog supporta la protezione [Confused Deputy](#) per API che vengono eseguiti con una richiesta Assume Role. Quando aggiungi un vincolo di avvio, puoi limitare l'accesso al ruolo di lancio utilizzando `sourceArn` le condizioni contenute nella `sourceAccount` policy di fiducia del ruolo di avvio. Garantisce che il ruolo di lancio venga richiamato da una fonte attendibile.

Nell'esempio seguente, l' AWS Service Catalog utente finale appartiene all'account 1111. Quando l' AWS Service Catalog amministratore crea un ruolo LaunchConstraint per un prodotto, l'utente finale può specificare le seguenti condizioni nella politica di fiducia del ruolo di avvio per limitare il ruolo di assunzione all'account 1111.

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

Un utente che fornisce a un prodotto il LaunchConstraint deve avere lo stesso AccountId (1111). In caso contrario, l'operazione fallisce con un AccessDenied errore, che impedisce l'uso improprio del ruolo di avvio.

Quanto segue AWS Service Catalog APIs è protetto dalla protezione di Confused Deputy:

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

La sourceArn protezione supporta AWS Service Catalog solo modelli ARNs, come "arn:<aws-partition>:servicecatalog:<region>:<accountId>:". Non supporta risorse specifiche. ARNs

Verifica del vincolo di avvio

Per verificare AWS Service Catalog utilizzi il ruolo per avviare il prodotto ed effettuare correttamente il provisioning del prodotto, avvia il prodotto dalla console. AWS Service Catalog Per testare un vincolo

prima della distribuzione agli utenti, crea un portafoglio di prova che contiene gli stessi prodotti e verifica i vincoli con quel portafoglio.

Avvio del prodotto

1. Nel menu della AWS Service Catalog console, scegli Service Catalog, Utente finale.
2. Scegli il prodotto per aprire la pagina dei dettagli del prodotto. Nella tabella delle opzioni di avvio, verifica che venga visualizzato l'Amazon Resource Name (ARN) del ruolo.
3. Scegli Launch product.
4. Esegui le fasi relative all'avvio, indicando le informazioni richieste.
5. Verifica che il prodotto venga avviato senza problemi.

AWS Service Catalog Vincoli di notifica

Note

AWS Service Catalog non supporta i vincoli di notifica per i prodotti Terraform Open Source o Terraform Cloud.

Un vincolo di notifica specifica un argomento di Amazon SNS per ricevere notifiche sugli eventi dello stack.

Utilizza la procedura seguente per creare un argomento di SNS e abbonarti allo stesso.

Creazione di un argomento di SNS e di un abbonamento

1. [Apri la console Amazon SNS nella versione v3/home. https://console.aws.amazon.com/sns/](https://console.aws.amazon.com/sns/)
2. Scegli Create topic (Crea argomento).
3. Digitare un nome di argomento, quindi scegliere Create topic (Crea argomento).
4. Scegli Create Subscription (Crea sottoscrizione).
5. Per Protocol (Protocollo), selezionare Email (E-mail). Per Endpoint, digitare l'indirizzo e-mail a cui devono essere inviate le notifiche. Scegli Create Subscription (Crea sottoscrizione).
6. Riceverai un'e-mail di conferma con l'oggetto AWS Notification - Subscription Confirmation. Apri l'e-mail e segui le istruzioni per completare l'iscrizione.

Utilizza la procedura seguente per applicare un vincolo di notifica utilizzando l'argomento di SNS creato nella procedura precedente.

Applicazione di un vincolo di notifica a un prodotto

1. Aprire la console Service Catalog all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Scegliere il portafoglio che contiene il prodotto.
3. Espandere Constraints (Vincoli) e scegliere Add constraints (Aggiungi vincoli).
4. Scegli il prodotto da Prodotto e imposta il tipo di vincolo su Notifica. Scegli Continua.
5. Scegliere Choose a topic from your account (Scegli un argomento dal tuo account) e selezionare l'argomento di SNS creato in Topic Name (Nome argomento).
6. Seleziona Invia.

AWS Service Catalog Vincoli di aggiornamento dei tag

Note

AWS Service Catalog non supporta i vincoli di aggiornamento dei tag per i prodotti Terraform Open Source.

Con i vincoli di aggiornamento dei tag, AWS Service Catalog gli amministratori possono consentire o impedire agli utenti finali di aggiornare i tag sulle risorse associate a un prodotto fornito. Se l'aggiornamento dei tag è consentito, i nuovi tag associati al prodotto o al portafoglio verranno applicati alle risorse assegnate durante un aggiornamento del prodotto fornito.

Per abilitare gli aggiornamenti di tag per un prodotto

1. Aprire la console Service Catalog all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Scegli il portfolio che contiene il prodotto che desideri aggiornare.
3. Scegli la scheda Vincoli e scegli Aggiungi vincoli.
4. In Constraint type (Tipo di vincolo), scegli Tag Update (Aggiornamento tag).
5. Scegli il prodotto da Product (Prodotto), quindi scegli Continue (Continua).
6. Nella pagina Tag Updates (Aggiornamenti tag), seleziona Enable Tag Updates (Abilita aggiornamenti tag).
7. Seleziona Invia.

AWS Service Catalog Vincoli Stack Set

Note

- AWS Service Catalog non supporta i vincoli dello stack set per i prodotti Terraform Open Source.
- AutoTags non sono attualmente supportati con CloudFormation StackSets

Un vincolo di stack set consente di configurare le opzioni di distribuzione del prodotto utilizzando CloudFormation StackSets. Puoi specificare più account e regioni per il lancio del prodotto. Gli utenti finali possono gestire tali account e determinare dove distribuire i prodotti e l'ordine di distribuzione.

Per applicare un vincolo di set di stack a un prodotto

1. Aprire la console Service Catalog all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Scegli il portafoglio con il prodotto che desideri.
3. Scegli la scheda Vincoli, quindi scegli Crea vincoli.
4. In Prodotto, scegli il prodotto. In Tipo di vincolo, scegli Stack Set.
5. Configura gli account, le regioni e le autorizzazioni per i vincoli dello stack set.
 - Nelle impostazioni dell'account, identifica gli account in cui desideri creare prodotti.
 - Nelle impostazioni della regione, scegli le aree geografiche in cui distribuire i prodotti e l'ordine in cui desideri che tali prodotti vengano distribuiti in tali regioni.
 - In Autorizzazioni, scegli un ruolo di StackSet amministratore IAM per gestire gli account di destinazione. Se non scegli un ruolo, StackSets utilizza l'ARN predefinito. [Ulteriori informazioni sull'impostazione delle autorizzazioni dei set di stack.](#)
6. Scegli Create (Crea).

AWS Service Catalog Vincoli del modello

Note

AWS Service Catalog non supporta i vincoli dei modelli per i prodotti Terraform Open Source o Terraform Cloud.

Per limitare le opzioni disponibili per gli utenti finali quando avviano un prodotto, devi applicare vincoli di modello. L'applicazione di tali vincoli consente agli utenti finali di utilizzare i prodotti senza violare i requisiti di conformità della tua organizzazione. Si applicano i vincoli del modello a un prodotto in un portafoglio. AWS Service Catalog Un portafoglio deve contenere uno o più prodotti affinché sia possibile definire vincoli di modello.

Un vincolo del modello è costituito da una o più regole che limitano i valori consentiti per i parametri definiti nel modello sottostante del prodotto. CloudFormation I parametri in un modello di CloudFormation definiscono il set di valori che gli utenti possono specificare durante la creazione di uno stack. Ad esempio, un parametro potrebbe definire i vari tipi di istanze tra cui gli utenti possono scegliere quando avviano uno stack che include istanze. EC2

Se il set di valori di parametro in un modello è troppo ampio per i destinatari del tuo portafoglio, puoi definire vincoli di modello per limitare i valori che gli utenti possono scegliere all'avvio di un prodotto. Ad esempio, se i parametri del modello includono tipi di EC2 istanza troppo grandi per gli utenti che dovrebbero utilizzare solo tipi di istanze di piccole dimensioni (come `t2.micro` o `t2.small`), puoi aggiungere un vincolo di modello per limitare i tipi di istanza che gli utenti finali possono scegliere. Per ulteriori informazioni sui parametri CloudFormation del modello, consulta [Parametri nella Guida](#) per l'CloudFormation utente.

I vincoli di modello sono associati in un portafoglio. Se applichi vincoli di modello a un prodotto in un portafoglio e quindi includi il prodotto in un altro portafoglio, i vincoli non verranno applicati al prodotto nel secondo portafoglio.

Se applichi un vincolo di modello a un prodotto che è già stato condiviso con gli utenti, il vincolo è immediatamente attivo per tutti gli avvii successivi del prodotto e per tutte le versioni del prodotto nel portafoglio.

È possibile definire le regole di vincolo del modello utilizzando un editor di regole o scrivendo le regole come testo JSON nella AWS Service Catalog console di amministrazione. Per ulteriori informazioni sulle regole, tra cui sintassi ed esempi, consulta [Regole di vincolo di modello](#).

Per testare un vincolo prima della distribuzione agli utenti, crea un portafoglio di prova che contiene gli stessi prodotti e verifica i vincoli con quel portafoglio.

Applicazione di vincoli di modello a un prodotto

1. Aprire la console Service Catalog all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Nella pagina Portafogli, scegli il portfolio che contiene il prodotto a cui desideri applicare un vincolo relativo al modello.

3. Espandi la sezione Vincoli e scegli Aggiungi vincoli.
4. Nella finestra Seleziona prodotto e tipo, per Prodotto scegli il prodotto per il quale desideri definire i vincoli del modello. Quindi, per Tipo di vincolo, scegli Modello. Scegli Continua.
5. Nella pagina Template Constraint Builder, modifica le regole di vincolo utilizzando l'editor JSON o l'interfaccia del generatore di regole.
 - Per modificare il codice JSON per la regola, scegli la scheda Constraint Text Editor. In questa scheda sono disponibili vari esempi per aiutarti a iniziare.

Per creare le regole utilizzando un'interfaccia per la creazione di regole, scegli la scheda Rule Builder. In questa scheda, puoi scegliere qualsiasi parametro specificato nel modello per il prodotto, nonché specificare i valori autorizzati per quel parametro. A seconda del tipo di parametro, devi specificare i valori consentiti selezionando elementi in un elenco di controllo, indicando un numero o specificando un set di valori in un elenco separato da virgole.

Quando hai finito di creare una regola, scegli Aggiungi regola. La regola viene visualizzata nella tabella della scheda Rule Builder. Per rivedere e modificare l'output JSON, scegli la scheda Constraint Text Editor.

6. Quando hai finito di modificare le regole per il tuo vincolo, scegli Invia. Per visualizzare il vincolo, vai alla pagina dei dettagli del portfolio ed espandi Vincoli.

Regole di vincolo di modello

Le regole che definiscono i vincoli del modello in un AWS Service Catalog portfolio descrivono quando gli utenti finali possono utilizzare il modello e quali valori possono specificare per i parametri dichiarati nel CloudFormation modello utilizzato per creare il prodotto che stanno tentando di utilizzare. Le regole sono utili per impedire agli utenti finali di specificare inavvertitamente un valore non corretto. Ad esempio, puoi aggiungere una regola per verificare se gli utenti finali hanno specificato una sottorete valida in un determinato VPC o hanno m1.small utilizzato tipi di istanza per ambienti di test. CloudFormation utilizza regole per convalidare i valori dei parametri prima di creare le risorse per il prodotto.

Ogni regola è costituita da due proprietà: una condizione di regola (facoltativa) e asserzioni (obbligatorie). La condizione di regola determina quando una regola viene attivata. Le asserzioni descrivono quali valori gli utenti possono specificare per un particolare parametro. Se non definisci una condizione di regola, le asserzioni della regola sono sempre attivate. Per definire una condizione e asserzioni di regola, devi utilizzare funzioni intrinseche specifiche delle regole, ovvero funzioni che

possono essere utilizzate solo nella sezione `Rules` di un modello. È possibile nidificare le funzioni, ma il risultato finale di una condizione o di un'asserzione di regola deve essere `true` o `false`.

Supponiamo, ad esempio, che hai dichiarato un VPC e un parametro di sottorete nella sezione `Parameters`. Puoi creare una regola che verifica che una data sottorete si trova in un determinato VPC. Pertanto, quando un utente specifica un VPC CloudFormation, valuta l'asserzione per verificare se il valore del parametro di sottorete si trova in quel VPC prima di creare o aggiornare lo stack. Se il valore del parametro non è valido, non riesci CloudFormation immediatamente a creare o aggiornare lo stack. Se gli utenti non specificano un VPC, CloudFormation non controlla il valore del parametro della sottorete.

Sintassi

La sezione `Rules` di un modello comporta il nome di chiave `Rules`, seguito da un segno di due punti. Tutte le dichiarazioni di regola sono racchiuse tra parentesi graffe. Se dichiari più regole, queste sono delimitate da virgole. Per ogni regola, dichiarare un nome logico tra virgolette seguito da un segno di due punti e parentesi graffe che racchiudono la condizione e le asserzioni di regola.

Una regola può includere una proprietà `RuleCondition` e deve includere una proprietà `Assertions`. Per ogni regola, puoi definire una sola condizione di regola nonché una o più asserzioni nella proprietà `Assertions`. Per definire una condizione e asserzioni di regola, si utilizzano funzioni intrinseche specifiche delle regole, come mostrato nello pseudo-modello seguente:

```
"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"
      }
    ]
  }
}

```

Il pseudomodello mostra una sezione `Rules` contenente due regole denominate `Rule01` e `Rule02`. `Rule01` include una condizione di regola e due asserzioni. Se la funzione nella condizione di regola restituisce `true`, entrambe le funzioni in ogni asserzione vengono valutate e applicate. Se la condizione di regola è falsa, la regola non viene applicata. `Rule02` diventa sempre effettiva perché non ha una condizione di regola, il che significa che la singola istruzione `Assert` viene sempre valutata e applicata.

[Per informazioni sulle funzioni intrinseche specifiche delle regole per definire le condizioni e le asserzioni delle regole, consulta *AWS Rule Functions* nella Guida per l'utente.](#)[AWS CloudFormation](#)

Esempio: verifica condizionale di un valore di parametro

Le due regole seguenti verificano il valore del parametro `InstanceType`. A seconda del valore del parametro `Environment` (`test` o `prod`), l'utente deve specificare `m1.small` o `m1.large` per il parametro `InstanceType`. I parametri `InstanceType` e `Environment` devono essere dichiarati nella sezione `Parameters` dello stesso modello.

```

"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 Azioni di servizio

Note

AWS Service Catalog non supporta azioni di servizio per i prodotti Terraform Open Source o Terraform Cloud.

AWS Service Catalog consente di ridurre la manutenzione amministrativa e la formazione degli utenti finali rispettando al contempo le misure di conformità e sicurezza. Con le operazioni di servizio, come amministratore puoi consentire agli utenti finali di eseguire attività operative, risolvere problemi, eseguire comandi approvati oppure richiedere le autorizzazioni in AWS Service Catalog. È possibile utilizzare i [documenti AWS Systems Manager](#) per definire le operazioni di servizio. I [AWS Systems Manager documenti](#) forniscono l'accesso ad azioni predefinite che implementano le AWS migliori pratiche, come l'arresto e il riavvio di Amazon EC2, e puoi anche definire azioni personalizzate.

In questo tutorial, offri agli utenti finali la possibilità di riavviare un'istanza Amazon EC2. Aggiungi le autorizzazioni necessarie, definisci l'operazione di servizio, associ l'operazione di servizio con un prodotto e testi l'esperienza dell'utente finale utilizzando l'operazione con un prodotto per il quale è stato effettuato il provisioning.

Prerequisiti

Questo tutorial presuppone che tu disponga delle autorizzazioni di AWS amministratore complete, che tu conosca già e che disponga già di un set base di prodotti, portafogli e utenti. AWS Service Catalog Se non lo conosci AWS Service Catalog, completa la sezione [Configurazione](#) e le [Nozioni di base](#) attività prima di utilizzare questo tutorial.

Argomenti

- [Fase 1: configurazione delle autorizzazioni degli utenti finali](#)
- [Fase 2: creazione di un'operazione di servizio](#)
- [Fase 3: associare l'operazione di servizio a una versione del prodotto](#)
- [Fase 4. Test dell'esperienza dell'utente finale](#)
- [Fase 5: Gestione delle azioni di servizio con AWS CloudFormation](#)
- [Fase 6: Risoluzione dei problemi](#)

Fase 1: configurazione delle autorizzazioni degli utenti finali

Gli utenti finali devono disporre delle autorizzazioni necessarie per visualizzare ed eseguire azioni di servizio specifiche. In questo esempio, l'utente finale necessita dell'autorizzazione per accedere alla funzionalità delle azioni di AWS Service Catalog servizio e per eseguire un riavvio di Amazon EC2.

Per aggiornare le autorizzazioni

1. Apri la console AWS Identity and Access Management (IAM) all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Dal menu, individua i gruppi di utenti.
3. Scegli i gruppi che gli utenti finali utilizzeranno per accedere alle AWS Service Catalog risorse. In questo esempio, viene selezionato il gruppo di utenti finali. Nella propria implementazione, selezionare il gruppo utilizzato dagli utenti finali rilevanti.
4. Nella scheda Autorizzazioni della pagina dettagli del gruppo, creare una nuova policy o modificare una policy esistente. In questo esempio, aggiungiamo le autorizzazioni alla politica esistente selezionando la politica personalizzata creata per le autorizzazioni AWS Service Catalog Provision e Terminate del gruppo.
5. Nella pagina Policy, selezionare Edit Policy (Modifica Policy) per aggiungere le autorizzazioni necessarie. È possibile utilizzare l'editor visivo o l'editor JSON per modificare la policy. In questo esempio, si utilizza l'editor JSON per aggiungere le autorizzazioni. Per questo tutorial, aggiungere le seguenti autorizzazioni alla policy:

JSON

```
{
```

```
"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. Dopo aver modificato la policy, esaminare e approvare la modifica alla policy. Gli utenti del gruppo di utenti finali dispongono ora delle autorizzazioni necessarie per eseguire l'azione di riavvio di Amazon EC2 in AWS Service Catalog

Fase 2: creazione di un'operazione di servizio

Successivamente, crei un'azione di servizio per riavviare le istanze Amazon EC2.

1. Apri la AWS Service Catalog console all'indirizzo. <https://console.aws.amazon.com/sc/>
2. Dal menu, selezionare Service actions (Operazioni di servizio).
3. Nella pagina Azioni di servizio, scegli Crea azione.
4. Nella pagina Crea azione, scegli un AWS Systems Manager documento per definire l'azione di servizio. L'azione di riavvio delle istanze Amazon EC2 è definita da un AWS Systems Manager documento, quindi manteniamo l'opzione predefinita nel menu a discesa, Amazon documents.
5. Cerca e scegli l'azione AWS EC2-Restart Instance.

6. Fornire un nome e una descrizione per l'operazione adatta all'ambiente e al team. L'utente finale vedrà questa descrizione, quindi è consigliabile selezionare qualcosa che lo aiuta a capire cosa fa l'operazione.
7. In Configurazione dei parametri e della destinazione, scegli il parametro del documento SSM che sarà la destinazione dell'azione (ad esempio, l'ID dell'istanza) e scegli la destinazione del parametro. Scegliere Add parameter (Aggiungi parametro) per aggiungere ulteriori parametri.
8. In Permissions (Autorizzazioni), scegliere un ruolo. Stiamo usando le autorizzazioni predefinite per questo esempio. Altre configurazioni di autorizzazione sono possibili e sono definite in questa pagina.
9. Dopo aver esaminato la configurazione, selezionare Create action (Crea operazione).
10. Nella pagina successiva, viene visualizzata una conferma quando l'operazione è stata creata ed è pronta per l'uso.

Fase 3: associare l'operazione di servizio a una versione del prodotto

Dopo aver definito un'operazione, devi associare un prodotto con quell'operazione.

1. Nella pagina Azioni di servizio, scegli AWS-Restart EC2instance, quindi scegli Associa azione.
2. Nella pagina Associate action (Associa operazione), selezionare il prodotto sul quale si desidera che gli utenti finali utilizzino l'operazione di servizio. In questo esempio, si seleziona Linux Desktop (Desktop Linux).
3. Selezionare una versione di prodotto. Notare che è possibile utilizzare la casella di controllo in alto per selezionare tutte le versioni.
4. Selezionare Associate action (Associa operazione).
5. Nella pagina successiva, viene visualizzato un messaggio di conferma.

È stata creata l'operazione di servizio in AWS Service Catalog. Il prossimo passaggio di questo tutorial è di utilizzare l'operazione di servizio come utente finale.

Fase 4. Test dell'esperienza dell'utente finale

Gli utenti finali possono eseguire operazioni di servizio sui prodotti sui quali è stato effettuato il provisioning. Ai fini di questo tutorial, l'utente finale deve avere almeno un prodotto sul quale è stato effettuato il provisioning. Il prodotto per cui è stato effettuato il provisioning deve essere avviato dalla versione del prodotto associata all'operazione di servizio nella fase precedente.

Per accedere all'operazione di servizio come utente finale

1. Accedi alla AWS Service Catalog console come utente finale.
2. Nella AWS Service Catalog dashboard, nel riquadro di navigazione, scegli Elenco di prodotti Provisioned. L'elenco mostra i prodotti per i quali è stato effettuato il provisioning per l'account dell'utente finale.
3. Nella pagina Provisioned products list (Elenco dei prodotti con provisioning), selezionare l'istanza per la quale è stato effettuato il provisioning.
4. Nella pagina dei dettagli del prodotto Provisioned, scegli Azioni in alto a destra, quindi scegli l'azione AWS EC2instance-Restart.
5. Confermare che si desidera eseguire l'operazione personalizzata. Si riceve conferma che l'operazione è stata inviata.

Fase 5: Gestione delle azioni di servizio con AWS CloudFormation

È possibile creare azioni di servizio e le relative associazioni con AWS CloudFormation le risorse. Per ulteriori informazioni, consultare gli argomenti seguenti nella Guida per l'utente di AWS CloudFormation :

- [AWS::ServiceCatalog::CloudFormationProduct ProvisioningArtifactProperties](#)
- [AWS::ServiceCatalog::ServiceActionAssociazione](#)

Note

Se gestisci le associazioni delle azioni di servizio con CloudFormation le risorse, non aggiungere o rimuovere azioni di servizio tramite AWS Command Line Interface o Console di gestione AWS. Quando esegui un aggiornamento dello stack, tutte le modifiche alle azioni del servizio apportate all'esterno vengono CloudFormation sostituite.

Fase 6: Risoluzione dei problemi

Se l'esecuzione dell'azione del servizio ha esito negativo, è possibile trovare il messaggio di errore nella sezione Output dell'evento di esecuzione dell'azione del servizio nella pagina Prodotto con provisioning. Di seguito puoi vedere le spiegazioni per i messaggi di errore comuni che potresti trovare.

Note

Il testo esatto del messaggio di errore è soggetto a modifiche, quindi dovresti evitare di utilizzarli in qualsiasi tipo di processo automatizzato.

Errore interno

AWS Service Catalog si è verificato un errore interno. Riprova più tardi. Se il problema persiste, contattare il supporto clienti.

Si è verificato un errore (ThrottlingException) durante la chiamata dell' StartAutomationExecution operazione

L'esecuzione dell'azione di servizio è stata limitata dal servizio di backend, ad esempio SSM.

Accesso negato assumendo il ruolo

AWS Service Catalog non è stato in grado di assumere il ruolo specificato nella definizione dell'azione del servizio. Assicurati che il principale servicecatalog.amazonaws.com o un principale regionale come servicecatalog.us-east-1.amazonaws.com sia inserito nella politica di attendibilità del ruolo.

Si è verificato un errore (AccessDeniedException) durante la chiamata dell' StartAutomationExecution operazione: L'utente non è autorizzato a eseguire: ssm: sulla risorsa. StartAutomationExecution

Il ruolo specificato nella definizione dell'azione di servizio non dispone delle autorizzazioni per richiamare ssm:. StartAutomationExecution Assicurati che il ruolo disponga delle autorizzazioni SSM appropriate.

Impossibile trovare risorse con il tipo di prodotto *TargetType* fornito

Il prodotto fornito non contiene risorse che corrispondano al tipo di destinazione specificato nel documento SSM, ad esempio: :EC2 AWS: :Instance. Verificare che il prodotto sottoposto a provisioning presenti queste risorse o verificare che il documento sia corretto.

Il documento con quel nome non esiste

Il documento specificato nella definizione dell'azione di servizio non esiste.

Impossibile descrivere il documento di Automazione SSM non riuscita

AWS Service Catalog ha riscontrato un'eccezione sconosciuta da SSM durante il tentativo di descrivere il documento specificato.

Impossibile recuperare le credenziali per il ruolo

AWS Service Catalog ha riscontrato un errore sconosciuto nell'assumere il ruolo specificato.

Il parametro ha un valore "**InvalidValue**" non trovato in **{ValidValue1}, {ValidValue2}**

Il valore del parametro passato a SSM non è nell'elenco dei valori consentiti per il documento. Verificare che i parametri forniti siano validi e riprovare.

Errore nel tipo di parametro. Il valore fornito per non **ParameterName** è una stringa valida.

Il valore del parametro passato a SSM non è valido per il tipo del documento.

Il parametro non è definito nella definizione dell'operazione del servizio

È stato passato un parametro non definito nella definizione dell'azione di servizio. AWS Service Catalog È possibile utilizzare solo i parametri definiti nella definizione dell'operazione del servizio.

Il passaggio fallisce quando si tratta di executing/canceling un'azione. **Error message**. Per ulteriori dettagli sulla diagnosi, fare riferimento alla Guida alla risoluzione dei problemi del servizio di automazione.

Un passaggio del documento di automazione SSM non è riuscito. Vedere l'errore nel messaggio per risolvere ulteriormente i problemi.

I seguenti valori per il parametro non sono consentiti perché non sono presenti nel prodotto fornito:
InvalidResourceId

L'utente ha richiesto un'azione su una risorsa non presente nel prodotto di cui è stato eseguito il provisioning.

TargetType non definito per il documento SSM Automation

Le azioni di servizio richiedono che i documenti di automazione SSM abbiano un TargetType documento definito. Controlla il tuo documento di automazione SSM.

Aggiungere Marketplace AWS prodotti al tuo portafoglio

Puoi aggiungere Marketplace AWS prodotti ai tuoi portafogli per renderli disponibili ai tuoi utenti AWS Service Catalog finali.

Marketplace AWS è un negozio online in cui puoi trovare, abbonarti e iniziare subito a utilizzare un'ampia selezione di software e servizi. I tipi di prodotti Marketplace AWS includono database, server di applicazioni, strumenti di test, strumenti di monitoraggio, strumenti di gestione dei contenuti e software di business intelligence. Marketplace AWS è disponibile all'indirizzo <https://aws.amazon.com/marketplace>. Tieni presente che non puoi aggiungere prodotti Software as a Service (SaaS) da Marketplace AWS. AWS Service Catalog

Puoi distribuire un Marketplace AWS prodotto agli utenti AWS Service Catalog finali copiando il prodotto con il CloudFormation modello in AWS Service Catalog e quindi aggiungendolo a un portfolio.

Note

AWS Service Catalog non supporta la distribuzione di Marketplace AWS prodotti agli utenti AWS Service Catalog finali utilizzando un modello di prodotto Terraform Open Source o Terraform Cloud.

Marketplace AWS supporta AWS Service Catalog direttamente o abbonati e aggiungi prodotti utilizzando l'opzione manuale. Consigliamo di aggiungere prodotti utilizzando la funzionalità appositamente progettata per AWS Service Catalog.

Gestione dei Marketplace AWS prodotti utilizzando AWS Service Catalog

Puoi aggiungere i Marketplace AWS prodotti sottoscritti direttamente AWS Service Catalog utilizzando un'interfaccia personalizzata. In [Marketplace AWS](#), seleziona Service Catalog. Per ulteriori informazioni, consulta [Copiare i prodotti](#) nella Marketplace AWS Guida e AWS Service Catalog nelle domande frequenti.

Gestione e aggiunta manuale Marketplace AWS dei prodotti

Completa i seguenti passaggi per abbonarti a un Marketplace AWS prodotto, definire quel prodotto in un CloudFormation modello e aggiungere il modello a un AWS Service Catalog portfolio.

Per abbonarsi a un Marketplace AWS prodotto

1. Vai Marketplace AWS a <https://aws.amazon.com/marketplace>.
2. Sfoglia i prodotti o cerca quello che vuoi aggiungere al tuo portafoglio di AWS Service Catalog. Scegli il prodotto per visualizzare la relativa pagina dei dettagli.

3. Scegli Continua per visualizzare la pagina di evasione, quindi scegli la scheda Avvio manuale.

Le informazioni nella pagina di evasione includono i tipi di istanze Amazon Elastic Compute Cloud (Amazon EC2) supportati, quelli supportati Regioni AWS e l'ID Amazon Machine Image (AMI) che il prodotto utilizza per ogni regione. AWS Nota che alcune scelte hanno un'incidenza sui costi. Utilizzerai queste informazioni per personalizzare il CloudFormation modello nei passaggi successivi.

4. Selezionare Accept Terms (Accetta termini) per abbonarsi al prodotto.

Dopo esserti abbonato a un prodotto, puoi accedere in qualsiasi Marketplace AWS momento alle informazioni sulla pagina di gestione del prodotto selezionando Il tuo software e quindi selezionando il prodotto.

Per definire il Marketplace AWS prodotto in un modello CloudFormation

Per completare i seguenti passaggi, utilizzerai uno dei modelli di CloudFormation esempio come punto di partenza e personalizzerai il modello in modo che rappresenti il tuo Marketplace AWS prodotto. Per accedere ai modelli di esempio, consultare [Modelli di esempio](#) nella Guida per l'utente di AWS CloudFormation .

1. Nella pagina Modelli di esempio della Guida per l' CloudFormation utente, scegli una AWS regione per il tuo prodotto. La AWS regione deve essere supportata dal Marketplace AWS prodotto. Puoi visualizzare le regioni supportate nella pagina di approvvigionamento del prodotto in Marketplace AWS.
2. Per visualizzare un elenco di modelli di servizio di esempio appropriati per la regione, scegli il link Servizi.
3. Come punto di partenza, puoi utilizzare uno qualsiasi degli esempi che risponde alle tue esigenze. Le fasi in questa procedura utilizzano il modello Amazon EC2 instance in a security group (Istanza Amazon EC2 in un gruppo di sicurezza). Per visualizzare il modello di esempio, selezionare View (Visualizza) e quindi salvare una copia del modello in locale in modo che sia possibile modificarla. Il file locale deve avere l'estensione `.template`.
4. Apri il file di modello in un editor di testo.
5. Personalizza la descrizione nella parte superiore del modello. La descrizione potrebbe essere simile a quanto segue:

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

6. Personalizza il parametro InstanceType di modo che includa solo i tipi di istanza EC2 supportati dal tuo prodotto. Se il modello include tipi di istanza EC2 non supportati, l'avvio del prodotto non riuscirà per i tuoi utenti finali.
 - a. Nella pagina di distribuzione del prodotto Marketplace AWS, visualizza i tipi di istanze EC2 supportati nella sezione Dettagli sui prezzi.

On-Demand Plans for Amazon EC2

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

| | |
|-------------------------|------------------|
| Region | Operating system |
| US East (N. Virginia) ▼ | Linux ▼ |
| Instance type | vCPU |
| All ▼ | 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. Nel modello, cambia il tipo di istanza di default in un tipo di istanza EC2 supportato di tua scelta.
- c. Modifica l'elenco AllowedValues di modo che includa solo i tipi di istanza EC2 supportati dal tuo prodotto.
- d. Rimuovi tutti i tipi di istanza EC2 che gli utenti finali non devono utilizzare quando avviano il prodotto dall'elenco AllowedValues.

Al termine della modifica, il parametro InstanceType potrebbe risultare simile all'esempio seguente:

```
"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. Nella sezione Mappings del modello, modifica le mappature AWSInstanceType2Arch di modo che siano inclusi solo i tipi di istanza EC2 e le architetture supportati.
 - a. Modifica l'elenco delle mappature rimuovendo tutti i tipi di istanza EC2 che non sono inclusi nell'elenco AllowedValues per il parametro InstanceType.
 - b. Modifica il valore Arch affinché ogni tipo di istanza EC2 sia il tipo di architettura supportato dal prodotto. I valori validi sono PV64, HVM64 e HVMG2. Per sapere quale architettura il prodotto supporta, consulta la pagina dei dettagli del prodotto in Marketplace AWS. Per sapere quali architetture sono supportate dalle famiglie di istanze EC2, consultare [Matrice del tipo di istanza AMI Amazon Linux](#).

Al termine della modifica delle mappature AWSInstanceType2Arch, il codice potrebbe essere simile a quanto segue:

```
"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. Nella Mappings sezione del modello, modifica le `AWSRegionArch2AMI` mappature per associare ogni AWS regione all'architettura e all'ID AMI corrispondenti per il prodotto.
 - a. Nella pagina di evasione del prodotto in Marketplace AWS, visualizza l'ID AMI utilizzato dal prodotto per ciascuna AWS regione, come nell'esempio seguente:

| Region | ID | |
|---------------------------|--------------|---|
| US East (N. Virginia) | ami-4379608 | Launch with EC2 Console |
| US West (Oregon) | ami-548a53ad | Launch with EC2 Console |
| US West (N. California) | ami-534866d7 | Launch with EC2 Console |
| EU (Frankfurt) | ami-24c48739 | Launch with EC2 Console |
| EU (Ireland) | ami-8672787 | Launch with EC2 Console |
| Asia Pacific (Singapore) | ami-89d9342 | Launch with EC2 Console |
| Asia Pacific (Sydney) | ami-4d94227 | Launch with EC2 Console |
| Asia Pacific (Tokyo) | ami-5ee545ae | Launch with EC2 Console |
| South America (Sao Paulo) | ami-867a86c5 | Launch with EC2 Console |

- b. Nel modello, rimuovi le mappature per tutte le AWS regioni che non supporti.
- c. Modifica la mappatura per ogni regione per rimuovere le architetture non supportate (PV64,HVM64, orHVMG2) e l'AMI associata. IDs
- d. Per ogni mappatura di AWS regione e architettura rimanente, specifica l'ID AMI corrispondente dalla pagina dei dettagli del prodotto in Marketplace AWS.

Al termine della modifica delle mappature `AWSRegionArch2AMI`, il codice potrebbe risultare simile all'esempio seguente:

```

"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"}  
}
```

Ora puoi utilizzare il modello per aggiungere il prodotto a un AWS Service Catalog portafoglio. Se si desidera apportare altre modifiche, consultare [Utilizzo di modelli di CloudFormation](#) per ulteriori informazioni sui modelli.

Per aggiungere il Marketplace AWS prodotto a un AWS Service Catalog portafoglio

1. Accedi a Console di gestione AWS e accedi alla console dell' AWS Service Catalog amministratore all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Nella pagina Portafogli, scegli il portafoglio a cui desideri aggiungere il Marketplace AWS prodotto.
3. Nella pagina dei dettagli del portfolio, scegli Carica nuovo prodotto.
4. Digita le informazioni richieste relative a prodotto e supporto.
5. Nella pagina Version details (Dettagli versione), selezionare Upload a template file (Carica un file di modello), quindi Browse (Sfoggia) e infine selezionare il file di modello.
6. Digita un titolo e una descrizione per la versione.
7. Scegli Next (Successivo).
8. Nella pagina di revisione, verifica che il riepilogo sia accurato, quindi scegli Conferma e carica. Il prodotto viene aggiunto al tuo portafoglio ed è disponibile per gli utenti finali che hanno accesso al portafoglio.

Usando CloudFormation StackSets

Note

AutoTags attualmente non sono supportati con CloudFormation StackSets.

Puoi utilizzarli CloudFormation StackSets per lanciare AWS Service Catalog prodotti su più Regioni AWS account. È possibile specificare l'ordine in cui i prodotti vengono distribuiti in sequenza

all'interno. Regioni AWS Tra gli account, i prodotti vengono distribuiti in parallelo. All'avvio, gli utenti possono specificare la tolleranza di errore e il numero massimo di account in cui distribuire in parallelo. Per ulteriori informazioni, consulta [Lavorare con](#). CloudFormation StackSets

Set di stack e istanze di stack

Un set di stack consente di creare pile in AWS account di diverse AWS regioni utilizzando un unico CloudFormation modello.

Un'istanza stack si riferisce a uno stack in un account di destinazione all'interno di una AWS regione ed è associata a un solo set di stack.

Per ulteriori informazioni, consulta [l'argomento relativo ai concetti di base di StackSets](#).

Vincoli del set di stack

In AWS Service Catalog, puoi utilizzare i vincoli dello stack set per configurare le opzioni di distribuzione del prodotto.

AWS Service Catalog supporta i vincoli dello stack set sui prodotti in due categorie AWS GovCloud (US) Regions: AWS GovCloud (Stati Uniti occidentali) e (Stati Uniti orientali). AWS GovCloud

[Per ulteriori informazioni, consulta Stack Set Constraints.AWS Service Catalog](#)

Gestione dei budget

Puoi utilizzare AWS Budgets per tenere traccia dei costi e dell'utilizzo del servizio all'interno. AWS Service Catalog Puoi associare i budget a AWS Service Catalog prodotti e portafogli.

Note

AWS Service Catalog non supporta i budget per i prodotti Terraform Open Source.

AWS Budgets ti dà la possibilità di impostare budget personalizzati che ti avvisano quando i costi o l'utilizzo superano (o si prevede che superino) l'importo preventivato. Le informazioni sui budget sono disponibili all'indirizzo. AWS <https://aws.amazon.com/aws-cost-management/aws-budgets>

Processi

- [Prerequisiti](#)

- [Creazione di un budget](#)
- [Associazione di un budget](#)
- [Visualizzazione di un budget](#)
- [Disassociazione di un budget](#)

Prerequisiti

Prima di utilizzare AWS Budgets, è necessario attivare i tag di allocazione dei costi nella console. Gestione dei costi e fatturazione AWS Per ulteriori informazioni, consulta la sezione relativa all'[attivazione dei tag per l'allocazione dei costi definiti dall'utente](#) nella Guida per l'utente di Gestione dei costi e fatturazione AWS .

Note

L'attivazione dei tag richiede fino a 24 ore.

È inoltre necessario abilitare l'accesso degli utenti alla Gestione dei costi e fatturazione AWS console per tutti gli utenti o i gruppi che utilizzeranno la funzionalità Budget. A tale scopo, crea una nuova policy per gli utenti.

Per consentire agli utenti di creare budget, devi anche consentire agli utenti di visualizzare le informazioni di fatturazione. Se desideri utilizzare le notifiche di Amazon SNS, puoi dare agli utenti la possibilità di creare notifiche Amazon SNS, come mostrato nell'esempio di policy riportato di seguito.

Per creare la policy dei budget

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, seleziona Policies (Policy).
3. Nel riquadro del contenuto seleziona Create policy (Crea policy).
4. Seleziona la scheda JSON e copia il testo dal documento della seguente policy JSON. Incolla il testo nella casella di testo JSON.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1435216493000",
      "Effect": "Allow",
      "Action": [
        "aws-portal:ViewBilling",
        "aws-portal:ModifyBilling",
        "budgets:ViewBudget",
        "budgets:ModifyBudget"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "Stmt1435216552000",
      "Effect": "Allow",
      "Action": [
        "sns:*"
      ],
      "Resource": [
        "arn:aws:sns:us-east-1:123456789012:*"
      ]
    }
  ]
}

```

5. Al termine, selezionare Review policy (Rivedi policy). In Policy Validator (Validatore di policy) vengono segnalati eventuali errori di sintassi.
6. Nella pagina Review (Revisione), assegnare un nome alla policy. Esamina il Summary (Riepilogo) della policy per visualizzare le autorizzazioni concesse dalla policy e seleziona Create policy (Crea policy) per salvare il proprio lavoro.

La nuova policy appare nell'elenco delle policy gestite ed è pronta a collegare utenti e gruppi. Per ulteriori informazioni, consulta [Creazione e collegamento di policy gestite dal cliente](#) nella Guida per l'utente AWS Identity and Access Management .

Creazione di un budget

Nella console di AWS Service Catalog amministrazione, le pagine Elenco prodotti e Portafogli elencano informazioni sui prodotti e sui portafogli esistenti e consentono di intraprendere azioni su di essi. Per creare un budget, decidi innanzitutto a quale prodotto o portafoglio desideri associare il budget.

Per creare un budget

1. Aprire la console Service Catalog all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Scegli Elenco di prodotti o portafogli.
3. Seleziona il prodotto o il portafoglio a cui desideri aggiungere un budget.
4. Apri il menu Azioni, quindi scegli Crea budget.
5. Nella pagina Budget creation (Creazione budget), associare un tipo di tag al budget.

Esistono due tipi di tag: AutoTags e TagOptions. AutoTags identifica il portafoglio, il prodotto e l'utente che ha lanciato un prodotto. AWS Service Catalog applica questi tag automaticamente alle risorse assegnate. A TagOption è una coppia chiave-valore definita dall'amministratore che viene gestita in AWS Service Catalog

Affinché le spese che si verificano in un portafoglio o un prodotto si riflettano sul budget associato, devono avere lo stesso tag. Tieni presente che una chiave di tag utilizzata per la prima volta può richiedere 24 ore per l'attivazione. Per ulteriori informazioni, consulta [the section called "Prerequisiti"](#).

6. Budget AWS Scegli Crea in. Verrai indirizzato alla pagina Imposta il tuo budget. Continua a impostare il budget seguendo la procedura descritta nella sezione [Creazione di un budget](#).

Note

Dopo aver creato un budget, è necessario associarlo al prodotto o al portafoglio.

Associazione di un budget

A ogni portafoglio o prodotto può essere associato un budget. Ogni budget può essere associato a più portafogli e prodotti.

Quando associ un budget a un portafoglio o a un prodotto, puoi visualizzare le informazioni sul budget dalla pagina dei dettagli di quel portafoglio o prodotto. Affinché la spesa relativa al portafoglio o al prodotto si rifletta nel budget, devi associare gli stessi tag al budget e al portafoglio o al prodotto.

Note

Se elimini un budget da Budget AWS, esistono ancora le associazioni esistenti con AWS Service Catalog prodotti e portafogli. AWS Service Catalog non sarà in grado di visualizzare alcuna informazione sul budget eliminato.

Per associare un budget

1. Aprire la console Service Catalog all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Scegli Elenco di prodotti o portafogli.
3. Seleziona il prodotto o il portafoglio a cui desideri associare un budget.
4. Apri il menu Azioni, quindi scegli Associa budget.
5. Nella pagina di associazione del budget, seleziona un budget esistente, quindi scegli Continua.
6. La tabella dei prodotti o dei portafogli ora include i dati relativi al budget appena aggiunto.

Visualizzazione di un budget


Se un budget è associato a un prodotto, è possibile visualizzare le informazioni sul budget nelle pagine dei dettagli del prodotto e dell'elenco dei prodotti. Se un budget è associato a un portafoglio, è possibile visualizzare le informazioni sul budget nelle pagine Portafogli e Dettagli del portafoglio.

Le pagine dei portafogli e dell'elenco dei prodotti visualizzano le informazioni sul budget per le risorse esistenti. Puoi visualizzare le colonne che mostrano Current vs. budget (Corrente e budget) e Forecast vs. budget (Previsione e budget).

Quando scegli un prodotto o un portafoglio, verrai indirizzato a una pagina dei dettagli. Le pagine dei dettagli del portafoglio e dei dettagli del prodotto contengono sezioni con informazioni dettagliate sui budget associati. Puoi visualizzare l'importo a budget, la spesa corrente e la spesa prevista. Hai anche la possibilità di visualizzare i dettagli del budget e modificare il budget.

Disassociazione di un budget

Puoi annullare l'associazione di un budget a un portafoglio o a un prodotto.

 Note

Se elimini un budget dai AWS budget, esistono ancora le associazioni esistenti con AWS Service Catalog prodotti e portafogli. AWS Service Catalog non sarà in grado di visualizzare alcuna informazione sul budget eliminato.

Per annullare l'associazione di un budget

1. Aprire la console Service Catalog all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Scegli Elenco di prodotti o portafogli.
3. Seleziona il prodotto o il portafoglio da cui desideri dissociare un budget.
4. Scegli Azioni. Dal menu a discesa, scegli Dissocia budget. Viene visualizzato un avviso di conferma.
5. Dopo aver confermato di voler eliminare il budget dal prodotto o dal portafoglio, scegli Conferma.

Gestione di prodotti con provisioning

AWS Service Catalog fornisce un'interfaccia per la gestione dei prodotti forniti. Puoi visualizzare, aggiornare e terminare tutti i prodotti con provisioning per il tuo catalogo in base al livello di accesso. Fai riferimento alle sezioni seguenti per esempi di procedure.

Argomenti

- [Gestione dei prodotti forniti in qualità di amministratore](#)
- [Modifica del proprietario del prodotto con provisioning](#)
- [Aggiornamento dei modelli per i prodotti forniti](#)
- [Esercitazione: identificazione dell'utente per l'allocazione delle risorse](#)
- [Gestione degli errori di stato del prodotto Terraform Open Source](#)
- [Gestione del file di stato del prodotto Terraform Open Source](#)

Gestione dei prodotti forniti in qualità di amministratore

Per gestire tutti i prodotti forniti per un account, è necessario disporre `AWSServiceCatalogAdminFullAccess` di un'autorizzazione IAM equivalente per accedere alle operazioni di scrittura dei prodotti forniti. Per ulteriori informazioni, consulta [Identity and Access Management in AWS Service Catalog](#).

Tip

Per il concatenamento statico dei prodotti forniti, è necessario fare riferimento agli output dei prodotti forniti in un modello di prodotto-artefatto prima che il prodotto fornito venga fornito. Per ulteriori informazioni, incluso un esempio, consulta quanto segue:

- [AWS::ServiceCatalog::CloudFormationProvisionedProduct](#) nella Guida per l'utente di AWS CloudFormation .
- [DescribeProvisioningParameters \(ProvisioningArtifactOutputKeys\)](#) nella Guida per gli AWS Service Catalog sviluppatori.

Visualizzazione e gestione di tutti i prodotti con provisioning

1. Apri la AWS Service Catalog console all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.

Se hai già effettuato l'accesso alla AWS Service Catalog console, scegli Service Catalog, quindi Utente finale.

2. Se necessario, scorri verso il basso fino alla sezione Prodotti forniti.
3. Nella sezione Prodotti forniti, scegli l'elenco Visualizza: e seleziona il livello di accesso che desideri visualizzare: Utente, Ruolo o Account. Questa azione mostra tutti i prodotti forniti nel catalogo.
4. Scegli un prodotto con provisioning da visualizzare, aggiornare o terminare. Per ulteriori informazioni sulle informazioni fornite in questa vista, consultare [Visualizzazione delle informazioni relative ai prodotti con provisioning](#).

Modifica del proprietario del prodotto con provisioning

È possibile modificare il proprietario di un prodotto con provisioning in qualsiasi momento. È necessario conoscere l'ARN dell'utente o del ruolo che si desidera impostare come nuovo proprietario.

Per impostazione predefinita, questa funzionalità è disponibile per gli amministratori che utilizzano la politica `AWSServiceCatalogAdminFullAccess` gestita. È possibile abilitarla per gli utenti finali concedendo loro l'`servicecatalog:UpdateProvisionedProductProperties` autorizzazione in AWS Identity and Access Management (IAM).

Per modificare il proprietario di un prodotto con provisioning

1. Nella AWS Service Catalog console, scegli Provisioned products list.
2. Individua il prodotto fornito che desideri aggiornare, quindi scegli i tre puntini accanto ad esso e scegli Cambia proprietario del prodotto fornito. È inoltre disponibile l'opzione Change owner (Cambia proprietario) nella pagina dei dettagli del prodotto con provisioning, nel menu Actions (Operazioni) .
3. Nella finestra di dialogo immettere l'ARN dell'utente o del ruolo che si desidera impostare come nuovo proprietario. Un ARN inizia con `arn:` e include altre informazioni separate da due punti o barre, ad esempio `arn:aws:iam::123456789012:user/NewOwner`.

4. Seleziona **Invia**. Viene visualizzato un messaggio con l'esito positivo quando il proprietario è stato aggiornato.

Vedi anche

- [UpdateProvisionedProductProperties](#)

Aggiornamento dei modelli per i prodotti forniti

È possibile modificare il modello corrente di un prodotto fornito con un modello diverso. Ad esempio, se hai un prodotto EC2 in Service Catalog, puoi aggiornare quel prodotto EC2 in modo che mantenga lo stesso ID prodotto fornito, ma modificare il modello in un bucket S3.

Note

L'aggiornamento dei modelli non è supportato per i prodotti Terraform Open Source o Terraform Cloud forniti. Se desideri utilizzare un modello diverso per un prodotto Terraform esistente, devi eliminare il prodotto e quindi creare un nuovo prodotto utilizzando il modello desiderato.

Per aggiornare un modello per un prodotto fornito

1. Nel menu di navigazione a sinistra, scegli **Provisioned products**.
2. In **Provisioned products**, scegli un prodotto fornito e seleziona **Azioni, Aggiorna**.

Tieni presente che puoi anche selezionare **Azioni, Aggiorna** nella pagina dei dettagli del prodotto **Provisioned**.

3. (Facoltativo) Nei dettagli del prodotto, scegli **Cambia prodotto**.

In **Cambia prodotto**, prendi nota di questo avviso:

La modifica del prodotto aggiornerà il prodotto fornito con un modello di prodotto diverso. Ciò potrebbe interrompere le risorse e creare nuove risorse.

È possibile aggiornare un prodotto fornito a una versione diversa all'interno dello stesso prodotto.

4. (Facoltativo) In Prodotti, scegli il prodotto che desideri aggiornare con un modello diverso. Quindi scegli Cambia.

Nei dettagli del prodotto, prendi nota di questo avviso:

[Nome prodotto] verrà aggiornato da [nome modello corrente] a [nuovo nome modello]. Tuttavia, il nome del prodotto fornito, [Nome prodotto fornito], non cambierà.

È possibile aggiornare un prodotto fornito a una versione diversa all'interno dello stesso prodotto.

5. In Versioni del prodotto, scegli la versione del prodotto che desideri.
6. In Parametri, scegli i parametri appropriati.
7. Scegliere Aggiorna.

In Provisioned product details, puoi vedere i dettagli dell'aggiornamento. Il nome del prodotto fornito non cambia, ma il prodotto fornito ora ha un modello diverso.

Esercitazione: identificazione dell'utente per l'allocazione delle risorse

È possibile identificare l'utente che ha fornito un prodotto e le risorse associate al prodotto utilizzando la console. AWS Service Catalog Questa esercitazione consente di adattare questo esempio ai tuoi prodotti con provisioning specifici.

Per gestire tutti i prodotti con provisioning per l'account, devi disporre dell'accesso `AWSServiceCatalogAdminFullAccess` o di un accesso equivalente alle operazioni di scrittura su prodotti con provisioning. Per ulteriori informazioni, vedere [Identity and Access Management](#) nella Guida AWS Service Catalog dell'amministratore.

Identificazione dell'utente che effettua il provisioning di un prodotto e delle risorse associate

1. Apri <https://console.aws.amazon.com/servicecatalog>.
2. Nel menu di navigazione a sinistra, scegli Provisioned product.
3. Nel menu a discesa Access Filter, scegli Account.

Service Catalog > Provisioned products

Provisioned products (0) [Info](#)

Search provisioned products

Access Filter: Account

Account

User

Account

Role

| Name | Created | ID | Product name | Version name | Status |
|------|---------|----|--------------|--------------|--------|
|------|---------|----|--------------|--------------|--------|

4. Nella visualizzazione Account, scegli e apri un prodotto fornito per visualizzarne i dettagli.

Provisioned products (1/6) [Info](#)

Search provisioned products

Access Filter: Account

| Name | Created | Product name | Version name | Status |
|-----------------------------------|-----------------------------------|--------------|--------------|--|
| s3bucket-03252118 | Thu, Mar 25, 2021, 5:28:40 PM EDT | s3bucket | 2 | ✔ Available |

Puoi vedere i dettagli del prodotto fornito.

Provisioned product details

Product description

-

| | | |
|--|---|--|
| Provisioned product ID pp-1a3m3m2d4c0vs | User name SCAdminAllow | Status ✔ Available |
| Product name shsen-test | User ARN arn:aws:iam::776643078058:user/SCAdminAllow | Version name - |
| Created Thu, Jul 15, 2021, 9:49:54 AM PDT | | |

▼ More details

| | | |
|---|---------------------------|----------------------------|
| Product ID prod-y7bnu3cn7eso | Type CFN_STACK | Support email contact - |
| Version ID pa-2d5ixhjrpypg4 | Product owner 53440542 | Support link - |

Support description

-

5. Scorri verso il basso per espandere la sezione Eventi. Nota i CloudformationStackARN valori Provisioned product ID and.

Events (4) [Info](#)

Search events

Sort by Newest < 1 > ⚙

▼ UPDATE_PROVISIONED_PRODUCT

| Date created | CloudFormationStackARN | Status |
|-----------------------------------|--|--|
| Thu, May 27, 2021, 5:06:38 PM EDT | Copy to clipboard | ✔ Succeeded |
| Record ID | Product name | Product version |
| rec- [redacted] | ssmImport | 1 |
| Provisioning artifact ID | | |
| pa- [redacted] | | |
| Output key | Output value | Output description |
| CloudformationStackARN | arn:aws:cloudformation:us-east-1:[account number]:stack/SC-[product name]-[id]-[redacted]-11eb-b851-0a8a0480d74d | The ARN of the launched Cloudformation Stack |

6. Utilizza l'ID del prodotto fornito per identificare il AWS CloudTrail record corrispondente a questo lancio e identificare l'utente richiedente (in genere, inserisci un indirizzo e-mail durante la federazione). In questo esempio è "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]
}

```

- Utilizzate il CloudFormationStackARN valore per identificare CloudFormation gli eventi e trovare informazioni sulle risorse create. Puoi anche utilizzare l' CloudFormation API per ottenere queste informazioni. Per ulteriori informazioni, consulta la [Documentazione di riferimento delle API AWS CloudFormation](#).

È possibile eseguire i passaggi da 1 a 4 utilizzando l' AWS Service Catalog API o il AWS CLI. Per ulteriori informazioni, consulta la [Guida per AWS Service Catalog gli sviluppatori](#) e [riferimento alla AWS Service Catalog riga di comando](#).

Gestione degli errori di stato del prodotto Terraform Open Source

I ProvisionProduct guasti di Terraform Open Source vengono indirizzati allo TAINTED stato, consentendo a ciascun prodotto fornito di procedere. UpdateProvisionedProduct Quando ciò si verifica:

- UpdateProvisionedProduct non tenta di aggiornare o correggere i tag o di creare o modificare un gruppo di risorse.
- UpdateProvisionedProduct non prende in considerazione i guasti derivanti da precedenti operazioni di approvvigionamento nel decidere se il prodotto fornito debba essere impostato su o. AVAILABLE TAINTED

AWS Service Catalog applica i tag solo durante. ProvisionProduct Qualsiasi etichettatura non riuscita derivante da un errore dell'ProvisionProduct operazione non viene risolta automaticamente.

Esempi di errori di stato

Esempio 1: AWS Service Catalog non crea un gruppo di risorse durante ProvisionProduct

Nello scenario seguente, avete un prodotto fornito nello AVAILABLE stato anche se non esiste un gruppo di risorse di supporto e senza alcun tag applicato alle risorse.

1. L'azione viene avviata ProvisionProduct.
2. Il motore di provisioning Terraform risponde ProvisionProduct con un errore del flusso di lavoro e non fornisce un. ResourceIdentifier
3. Il ProvisionProduct flusso di lavoro non crea un gruppo di risorse e quindi imposta lo stato del prodotto fornito su. ERROR
4. Quindi si avvia l'operazione. UpdateProvisionedproduct
5. Il motore di provisioning Terraform risponde indicando «successo».
6. Di conseguenza, il UpdateprovisionedProduct flusso di lavoro imposta lo stato del prodotto fornito suAVAILABLE, ma non crea un gruppo di risorse né tenta di applicare alcun tag.

Esempio 2: AWS Service Catalog crea nuove risorse durante UpdateProvisionedProduct

Nello scenario seguente, hai un prodotto fornito nello AVAILABLE stato anche se alle nuove risorse non è applicato alcun tag.

1. L'azione viene avviata ProvisionProduct.
2. Il motore di provisioning Terraform risponde indicando «successo» e fornisce un ResourceIdentifier.
3. Il ProvisionProduct flusso di lavoro crea un gruppo di risorse e applica i tag a tutte le risorse identificate.
4. Si inizia UpdateProvisionedProduct con un nuovo artefatto che crea nuove risorse.
5. Il motore di provisioning Terraform risponde indicando «successo».
6. Il UpdateProvisionedProduct flusso di lavoro imposta lo stato del prodotto fornito AVAILABLE ma non tenta di applicare tag aggiuntivi alle nuove risorse.

Soluzione degli errori di stato

AWS Service Catalog assicura la creazione di un gruppo di risorse per tutti i prodotti forniti impostati su TAIANTED from ProvisionProduct. Se il motore di provisioning Terraform non restituisce un ResourceIdentifier gruppo di risorse o se AWS Service Catalog non riesce a creare un gruppo di risorse, il prodotto fornito viene impostato ERROR sullo stato, costringendo l'utente a terminare.

Gestione del file di stato del prodotto Terraform Open Source

Ogni prodotto Terraform Open Source fornito ha un file a stato singolo. Esiste una relazione 1:1 tra il prodotto fornito e il relativo file di stato. I file vengono archiviati in un bucket Amazon S3 denominato sc-terraform-engine-state-`-${AWS::AccountId}-${AWS::Region}` Il file di stato viene salvato con la chiave AccountID o ProvisionedProductID object.

L'accesso ai file di stato è limitato ai GetStateFile AWS Lambda modelli di avvio di Amazon EC2. AWS Service Catalog gli amministratori non hanno accesso diretto ai file di stato in Amazon S3. Gli amministratori devono accedere ai file utilizzando Amazon EC2. Per impostazione predefinita, AWS Service Catalog gli amministratori possono visualizzare l'elenco dei file di stato, ma non possono leggere o scrivere il contenuto del file. Solo il motore di provisioning Terraform può leggere o scrivere il contenuto del file.

Gestione dei tag in AWS Service Catalog

AWS Service Catalog fornisce tag in modo da poter classificare le risorse. Esistono due tipi di tag: AutoTags e TagOptions.

AutoTags sono tag che identificano le informazioni sull'origine di una risorsa fornita AWS Service Catalog e vengono applicati automaticamente AWS Service Catalog alle risorse assegnate.

TagOptions sono coppie chiave-valore gestite in AWS Service Catalog che fungono da modelli per la creazione di tag. AWS

Argomenti

- [AWS Service Catalog AutoTags](#)
- [AWS Service Catalog TagOption Biblioteca](#)

AWS Service Catalog AutoTags

Note

AWS Service Catalog non supporta AutoTags i prodotti Terraform Open Source.

AutoTags sono tag che identificano le informazioni sull'origine di una risorsa fornita AWS Service Catalog e vengono applicati automaticamente alle risorse fornite. AWS Service Catalog

AutoTags includono tag per gli identificatori univoci di portafoglio, prodotto, utente, versione del prodotto e prodotto fornito. Ciò fornisce una serie di tag che riflettono la AWS Service Catalog struttura che i clienti hanno configurato nel catalogo. AutoTags non vengono conteggiati ai fini del limite di 50 tag del cliente.

Note

AWS Service Catalog non supporta AutoTags i prodotti Terraform Open Source.

AWS Service Catalog AutoTags può aiutare a fornire tag coerenti per le risorse, il che è utile quando si impostano i budget per un portafoglio, un prodotto o un utente. Puoi anche utilizzare il

AutoTags per identificare le risorse per le operazioni successive al lancio, come l'impostazione delle regole. AWS Config AutoTags è possibile visualizzare le risorse fornite nella sezione Tag dei servizi downstream utilizzati per il provisioning, ad esempio Amazon e CloudFormation Amazon EC2 S3.

Note

AWS Service Catalog non si aggiorna AutoTags dopo aver richiesto il provisioning delle risorse AutoTags . Se aggiorni il prodotto fornito a un prodotto diverso, a un elemento fornito o a un nuovo percorso di lancio, quello esistente mostra AutoTags ancora i valori originali.

AutoTag dettagli

- `aws:servicecatalog:portfolioArn` – ARN del portafoglio da cui è stato avviato il prodotto con provisioning.
- `aws:servicecatalog:productArn` – L'ARN del prodotto da cui è stato avviato il prodotto con provisioning.
- `aws:servicecatalog: provisioningPrincipalArn` - L'ARN del principale di provisioning (utente) che ha creato il prodotto fornito.
- `aws:servicecatalog: - provisionedProductArn` L'ARN del prodotto fornito.
- `aws:servicecatalog: - L'ID dell'elemento di provisioning originale (versione del prodotto).`
`provisioningArtifactIdentifier`

AWS Service Catalog TagOption Biblioteca

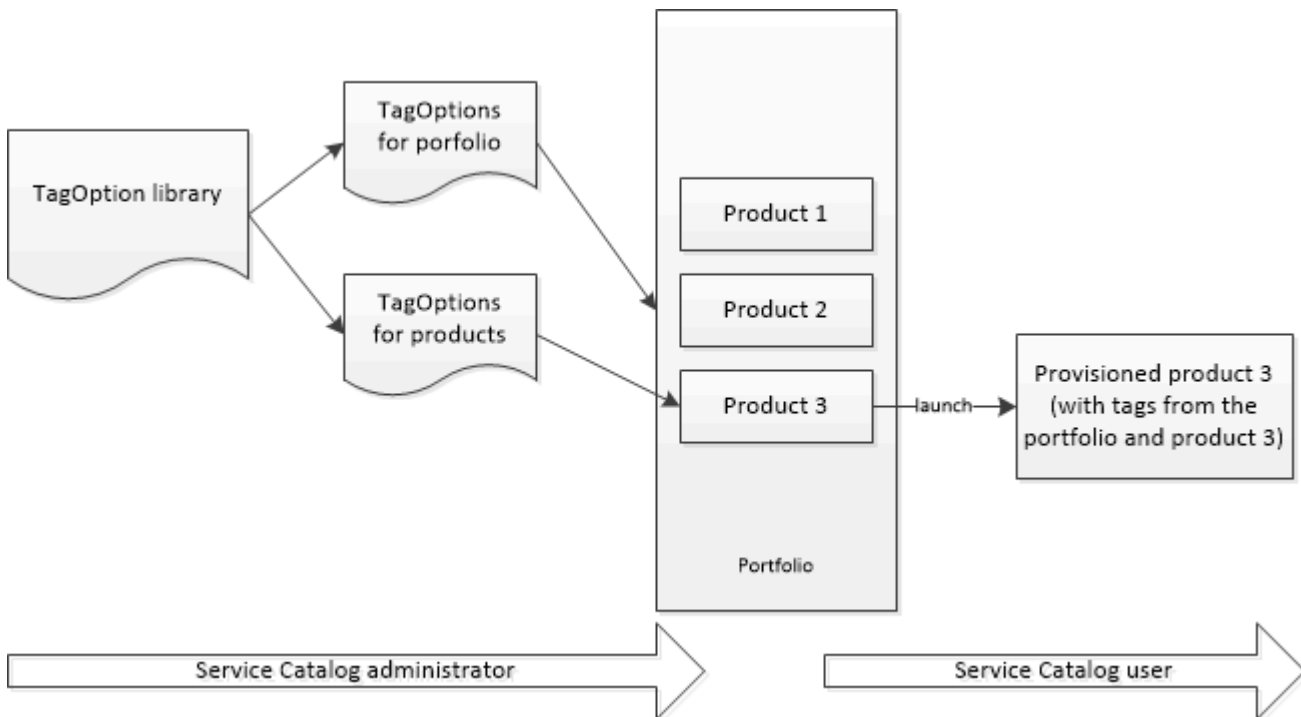
Per consentire agli amministratori di gestire facilmente i tag sui prodotti forniti, AWS Service Catalog fornisce una TagOption libreria. A TagOption è una coppia chiave-valore gestita in. AWS Service Catalog Non è un AWS tag, ma funge da modello per creare un AWS tag basato su. TagOption

AWS Service Catalog non supporta TagOptions i prodotti Terraform Open Source o Terraform Cloud.

La TagOption libreria semplifica l'applicazione di quanto segue:

- Una tassonomia coerente
- Etichettatura corretta delle risorse AWS Service Catalog
- Opzioni definite e selezionabili dall'utente per tag consentiti

Gli amministratori possono TagOptions associarsi a portafogli e prodotti. Durante il lancio di un prodotto (provisioning), AWS Service Catalog aggrega il portafoglio e il prodotto associati e li applica al prodotto fornito TagOptions, come illustrato nel diagramma seguente.



Con la TagOption libreria, puoi disattivare TagOptions e mantenere le loro associazioni a portafogli o prodotti e riattivarle quando ne hai bisogno. Questo approccio non solo aiuta a mantenere l'integrità della libreria, ma consente anche di gestire TagOptions l'eventuale utilizzo a intermittenza o solo in circostanze particolari.

Puoi gestire TagOptions con la AWS Service Catalog console o l'API della TagOption libreria. Per ulteriori informazioni, vedere [Service Catalog API Reference](#).

Indice

- [Lancio di un prodotto con TagOptions](#)
- [Gestire TagOptions](#)
- [Utilizzo TagOptions con le politiche dei AWS Organizations tag](#)

Lancio di un prodotto con TagOptions

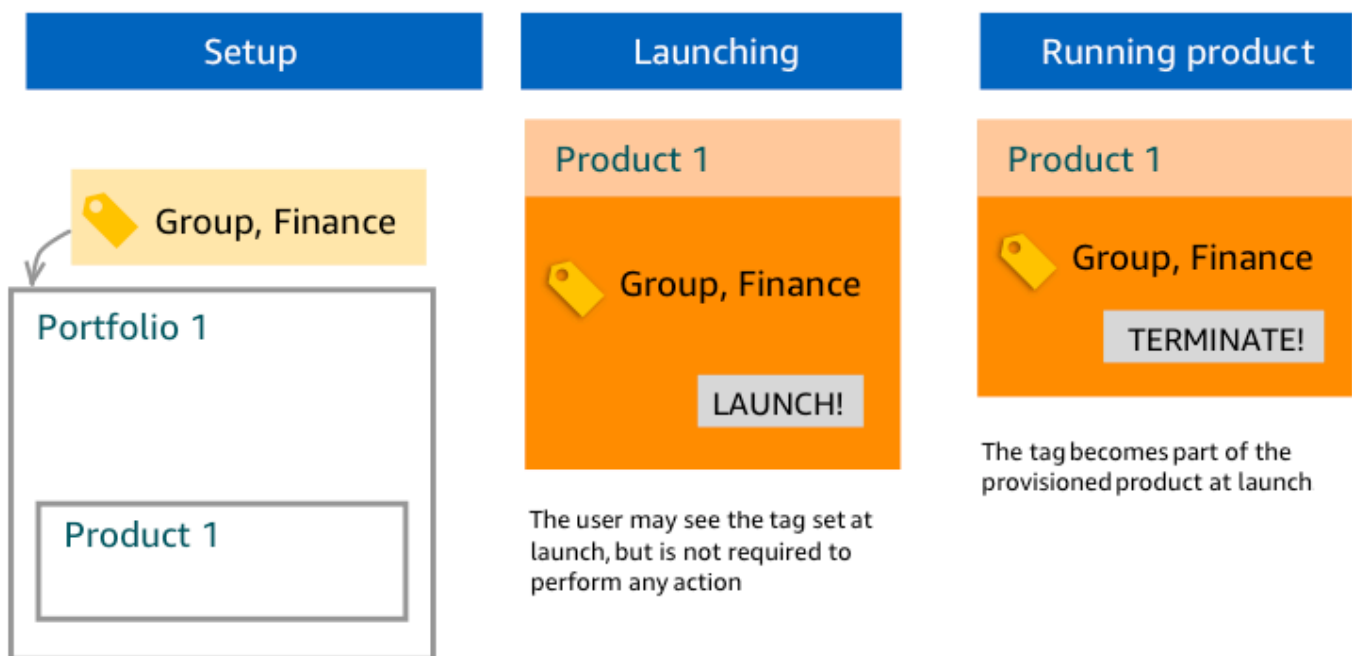
Quando un utente lancia un prodotto che lo ha TagOptions, AWS Service Catalog esegue le seguenti azioni per tuo conto:

- Raccoglie tutto TagOptions per il prodotto e il portafoglio di lancio.
- Assicura che in un tag sul prodotto fornito vengano utilizzate solo TagOptions chiavi univoche. Gli utenti ottengono un elenco di valori a scelta multipla per una chiave. Dopo che l'utente sceglie un valore, questo diventa un tag sul prodotto con provisioning.
- Consente agli utenti di aggiungere tag non conflittuali al prodotto durante il provisioning.

I seguenti casi d'uso dimostrano come TagOptions funzionano durante il lancio.

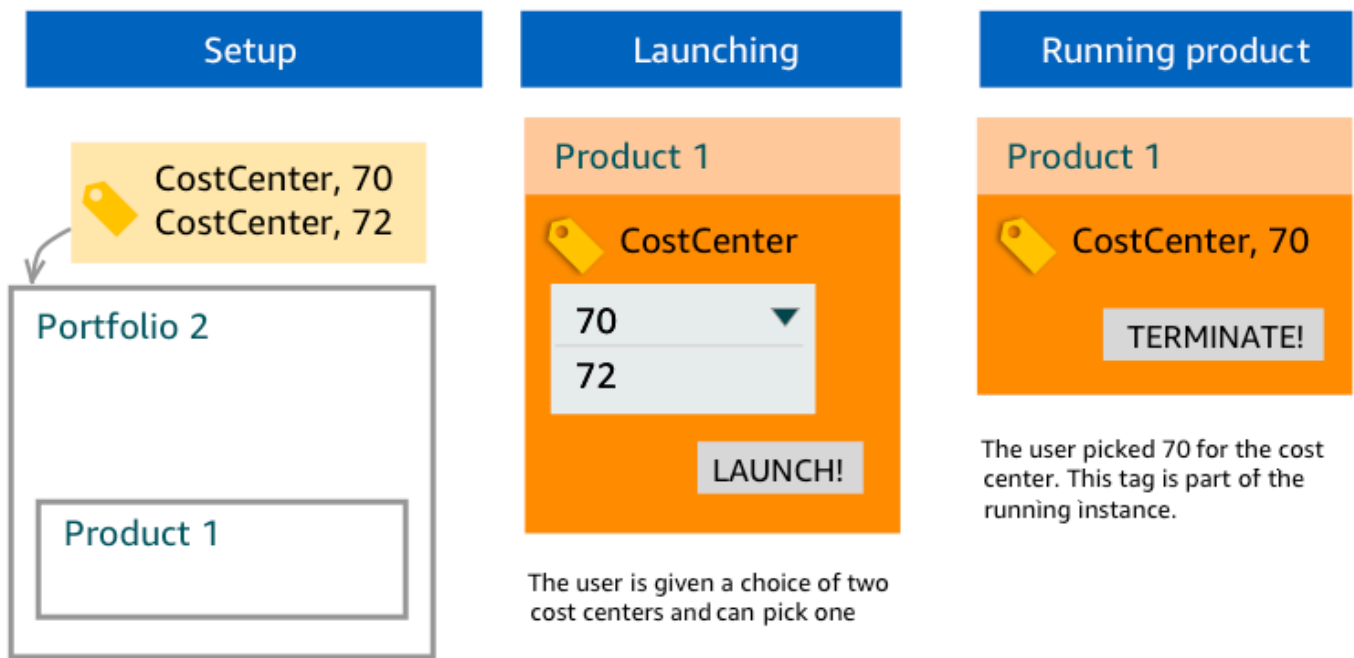
Esempio 1: una TagOption chiave unica

Un amministratore crea TagOption[Group=Finance] e lo associa a Portfolio1, che ha Product1 con no. TagOptions. Quando un utente avvia il prodotto fornito, il singolo TagOption diventa Tag [Group=Finance], come segue:



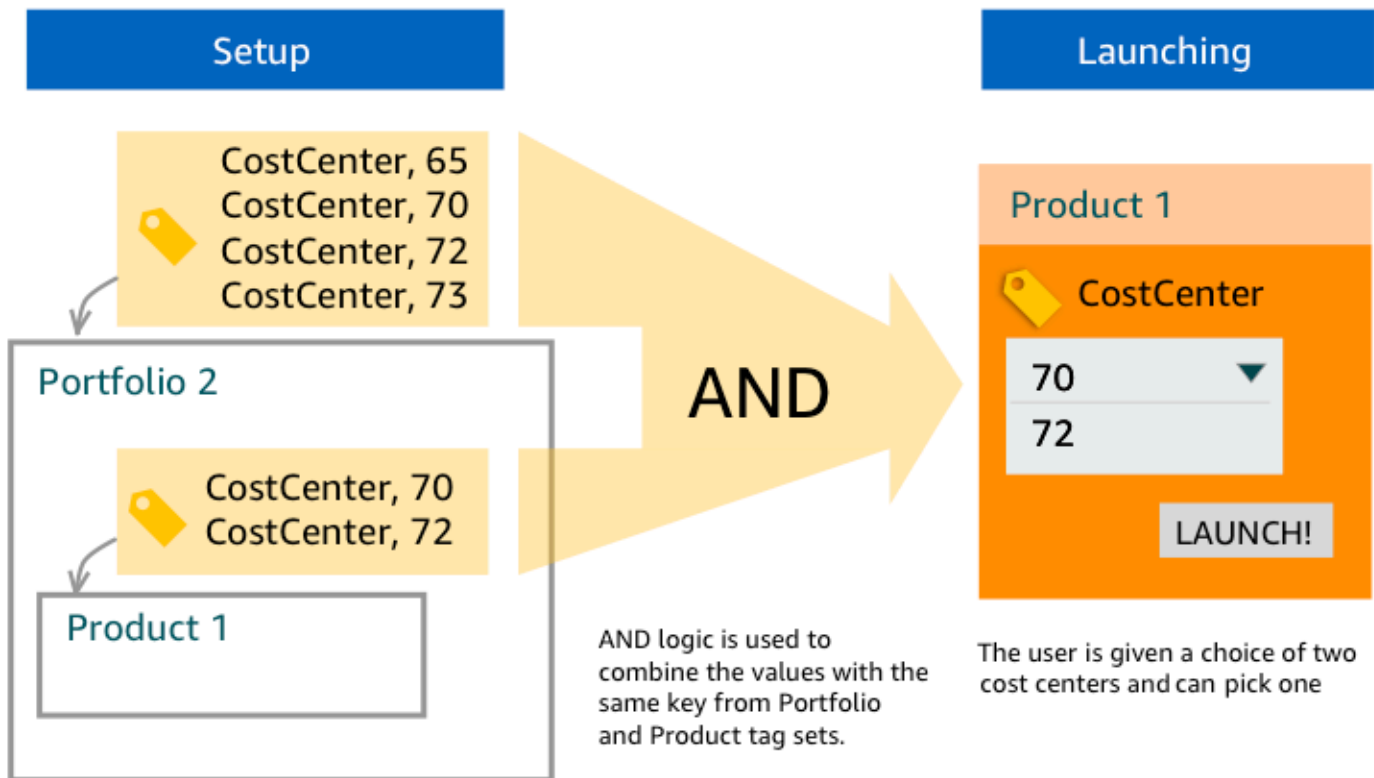
Esempio 2: un set TagOptions con la stessa chiave su un portafoglio

Un amministratore ne ha inseriti due TagOptions con la stessa chiave in un portafoglio e non ce ne sono TagOptions con la stessa chiave su nessun prodotto all'interno di quel portafoglio. Durante l'avvio, l'utente deve selezionare uno dei due valori associati alla chiave. Il prodotto con provisioning viene quindi taggato con la chiave e il valore selezionato dall'utente.



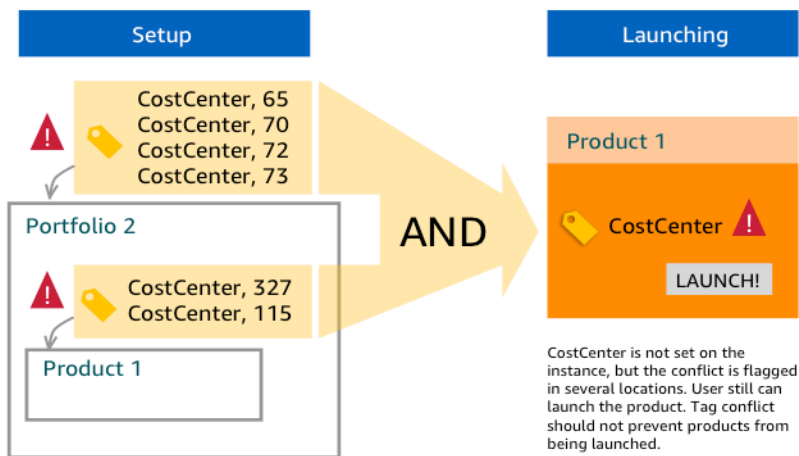
Esempio 3: un set TagOptions con la stessa chiave sia sul portafoglio che su un prodotto in quel portafoglio

Un amministratore ne ha posizionati diversi TagOptions con la stessa chiave in un portafoglio e ce ne sono anche diversi TagOptions con la stessa chiave sul prodotto all'interno di quel portafoglio. AWS Service Catalog crea un insieme di valori dall'aggregazione (operazione AND logica) di TagOptions. Quando l'utente avvia il prodotto, vede tale set di valori ed esegue la selezione. Il prodotto con provisioning viene taggato con la chiave e il valore selezionato dall'utente.



Esempio 4: multipli TagOptions con la stessa chiave e valori in conflitto

Un amministratore ne ha inseriti diversi TagOptions con la stessa chiave in un portafoglio e ce ne sono anche diversi TagOptions con la stessa chiave sul prodotto di quel portafoglio. AWS Service Catalog crea un insieme di valori dall'aggregazione (operazione AND logica) di TagOptions. Se l'aggregazione non trova i valori per la chiave, AWS Service Catalog crea un tag con la stessa chiave e il valore `disc-tagconflict-portfolioid-productid`, dove *portfolioid* e *productid* sono il ARNs portafoglio e il prodotto. In questo modo, il prodotto con provisioning viene taggato con la chiave corretta e con un valore che l'amministratore può trovare e correggere.



Gestire TagOptions

In qualità di amministratore, puoi eseguire le seguenti azioni da gestire TagOptions nella TagOptions libreria:

- Creare ed eliminare
- Attiva o disattiva
- Associare o dissociare
- Modifica

Per creare TagOptions nella console

1. Aprire la console Service Catalog all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Nel menu di navigazione a sinistra, scegli TagOptionslibreria.
3. In Crea nuovo TagOption, inserisci una chiave e un valore, quindi scegli Aggiungi.

Una volta creato, il nuovo TagOption viene raggruppato per coppia chiave-valore e ordinato alfabeticamente nell'elenco. TagOptions

Per creare un file utilizzando l'API, consulta TagOption . AWS Service Catalog [CreateTagOption](#)

Per eliminare TagOptions nella console

1. Aprire la console Service Catalog all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Nel menu di navigazione a sinistra, scegli TagOptions libreria, quindi scegli Azioni.

3. Seleziona Elimina e conferma l'eliminazione.

Per attivarne o disattivarne uno o più TagOptions nella console

1. Aprire la console Service Catalog all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Nel menu di navigazione a sinistra, scegli TagOptions libreria, quindi scegli Azioni.
3. Per attivarlo, scegli quello inattivo TagOption che desideri. Quindi scegli Azioni e seleziona Attiva dal menu a discesa e conferma la selezione.

Per disattivarlo, scegli l'attivo TagOption che desideri. Quindi scegli Azioni e seleziona Disattiva dal menu a discesa e conferma la selezione.

Per associare o dissociare uno o più TagOptions portfolio nella console

1. Aprire la console Service Catalog all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Nel menu di navigazione a sinistra, scegli Portafogli, quindi apri il portfolio che desideri associare o dissociare.
3. Scegli la TagOptionsscheda e selezionane una o più TagOptions da associare o dissociare dal portfolio.
4. Scegli Azioni. Quindi seleziona Associa o Dissocia e conferma la selezione.

Per associare o dissociare uno o più TagOptions prodotti nella console

1. Apri la AWS Service Catalog console all'indirizzo: <https://console.aws.amazon.com/servicecatalog/>.
2. Nel menu di navigazione a sinistra, in Amministrazione, scegli Prodotti. Quindi apri il prodotto che desideri associare o dissociare.
3. Scegli la TagOptionsscheda e selezionane una o più TagOptions da associare o dissociare dal portfolio.
4. Scegli Azioni. Quindi seleziona Associa o Dissocia e conferma la selezione.

Note

Per TagOptions associarti a un portafoglio o a un prodotto utilizzando l' AWS Service Catalog API, consulta [AssociateTagOptionWithResource](#).

Per rimuovere (dissociare) TagOptions utilizzando l' AWS Service Catalog API, consulta [DisassociateTagOptionFromResource](#).

Per modificare i valori di TagOptions nella console

1. Aprire la console Service Catalog all'indirizzo <https://console.aws.amazon.com/servicecatalog/>.
2. Nel menu di navigazione a sinistra, scegli TagOptionslibreria.
3. Scegli un TagOption e apri il valore. (Il valore è collegato a un collegamento ipertestuale). Quindi scegliere Edit (Modifica).
4. Nel campo Valore, modifica il valore e scegli Salva modifiche.

Utilizzo TagOptions con le politiche dei AWS Organizations tag

Questo argomento fornisce una breve panoramica delle politiche relative ai tag per AWS Organizations e TagOptions per AWS Service Catalog. Suggerisce inoltre come prevenire i conflitti di tag quando si utilizzano entrambe le funzionalità contemporaneamente.

TagOptions per AWS Service Catalog applicarsi ai prodotti forniti (CloudFormationpile), mentre le politiche di AWS Organizations etichettatura si applicano agli AWS account e alle unità organizzative (OU) o alla radice dell'organizzazione. Ad esempio, se si allega una politica di tag a un'unità organizzativa, la stessa politica di tag si applica a tutti gli account di quell'unità organizzativa. Se si utilizzano entrambe le funzionalità di etichettatura contemporaneamente, è necessario configurarle in modo che non si verifichino conflitti.

Policy di tag

Le politiche sui tag ti consentono di definire regole su come utilizzare i tag sulle AWS risorse dei tuoi account in AWS Organizations. Puoi utilizzare le politiche sui tag per creare e mantenere un approccio coerente per l'etichettatura AWS delle risorse a livello di account.

Le politiche sui tag forniscono un modo semplice per garantire che gli utenti applichino tag coerenti, controllino le risorse con tag e mantengano una corretta categorizzazione delle risorse. Puoi anche definire in che modo le chiavi dei tag devono essere scritte in maiuscolo e i valori che desideri consentire. Ad esempio, puoi richiedere che tutte le istanze EC2 di un account abbiano una chiave di tag impostata come **CostCenter** e i valori corrispondenti a quel tag siano o. **Data Insights Marketing**

Le politiche relative ai tag consentono di selezionare opzioni per applicare le regole di etichettatura, impedire operazioni non conformi sui tag e specificare i tipi di risorse a cui applicare l'applicazione. Se non scegli un'opzione di imposizione, le policy sui tag ti consentono di creare o modificare i tag non conformi, ma li segnalano come non conformi nella console. AWS Organizations

[Per ulteriori informazioni su come impostare l'applicazione dei tag a livello di account, consulta le politiche relative ai tag in. AWS Organizations](#)

TagOptions

TagOptions sono una funzionalità di etichettatura che AWS Service Catalog si applica ai prodotti forniti a livello di CloudFormation stack se applicata a un prodotto associato. AWS Service Catalog fornisce una TagOptions libreria in cui è possibile definire le coppie chiave-valore da associare ai prodotti. AWS Service Catalog Quando lanci un AWS Service Catalog prodotto, devi scegliere TagOption i valori per le TagOption chiavi esistenti associate a quel portafoglio o prodotto per lanciare quel prodotto. Poiché li imposti TagOptions a livello di portafoglio o di prodotto, puoi applicare una tassonomia coerente per l'etichettatura dei portafogli condivisi tra account e aree geografiche.

[Per ulteriori informazioni su come eseguire la configurazione in, consulta Libreria. TagOptions AWS Service CatalogAWS Service Catalog TagOption](#)

Evitare conflitti tra le politiche relative ai AWS Organizations tag e AWS Service Catalog TagOptions

Se configuri le politiche sui AWS Organizations tag per gli account della tua organizzazione, ti consigliamo quanto segue:

- Condividi i requisiti per la conformità dei tag con gli amministratori che gestiscono anche i AWS Service Catalog portafogli e TagOptions i prodotti.
- Condividi i requisiti per i tag conformi con gli utenti finali che potrebbero lanciare prodotti AWS Service Catalog e aggiungi tag opzionali per gli utenti finali al lancio dei loro prodotti.

Supponiamo di voler lanciare un prodotto AWS Service Catalog che utilizza la TagOption chiave `city` e di disporre di una politica di tag che richiede che le chiavi di tag abbiano valori di tag delle città degli Stati Uniti, ad esempio, `city Atlanta San Francisco Austin` AWS Service Catalog non consente di lanciare un prodotto senza aver selezionato TagOption i valori per le TagOption chiavi richieste per un prodotto.

In questo caso, se hai TagOption valori per la TagOption chiave `city` che includono città del Sud America, come **Rio de Janeiro** o **Buenos Aires**, AWS Service Catalog non lancerà il prodotto. Al contrario, devi selezionare un TagOption valore che includa una città degli Stati Uniti durante il lancio per rispettare la politica sui tag.

La tabella seguente fornisce scenari che descrivono come risolvere i problemi di conflitto di tag che potrebbero verificarsi quando si utilizzano le politiche sui tag e TagOptions contemporaneamente.

| Scenario | Motivo | Soluzione |
|--|---|---|
| Il prodotto non viene avviato a causa di tag non conformi se l'applicazione dei tag è verificata nella politica dei tag. | <p>Specificare TagOptions con chiavi e valori che non sono stati aggiunti all'elenco o consentito di tag conformi nella politica sui tag.</p> <p>Aggiungere tag personalizzati opzionali che non sono conformi alla tua politica sui tag.</p> | <p>Se configuri uno schema di capitalizzazione specifico nell'applicazione delle maiuscole nelle chiavi dei tag policy, assicurati che le chiavi dei TagOptions tag e le chiavi di tag personalizzate opzionali siano coerenti con quanto specificato nella politica dei tag.</p> <p>Nota che quando la casella di imposizione delle lettere maiuscole nei tag non è selezionata nella tua politica sui tag, tutte le chiavi dei tag minuscole sono conformi e assicura che le chiavi dei TagOptions tag e le chiavi dei tag personalizzate opzionali siano coerenti (ad esempio tutte in minuscolo) con quanto richiesto nella tua politica sui tag.</p> |
| Il prodotto non riesce ad avviarsi a causa della non | Specificazione di una maiuscola nelle TagOptions | Configura correttamente le tue politiche sui tag. Se non |

| Scenario | Motivo | Soluzione |
|--|--|---|
| conformità delle maiuscole nelle chiavi dei tag. | chiavi che non è coerente con le regole di applicazione delle maiuscole della policy dei tag. | <p>specifichi la conformità delle maiuscole nelle chiavi dei tag, le maiuscole delle chiavi dei tag di default sono tutte in minuscolo.</p> <p>Inoltre, se non specifichi la conformità alle lettere maiuscole nei tag nella tua politica sui tag, assicurati che le chiavi dei TagOptions tag AWS Service Catalog siano tutte minuscole per rispettare le regole di applicazione.</p> <p>Se utilizzi una politica di tag che non ha abilitato la conformità alle lettere maiuscole, tale politica considera conformi solo tutte le chiavi dei tag minuscole.</p> |
| Il prodotto non si avvia a causa di valori di tag incompatibili. | Selezione di un valore di TagOptions tag per il lancio di un prodotto che non è presente nell'elenco dei tag consentiti dalla politica sui tag Tag Value Compliance. | TagOptions Associa ai tuoi prodotti e portafogli i valori dei tag consentiti da Tag Value Compliance a quanto richiesto nella policy di elenco. |

Motori esterni per AWS Service Catalog

In AWS Service Catalog, i motori esterni sono rappresentati tramite un tipo di EXTERNAL prodotto. Il tipo di EXTERNAL prodotto consente l'integrazione di motori di provisioning di terze parti, come Terraform. È possibile utilizzare motori esterni per estendere le funzionalità di Service Catalog oltre i AWS CloudFormation modelli nativi, abilitando l'uso di altri strumenti Instructure as Code (IaC).

Il tipo di EXTERNAL prodotto consente di gestire e distribuire le risorse utilizzando l'interfaccia familiare di Service Catalog sfruttando al contempo le funzionalità e la sintassi specifiche dello strumento IaC scelto.

Per abilitare i tipi di EXTERNAL prodotto in Service Catalog, devi definire un set di risorse standard nel tuo account. Queste risorse sono note come motore. Service Catalog delega le attività al motore in punti specifici delle operazioni di analisi e provisioning degli artefatti.

Un elemento di provisioning rappresenta la versione specifica di un prodotto all'interno di Service Catalog, che consente di gestire e distribuire risorse coerenti.

Quando si richiamano AWS Service Catalog le [DescribeProvisioningParameters](#) operazioni [DescribeProvisioningArtifact](#) per un elemento di provisioning per un tipo di EXTERNAL prodotto, Service Catalog richiama una AWS Lambda funzione nel motore. Ciò è necessario per estrarre l'elenco dei parametri dall'elemento di provisioning fornito e restituirli a. AWS Service Catalog Questi parametri verranno utilizzati successivamente come parte del processo di provisioning.

Quando effettui il EXTERNAL provisioning di un elemento di provisioning tramite chiamata [ProvisionProduct](#), Service Catalog esegue prima alcune azioni internamente, quindi invia un messaggio a una coda Amazon SQS nel motore. Successivamente, il motore assume il ruolo di lancio fornito (il ruolo IAM assegnato a un prodotto come vincolo di lancio), effettua il provisioning delle risorse in base all'elemento di provisioning fornito e richiama l'API per segnalare l'esito positivo o negativo. [NotifyProvisionProductEngineWorkflowResult](#)

Le chiamate verso [UpdateProvisionedProduct](#) e [TerminateProvisionedProduct](#) vengono gestite in modo simile, ognuna con una coda distinta e Notify: APIs

- [NotifyProvisionProductEngineWorkflowResult](#)
- [NotifyUpdateProvisionedProductEngineWorkflowResult](#)
- [NotifyTerminateProvisionedProductEngineWorkflowResult](#).

Argomenti

- [Considerazioni](#)
- [Analisi dei parametri](#)
- [Fornitura](#)
- [Aggiornamento in corso](#)
- [Terminare](#)
- [Assegnazione di tag](#)

Considerazioni

Limite di un motore esterno per account hub

È possibile utilizzare un solo motore di EXTERNAL provisioning per account hub Service Catalog. Il hub-and-spoke modello Service Catalog consente all'account hub di creare prodotti di base e condividere il portafoglio, mentre gli account spoke importano i portafogli e sfruttano i prodotti.

Questo limite è dovuto al fatto che EXTERNAL può essere indirizzato a un solo motore in un account. Se un amministratore desidera disporre di più motori esterni, deve configurare i motori esterni (insieme ai portafogli e ai prodotti) in diversi account hub.

I motori esterni supportano solo ruoli di lancio con vincoli di avvio

EXTERNAL gli artefatti di provisioning supportano solo il provisioning con ruoli di avvio specificati utilizzando i vincoli di avvio. Un vincolo di avvio specifica il ruolo IAM che Service Catalog assume quando un utente finale avvia, aggiorna o chiude un prodotto. [Per ulteriori informazioni sui vincoli di lancio, consulta Launch Constraints.AWS Service Catalog](#)

Analisi dei parametri

EXTERNAL gli artefatti di approvvigionamento possono essere di qualsiasi formato. Ciò significa che quando si crea un tipo di EXTERNAL prodotto, il motore deve estrarre l'elenco dei parametri dall'elemento di provisioning fornito e restituirli a Service Catalog. Questo viene fatto creando una funzione Lambda nell'account in grado di accettare il seguente formato di richiesta, elaborare l'elemento di provisioning e restituire il seguente formato di risposta.

⚠ Important

La funzione Lambda deve essere denominata.
ServiceCatalogExternalParameterParser

Sintassi della richiesta:

```
{
  "artifact": {
    "path": "string",
    "type": "string"
  },
  "launchRoleArn": "string"
}
```

| Campo | Tipo | Campo obbligatorio | Descrizione |
|--------------------|---------|--------------------|---|
| artefatto | oggetto | Sì | Dettagli sull'artefatto da analizzare. |
| artefatto/percorso | stringa | Sì | Posizione da cui il parser scarica l'artefatto. Ad esempio, perAWS_S3, questo è l'URI di Amazon S3. |
| artefatto/tipo | stringa | Sì | Tipo di artefatto. Valore consentito: AWS_S3 |
| LaunchRole | stringa | No | L'Amazon Resource Name (ARN) del ruolo di avvio da assumere durante il download dell'artefatto. Se non viene fornito alcun ruolo di |

| Campo | Tipo | Campo obbligatorio | Descrizione |
|-------|------|--------------------|---|
| | | | avvio, viene utilizzato il ruolo di esecuzione di Lambda. |

Sintassi della risposta:

```
{
  "parameters": [
    {
      "key": "string",
      "defaultValue": "string",
      "type": "string",
      "description": "string",
      "isNoEcho": boolean
    },
  ]
}
```

| Campo | Tipo | Campo obbligatorio | Descrizione |
|-----------|---------|--------------------|--|
| parametri | elenco | Sì | L'elenco dei parametri che Service Catalog chiede all'utente finale di fornire durante il provisioning di un prodotto o l'aggiornamento di un prodotto fornito. Se nell'elemento non è definito alcun parametro, viene restituito un elenco vuoto. |
| key | stringa | Sì | La chiave del parametro. |

| Campo | Tipo | Campo obbligatorio | Descrizione |
|--------------|----------|--------------------|--|
| defaultValue | stringa | No | Il valore predefinito del parametro se l'utente finale non fornisce un valore. |
| tipo | stringa | Sì | Il tipo previsto del valore del parametro per il motore. Ad esempio, una stringa, un valore booleano o una mappa. I valori consentiti sono specifici per ogni motore. Service Catalog passa ogni valore di parametro al motore come stringa. |
| description | stringa | No | Descrizione del parametro. Si raccomanda che sia facile da usare. |
| isNoEcho | booleano | no | Determina se il valore del parametro non viene ripreso nei log. Il valore predefinito è falso (i valori dei parametri vengono ripresi). |

Fornitura

Per l'[ProvisionProduct](#) operazione, Service Catalog delega l'effettivo approvvigionamento delle risorse al motore. Il motore è responsabile dell'interfacciamento con la soluzione IaC preferita (come

Terraform) per fornire le risorse come definito nell'artefatto. Il motore è inoltre responsabile della notifica del risultato a Service Catalog.

Service Catalog invia tutte le richieste di Provision a una coda Amazon SQS nel tuo account denominato. `ServiceCatalogExternalProvisionOperationQueue`

Sintassi della richiesta:

```
{
  "token": "string",
  "operation": "string",
  "provisionedProductId": "string",
  "provisionedProductName": "string",
  "productId": "string",
  "provisioningArtifactId": "string",
  "recordId": "string",
  "launchRoleArn": "string",
  "artifact": {
    "path": "string",
    "type": "string"
  },
  "identity": {
    "principal": "string",
    "awsAccountId": "string",
    "organizationId": "string"
  },
  "parameters": [
    {
      "key": "string",
      "value": "string"
    }
  ],
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

| Campo | Tipo | Campo obbligatorio | Descrizione |
|------------------------|---------|--------------------|--|
| token | stringa | Sì | Il token che identifica questa operazione. Il token deve essere restituito a Service Catalog per notificare i risultati dell'esecuzione. |
| operation | stringa | Sì | Questo campo deve essere utilizzato o PROVISION_PRODUCT per questa operazione. |
| provisionedProductId | stringa | Sì | ID del prodotto fornito. |
| provisionedProductName | stringa | Sì | Nome del prodotto fornito. |
| ID del prodotto | stringa | Sì | ID del prodotto. |
| provisioningArtifactId | stringa | Sì | ID dell'elemento di approvvigionamento. |
| recordId | stringa | Sì | ID del record Service Catalog per questa operazione. |
| launchRoleArn | stringa | Sì | Amazon Resource Name (ARN) per il ruolo IAM da utilizzare e per il provisioning delle risorse. |
| artefatto | oggetto | Sì | Dettagli sull'artefatto che definisce il modo |

| Campo | Tipo | Campo obbligatorio | Descrizione |
|--------------------|---------|--------------------|--|
| | | | in cui vengono fornite le risorse. |
| artefatto/percorso | stringa | Sì | Posizione da cui il motore scarica l'artefatto. Ad esempio, perAWS_S3, questo è l'URI di Amazon S3. |
| artefatto/tipo | stringa | Sì | Tipo di artefatto. Valore consentito:. AWS_S3 |
| identità | stringa | No | Il campo non è attualmente utilizzato. |
| parametri | elenco | Sì | Elenco delle coppie chiave-valore dei parametri immesse dall'utente in Service Catalog come input per questa operazione. |
| tag | elenco | Sì | Elenco key-value -pairs degli utenti inseriti in Service Catalog come tag da applicare alle risorse fornite. |

Notifica dei risultati del flusso di lavoro:

Richiama l'[NotifyProvisionProductEngineWorkflowResult](#) API con l'oggetto di risposta specificato nella pagina dei dettagli dell'API.

Aggiornamento in corso

Per l'[UpdateProvisionedProduct](#) operazione, Service Catalog delega l'aggiornamento effettivo delle risorse al motore. Il motore è responsabile dell'interfacciamento con la soluzione IaC preferita (come Terraform) per l'aggiornamento delle risorse come definito nell'artefatto. Il motore è inoltre responsabile della notifica del risultato a Service Catalog.

Service Catalog invia tutte le richieste di aggiornamento a una coda Amazon SQS nel tuo account denominato `ServiceCatalogExternalUpdateOperationQueue`

Sintassi della richiesta:

```
{
  "token": "string",
  "operation": "string",
  "provisionedProductId": "string",
  "provisionedProductName": "string",
  "productId": "string",
  "provisioningArtifactId": "string",
  "recordId": "string",
  "launchRoleArn": "string",
  "artifact": {
    "path": "string",
    "type": "string"
  },
  "identity": {
    "principal": "string",
    "awsAccountId": "string",
    "organizationId": "string"
  },
  "parameters": [
    {
      "key": "string",
      "value": "string"
    }
  ],
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

}

| Campo | Tipo | Campo obbligatorio | Descrizione |
|------------------------|---------|--------------------|--|
| token | stringa | Sì | Il token che identifica questa operazione. Il token deve essere restituito a Service Catalog per notificare e i risultati dell'esecuzione. |
| operation | stringa | Sì | Questo campo deve essere utilizzato o UPDATE_PROVISIONING_PRODUCT per questa operazione. |
| provisionedProductId | stringa | Sì | ID del prodotto fornito. |
| provisionedProductName | stringa | Sì | Nome del prodotto fornito. |
| ID del prodotto | stringa | Sì | ID del prodotto. |
| provisioningArtifactId | stringa | Sì | ID dell'elemento di approvvigionamento. |
| recordId | stringa | Sì | ID del record Service Catalog per questa operazione. |
| launchRoleArn | stringa | Sì | Amazon Resource Name (ARN) per il ruolo IAM da utilizzare e per il provisioning delle risorse. |

| Campo | Tipo | Campo obbligatorio | Descrizione |
|--------------------|---------|--------------------|--|
| artefatto | oggetto | Sì | Dettagli sull'artefatto che definisce il modo in cui vengono fornite le risorse. |
| artefatto/percorso | stringa | Sì | Posizione da cui il motore scarica l'artefatto. Ad esempio, perAWS_S3, questo è l'URI di Amazon S3. |
| artefatto/tipo | stringa | Sì | Tipo di artefatto. Valore consentito: AWS_S3 |
| identità | stringa | No | Il campo non è attualmente utilizzato. |
| parametri | elenco | Sì | Elenco delle coppie chiave-valore dei parametri immesse dall'utente in Service Catalog come input per questa operazione. |
| tag | elenco | Sì | Elenco key-value -pairs degli utenti inseriti in Service Catalog come tag da applicare alle risorse fornite. |

Notifica dei risultati del flusso di lavoro:

Richiama l'[NotifyUpdateProvisionedProductEngineWorkflowResult](#) API con l'oggetto di risposta specificato nella pagina dei dettagli dell'API.

Terminare

Per l'[TerminateProvisionedProduct](#) operazione, Service Catalog delega l'effettiva cessazione delle risorse al motore. Il motore è responsabile dell'interfacciamento con la soluzione IaC preferita (come Terraform) per terminare le risorse come definito nell'artefatto. Il motore è inoltre responsabile della notifica del risultato a Service Catalog.

Service Catalog invia tutte le richieste Terminate a una coda Amazon SQS nel tuo account denominato `ServiceCatalogExternalTerminateOperationQueue`.

Sintassi della richiesta:

```
{
  "token": "string",
  "operation": "string",
  "provisionedProductId": "string",
  "provisionedProductName": "string",
  "recordId": "string",
  "launchRoleArn": "string",
  "identity": {
    "principal": "string",
    "awsAccountId": "string",
    "organizationId": "string"
  }
}
```

| Campo | Tipo | Campo obbligatorio | Descrizione |
|-------|---------|--------------------|--|
| token | stringa | Sì | Il token che identifica questa operazione. Il token deve essere restituito a Service Catalog per notificare e i risultati dell'esecuzione. |

| Campo | Tipo | Campo obbligatorio | Descrizione |
|------------------------|---------|--------------------|---|
| operation | stringa | Sì | Questo campo deve essere utilizzato o <code>TERMINATE_PROVISION_PRODUCT</code> per questa operazione. |
| provisionedProductId | stringa | Sì | ID del prodotto fornito. |
| provisionedProductName | stringa | Sì | Nome del prodotto fornito. |
| recordId | stringa | Sì | ID del record Service Catalog per questa operazione. |
| launchRoleArn | stringa | Sì | Amazon Resource Name (ARN) per il ruolo IAM da utilizzare e per il provisioning delle risorse. |
| identità | stringa | No | Il campo non è attualmente utilizzato. |

Notifica dei risultati del flusso di lavoro:

Richiama l'[NotifyTerminateProvisionedProductEngineWorkflowResult](#) API con l'oggetto di risposta specificato nella pagina dei dettagli dell'API.

Assegnazione di tag

Per gestire i tag tramite Resource Groups, il tuo ruolo di lancio richiede le seguenti istruzioni di autorizzazione aggiuntive:

```
{
```

```
"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

Il ruolo di lancio richiede anche le autorizzazioni di etichettatura sulle risorse specifiche dell'artefatto, ad esempio. `ec2:CreateTags`

Monitoraggio in AWS Service Catalog

Puoi monitorare AWS Service Catalog le tue risorse utilizzando Amazon CloudWatch, che raccoglie ed elabora i dati grezzi AWS Service Catalog trasformandoli in metriche leggibili. Queste statistiche vengono registrate per un periodo di due settimane, in modo da poter accedere alle informazioni storiche e avere una prospettiva migliore sulle prestazioni del servizio. AWS Service Catalog i dati metrici vengono inviati automaticamente CloudWatch in periodi di 1 minuto. Per ulteriori informazioni CloudWatch, consulta la [Amazon CloudWatch User Guide](#).

Per un elenco di parametri e dimensioni disponibili, consulta [AWS Service Catalog CloudWatch Metriche](#).

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni delle AWS Service Catalog tue AWS soluzioni. È necessario raccogliere i dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica. Prima di iniziare il monitoraggio AWS Service Catalog, è necessario creare un piano di monitoraggio che includa le risposte alle seguenti domande:

- Quali sono gli obiettivi del monitoraggio?
- Di quali risorse si intende eseguire il monitoraggio?
- Con quale frequenza sarà eseguito il monitoraggio di queste risorse?
- Quali strumenti di monitoraggio verranno utilizzati?
- Chi eseguirà i processi di monitoraggio?
- Chi deve ricevere una notifica quando si verifica un problema?

Strumenti di monitoraggio

AWS fornisce vari strumenti che è possibile utilizzare per il monitoraggio AWS Service Catalog. Alcuni di questi strumenti possono essere configurati in modo che eseguano automaticamente il monitoraggio, mentre altri richiedono l'intervento manuale. Si consiglia di automatizzare il più possibile i processi di monitoraggio.

Strumenti di monitoraggio automatici

Puoi utilizzare Amazon CloudWatch alarms per monitorare AWS Service Catalog e segnalare interruzioni.

CloudWatch gli allarmi controllano una singola metrica in un periodo di tempo specificato ed eseguono una o più azioni in base al valore della metrica rispetto a una determinata soglia in diversi periodi di tempo. L'azione è una notifica inviata a un argomento di Amazon Simple Notification Service (Amazon SNS) o a una politica di Amazon Auto EC2 Scaling. CloudWatch gli allarmi non richiamano azioni semplicemente perché si trovano in uno stato particolare; lo stato deve essere cambiato e mantenuto per un determinato numero di periodi. Per informazioni su come creare un allarme, consulta [Creazione di CloudWatch allarmi Amazon](#). Per ulteriori informazioni sull'utilizzo dei CloudWatch parametri di Amazon con AWS Service Catalog, consulta [AWS Service Catalog CloudWatch Metriche](#).

AWS Service Catalog CloudWatch Metriche

Puoi monitorare AWS Service Catalog le tue risorse utilizzando Amazon CloudWatch, che raccoglie ed elabora i dati grezzi AWS Service Catalog trasformandoli in metriche leggibili. Queste statistiche vengono registrate per un periodo di due settimane, in modo da poter accedere alle informazioni storiche e avere una prospettiva migliore sulle prestazioni del servizio. AWS Service Catalog i dati metrici vengono inviati automaticamente CloudWatch in periodi di 1 minuto. Per ulteriori informazioni CloudWatch, consulta la [Amazon CloudWatch User Guide](#).

Argomenti

- [Abilitazione delle CloudWatch metriche](#)
- [Parametri e dimensioni disponibili](#)
- [Visualizzazione delle metriche AWS Service Catalog](#)

Abilitazione delle CloudWatch metriche

Le CloudWatch metriche di Amazon sono abilitate per impostazione predefinita.

Parametri e dimensioni disponibili

Le metriche e le dimensioni AWS Service Catalog inviate ad Amazon CloudWatch sono elencate di seguito.

AWS Service Catalog Metriche

Lo spazio dei nomi AWS/ServiceCatalog include i parametri descritti di seguito.

| Metrica | Description |
|------------------------------|---|
| ProvisionedProductLaunch | <p>Il numero di prodotti assegnati avviati per un prodotto specifico e artefatto di provisioning in un periodo di tempo specificato. Le dimensioni vengono pubblicate come record separati nei CloudWatch log.</p> <p>Unità: Count</p> <p>Statistiche valide:Minimum,,Maximum, Sum Average</p> <p>Dimensioni:State,PPState,ProductId , ProvisioningArtifactId</p> |
| ProductProvisioningOperation | <p>Il numero di operazioni eseguite sull'id del prodotto,provisioningArtifactId . Le dimensioni vengono pubblicate come un unico record nei CloudWatch log.</p> <p>Unità: Count</p> <p>Statistiche valide:Minimum,,Maximum, Sum Average</p> <p>Dimensioni:State,PPState,ProductId , ProvisioningArtifactId</p> |

Dimensioni per le AWS Service Catalog metriche

AWS Service Catalog invia le seguenti dimensioni ad Amazon CloudWatch.

| Dimensione | Description |
|------------|--|
| PPState | <p>Questa dimensione esegue il filtro dei dati richiesti per tutti i prodotti assegnati avviati con questo stato specificato. Ciò consente di organizzare i dati in categorie in base allo stato di avvio.</p> <p>Stato valido: DISPONIBILE, CONTAMINATO, ERRORE</p> |

| Dimensione | Description |
|------------------------|--|
| ProductId | Questa dimensione esegue il filtro dei dati richiesti solo per l'ID prodotto identificato. Questo consente di evidenziare un prodotto esatto da cui eseguire l'avvio. |
| ProvisioningArtifactId | Questa dimensione esegue il filtro dei dati richiesti solo per l'ID artefatto di provisioning identificato. Questo consente di evidenziare una versione esatta di prodotti da cui eseguire l'avvio. |
| State | Questa dimensione esegue il filtro dei dati richiesti per tutti i prodotti assegnati avviati con questo stato specificato. Ciò consente di organizzare i dati in categorie in base allo stato di avvio. Stato valido: SUCCEEDED, FAILED |

Visualizzazione delle metriche AWS Service Catalog

Puoi visualizzare i CloudWatch parametri di Amazon nella CloudWatch console Amazon, che fornisce una visualizzazione dettagliata e personalizzabile delle tue risorse, nonché il numero di attività in esecuzione in un servizio.

Argomenti

- [Visualizzazione delle AWS Service Catalog metriche nella console Amazon CloudWatch](#)

Visualizzazione delle AWS Service Catalog metriche nella console Amazon CloudWatch

Puoi visualizzare le AWS Service Catalog metriche nella CloudWatch console Amazon. La CloudWatch console Amazon fornisce una visualizzazione dettagliata delle AWS Service Catalog metriche e puoi personalizzare le visualizzazioni in base alle tue esigenze. Per ulteriori informazioni su Amazon CloudWatch, consulta la [Amazon CloudWatch User Guide](#).

Per visualizzare le metriche nella console Amazon CloudWatch

1. Apri la CloudWatch console Amazon all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.
2. Nella sezione Metrics (Parametri) nel riquadro di navigazione a sinistra, scegliere Service Catalog.
3. Scegli i parametri da visualizzare.

Registrazione delle chiamate AWS Service Catalog API utilizzando AWS CloudTrail

AWS Service Catalog è integrato con AWS CloudTrail, un servizio che fornisce una registrazione delle azioni intraprese da un utente, un ruolo o un AWS servizio in AWS Service Catalog. CloudTrail acquisisce tutte le chiamate API AWS Service Catalog come eventi. Le chiamate acquisite includono chiamate dalla AWS Service Catalog console e chiamate di codice alle operazioni AWS Service Catalog API. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per. AWS Service Catalog Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare a quale richiesta è stata inviata AWS Service Catalog, l'indirizzo IP da cui è stata effettuata, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la [Guida AWS CloudTrail per l'utente](#).

AWS Service Catalog informazioni in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione. Quando si verifica un'attività in AWS Service Catalog, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo AWS account. Per ulteriori informazioni, consulta [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#).

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi di AWS Service Catalog, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare

ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Panoramica della creazione di un percorso](#)
- [AWS CloudTrail servizi e integrazioni supportati](#)
- [Configurazione delle notifiche Amazon SNS per AWS CloudTrail](#)
- [Ricezione di file di AWS CloudTrail registro da più regioni](#) e [ricezione di file di AWS CloudTrail registro da più account](#)

CloudTrail [registra tutte le](#) AWS Service Catalog azioni. Ad esempio, le chiamate a [CreateProduct](#) e [UpdateProvisionedProduct](#) le azioni generano voci nei file di CloudTrail registro. [CreatePortfolio](#)

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta [Elemento CloudTrail userIdentity](#).

Comprensione delle AWS Service Catalog voci dei file di registro

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico. L'esempio seguente mostra una voce di CloudTrail registro che illustra l'CreateApplicationAPI.

```
{
  "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 boto3/1.17.63",
  "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"
}

```

Preferenze di branding della console

AWS Service Catalog consente agli amministratori di specificare le preferenze di branding della console per gli account. Gli amministratori possono utilizzare il marchio della console per specificare il nome dell'azienda, l'immagine del logo e un colore primario e secondario (accento) per una varietà di componenti del sito. Queste preferenze di branding sono visibili sia agli amministratori che agli utenti finali quando utilizzano la console.

Le preferenze di branding della console migliorano l'aspetto di un account e consentono di ottenere quanto segue:

- Crea una transizione visiva senza interruzioni tra la console e le applicazioni interne
- Distingue gli account utilizzati da diversi team interni all'interno della stessa azienda
- Distingue gli account in più ambienti, come lo sviluppo, la gestione temporanea o la produzione

Note

Gli amministratori specificano le preferenze di branding della console a livello di account.

Per specificare le preferenze di branding della console

1. Nel menu di navigazione a sinistra, scegli Preferenze.
2. Scegli Modifica per le preferenze di branding in modalità chiara o in modalità scura.
3. Carica un logo, inserisci il nome del marchio, quindi seleziona il Colore primario e il Colore secondario.
4. Scegli Save (Salva).

Per un elenco delle aree geografiche in cui è AWS Service Catalog supportato il marchio delle console, consulta il [Regione AWS supporto per il branding delle console](#).

Regione AWS supporto per le preferenze di branding della console

AWS Service Catalog supporta le preferenze di branding delle console Regioni AWS elencate nella tabella seguente.

| Regione AWS nome | Regione AWS identità |
|---|----------------------|
| Stati Uniti orientali (Virginia settentrionale) | us-east-1 |
| Stati Uniti orientali (Ohio) | us-east-2 |
| Stati Uniti occidentali (California settentrionale) | us-west-1 |
| US West (Oregon) | us-west-2 |
| Africa (Città del Capo) | af-south-1 |
| Asia Pacific (Hong Kong) | ap-east-1 |
| Asia Pacifico (Giacarta) | ap-southeast-3 |
| Asia Pacifico (Mumbai) | ap-south-1 |
| Asia Pacifico (Osaka-Locale) | ap-northeast-3 |
| Asia Pacifico (Seoul) | ap-northeast-2 |
| Asia Pacific (Singapore) | ap-southeast-1 |
| Asia Pacific (Sydney) | ap-southeast-2 |
| Asia Pacific (Tokyo) | ap-northeast-1 |
| Canada (Central) | ca-central-1 |
| Europa (Francoforte) | eu-central-1 |
| Europe (Ireland) | eu-west-1 |
| Europe (London) | eu-west-2 |
| Europe (Milan) | eu-south-1 |
| Europa (Parigi) | eu-west-3 |

| Regione AWS nome | Regione AWS identità | |
|--|----------------------|--|
| Europe (Stockholm) | eu-north-1 | |
| Medio Oriente (Bahrein) | me-south-1 | |
| Sud America (San Paolo) | sa-east-1 | |
| AWS GovCloud (Stati Uniti orientali) | us-gov-east-1 | |
| AWS GovCloud (Stati Uniti occidentali) | us-gov-west-1 | |

Cronologia dei documenti

La tabella seguente descrive le modifiche importanti alla documentazione per AWS Service Catalog. Per ricevere notifiche sugli aggiornamenti di questa documentazione, è possibile iscriversi a un feed RSS.

- Versione API: 12-11-2014
- Ultimo aggiornamento della documentazione: 16 maggio 2024

| Modifica | Descrizione | Data |
|--|---|----------------|
| Motori esterni per AWS Service Catalog | <p>AWS Service Catalog aggiunge nuova documentazione per i motori esterni.</p> <p>I motori esterni sono rappresentati tramite un tipo di EXTERNAL prodotto. Il tipo di EXTERNAL prodotto consente l'integrazione di motori di provisioning di terze parti, come Terraform. È possibile utilizzare motori esterni per estendere le funzionalità di Service Catalog oltre i AWS CloudFormation modelli nativi, abilitando l'uso di altri strumenti Instructure as Code (IaC). Per ulteriori informazioni, vedere Motori esterni per AWS Service Catalog</p> | 16 maggio 2024 |
| Aggiornamento IAM di sicurezza | <p>AWS Service Catalog aggiorna la <code>AWSServiceCatalogSyncServiceRolePolicy</code> politica a <code>codestar-connectio</code></p> | 7 maggio 2024 |

ns cui passarecodeconne
 ctions . Per ulteriori
 informazioni, consulta [Policy
 gestite da AWS per AWS
 Service Catalog AppRegistry](#).

Aggiornamenti precedenti

La tabella seguente descrive la cronologia dei rilasci della documentazione AWS Service Catalog precedenti al 25 aprile 2024.

| Funzionalità | Description | Data di rilascio |
|---------------------|---|------------------|
| AWS Service Catalog | Per ulteriori informazioni sulle modifiche apportate da Hashicorp alle licenze Terraform e all'aggiornamento al tipo di prodotto External, consulta. Aggiornamento dei prodotti Terraform Open Source esistenti e dei prodotti forniti al tipo di prodotto esterno | 20 ottobre 2023 |
| AWS Service Catalog | Per ulteriori informazioni sulla condivisione di un portafoglio AWS Organizations e sull'autorizzazione AWS Service Catalog alla sincronizzazione con AWS Organizations , consulta la AWSServiceCatalogOrgsDataSyncServiceRolePolicy politica e il ruolo collegato al servizio. AWSServiceRoleForServiceCatalogOrgsDataSync | 14 aprile 2023 |

| Funzionalità | Description | Data di rilascio |
|--|--|------------------|
| AWS Service Catalog | Per saperne di più sulla gestione dei prodotti connessi a git e su come consentire e AWS Service Catalog la sincronizzazione dei modelli in un archivio esterno con i tuoi AWS Service Catalog prodotti, consulta la policy e il ruolo collegato ai servizi. AWSServiceCatalogSyncServiceRolePolicyAWSServiceRoleForServiceCatalogSync | 18 novembre 2022 |
| AWS Service Catalog AppRegistry | Per ulteriori informazioni su come è possibile AppRegistry archiviare AWS le applicazioni, le raccolte di risorse associate e i gruppi di attributi delle applicazioni, consulta. AWS Service Catalog AppRegistry | 15 giugno 2022 |
| AWS Service Management Connector | Per ulteriori informazioni su Connectors for Jira Service Management e ServiceNow, consulta AWS Service Management Connector . | 09 giugno 2022 |
| Connettore per Jira Service Management | Per ulteriori informazioni sugli aggiornamenti al Connector for Jira Service Management, consulta AWS Service Management Connector for Jira Service Management . | 25 maggio 2021 |

| Funzionalità | Description | Data di rilascio |
|----------------------------------|--|-------------------|
| Connettore per ServiceNow | Per informazioni sugli aggiornamenti al Connector per ServiceNow, vedi AWS Service Management Connector per ServiceNow . | 7 Aprile 2021 |
| Connettore per ServiceNow | Per informazioni sugli aggiornamenti al Connector per ServiceNow, vedi AWS Service Management Connector per ServiceNow . | 24 settembre 2020 |
| AWS Service Quotas | Per informazioni su come AWS Service Catalog funziona con AWS Service Quotas, consulta Service Quotas AWS Service Catalog predefinite . | 24 marzo 2020 |
| Libreria introduttiva | Per ulteriori informazioni sulla libreria di modelli di prodotto ben progettati offerta da, consulta AWS Service Catalog Libreria introduttiva | 10 marzo 2020 |
| Guida alla versione | Per ulteriori informazioni sulle linee guida sulla versione del prodotto, consulta la Guida alla versione . | 17 dicembre 2019 |
| Connettore per Jira Service Desk | Per iniziare a utilizzare il Connector for Jira Service Desk, consulta AWS Service Management Connector per Jira Service Desk . | 21 novembre 2019 |

| Funzionalità | Description | Data di rilascio |
|--|--|------------------|
| Connettore per ServiceNow | Per informazioni sugli aggiornamenti al Connector per ServiceNow, vedi AWS Service Management Connector per ServiceNow . | 18 novembre 2019 |
| Nuovo capitolo sulla sicurezza | Per ulteriori informazioni sulla sicurezza in AWS Service Catalog, vedi Sicurezza in AWS Service Catalog . | 31 ottobre 2019 |
| Modifica del proprietario del prodotto assegnato | Per ulteriori informazioni su come modificare il proprietario dei prodotti forniti, consulta Changing Provisioned Product Owner . | 31 ottobre 2019 |
| Nuovo vincolo di aggiornamento delle risorse | Per informazioni su come utilizzare il vincolo RESOURCE_UPDATE per aggiornare i tag nei prodotti forniti, consulta Tag Update Constraints .AWS Service Catalog | 17 aprile 2019 |
| Connettore per ServiceNow | Per iniziare a utilizzare il Connector per ServiceNow, vedi AWS Service Management Connector per ServiceNow . | 19 marzo 2019 |
| Support per AWS CloudFormation StackSets | Per iniziare a usare AWS CloudFormation StackSets, vedi Uso AWS CloudFormation StackSets . | 14 novembre 2018 |

| Funzionalità | Description | Data di rilascio |
|---|--|-------------------|
| Operazioni self-service | Per iniziare a utilizzare le azioni self-service, vedi AWS CloudFormation Service Actions . | 17 ottobre 2018 |
| CloudWatch Metriche Amazon | Per ulteriori informazioni sui CloudWatch parametri di Amazon, consulta AWS Service Catalog Amazon CloudWatch . | 26 settembre 2018 |
| Support per TagOptions | Per gestire i tag, consulta AWS Service Catalog TagOptionLibreria . | 28 giugno 2017 |
| Importazione di un portafoglio | Per importare un portafoglio condiviso da un altro AWS account, vedi Importazione di un portafoglio . | 16 febbraio 2016 |
| Aggiornamenti delle informazioni sulle autorizzazioni | Per concedere l'accesso alla visualizzazione della console dell'utente finale, consulta Accesso alla console per gli utenti finali . | 16 febbraio 2016 |
| Rilascio iniziale | Questa è la versione iniziale della Guida per l' AWS Service Catalog amministratore. | 9 luglio 2015 |

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.