aws

User Guide

AWS Proton

AWS Proton: User Guide

Table of Contents

Was ist AWS Proton?

AWS Protonist:

- Automatisierte Infrastruktur als Code-Provisioning und Bereitstellung von serverlosen und containerbasierten Anwendungen

  DieAWS Protonservice ist ein zweigleisiges Automatisierungs-Framework. Als Administrator erstellen Sieversionierte Servicevorlagendie standardisierte Infrastruktur und Bereitstellungstools für serverlose und containerbasierte Anwendungen definieren. Als Anwendungsentwickler können Sie aus den verfügbarenService-Vorlagenum Ihre Anwendungs- oder Servicebereitstellungen zu automatisieren.

  AWS Protonidentifiziert alle vorhandenenService-Instancesdie eine veraltete Vorlagenversion für Sie verwenden. Als Administrator können Sie eine Anfrage stellenAWS Protonum sie mit einem Klick zu aktualisieren.
- Standardisierte Infrastruktur

  Plattformteams können nutzenAWS Protonund versionierte Infrastruktur als Codevorlagen. Sie können diese Vorlagen verwenden, um Standardanwendungs-Stacks zu definieren und zu verwalten, die die Architektur, Infrastrukturressourcen und die CI/CD-Softwarebereitstellungspipeline enthalten.
- In CI/CD integrierte Bereitstellungen

  Wenn Entwickler dasAWS ProtonSelf-Service-Oberfläche zur Auswahl einesService-Instancewählen sie eine standardisierte Anwendungs-Stack-Definition für ihre Codebereitstellungen aus.AWS Protonstellt die Ressourcen automatisch bereit, konfiguriert die CI/CD-Pipeline und stellt den Code in der definierten Infrastruktur bereit.

AWS Protonfür Plattformteams

Erstellen Sie als Administrator oder Mitglieder Ihres PlattformteamsUmgebungs-TemplatesundService-Vorlagenenthält Infrastruktur als Code. Dieumgebung-vorlagedefiniert gemeinsam genutzte Infrastruktur, die von mehreren Anwendungen oder Ressourcen genutzt wird. DieService-Instancedefiniert die Art der Infrastruktur, die für die Bereitstellung und Wartung einer einzelnen Anwendung oder eines Microservices in einemUmweltaus. Importieren in &S3;AWS Proton Bedienungist eine Instanziierung von aService-Instance, das normalerweise

mehrereService-Instancesund einRohrleitungaus. Importieren in &S3;AWS Proton Service-Instanceist eine Instanziierung von aService-Instancein einer bestimmtenUmweltaus. Sie oder andere Mitglieder Ihres Teams können angeben, welcheUmgebungs-Templatessind kompatibel mit einem bestimmtenService-Instanceaus. Weitere Informationen zuVorlagenfinden Sie unterAWS Proton-Vorlagenaus.

Sie können die folgende Infrastruktur als -Codeprovider verwenden mitAWS Proton:

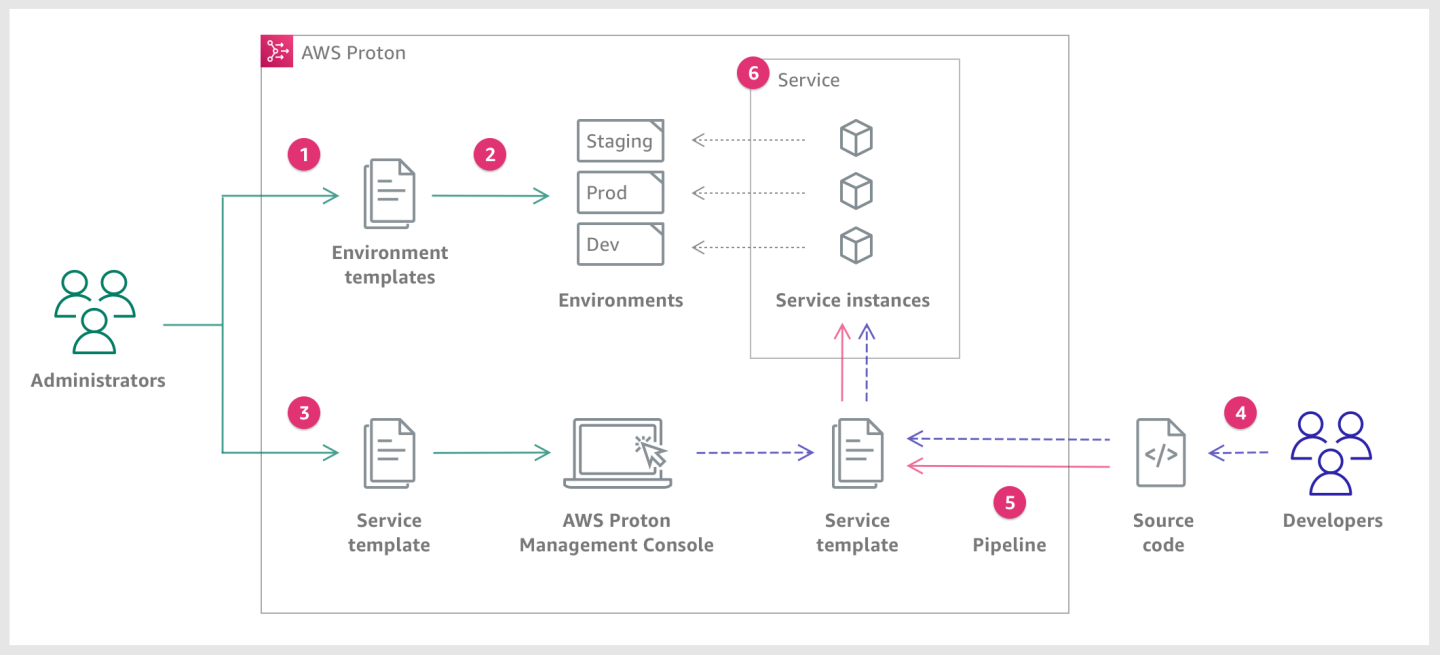
- AWS CloudFormation
- Terraform

AWS Protonfür Entwickler

Als Anwendungsentwickler wählen Sie eine standardisierteService-InstanceDasAWS Protonverwendet, um eine zu erstellenBedienungdie Ihre Anwendung in einemService-Instanceaus. Importieren in &S3;AWS Proton Bedienungist eine Instanziierung von aService-Instance, das normalerweise mehrereService-Instancesund einRohrleitungaus.

AWS ProtonArbeitsablauf

Das folgende Diagramm ist eine Visualisierung der wichtigstenAWS ProtonKonzepte, die im vorherigen Absatz erörtert wurden. Es bietet auch einen allgemeinen Überblick darüber, was eine einfacheAWS Proton-Workflow.



1. Als-Administratorerstellen und registrieren Sie eineUmwelt TemplatemitAWS Proton, das die gemeinsam genutzten Ressourcen definiert.

2. AWS Protonstellt mindestens eine bereitUmgebungen, basierend auf einemUmwelt Templateaus.

3. Als-Administratorerstellen und registrieren Sie eineServicevorlagemitAWS Proton, die die zugehörigen Infrastruktur-, Monitoring- und CI/CD-Ressourcen definiert sowie kompatibelUmgebungen-Vorlageaus.

4. AlsDev Sie ein registriertesServicevorlageund geben Sie einen Link zu IhremQuellcode-Repository.

5. AWS Proton-Bestimmungen-Servicemit einemCI/CD-PipelinefürService-Instancesaus.

6. AWS Protonstellt bereit und verwaltet die-Serviceund dieService-Instancesdie laufenQuellcodewie in der ausgewählten definiert wurdeServicevorlageaus. EINService-Instanceist eine Instanziierung des ausgewähltenServicevorlagein einemUmgebungfür eine einzelne Stufe einerPipeline(zum Beispiel Prod).

Einrichtung

Führen Sie die Aufgaben in diesem Abschnitt aus, damit Sie Service- und Umgebungsvorlagen erstellen und registrieren können. Sie benötigen diese, um Umgebungen und Dienste bereitzustellenAWS Proton.

> **Note**
>
> Wir bieten sie ohne zusätzliche Kosten AWS Proton an. Sie können Service- und Umgebungsvorlagen kostenlos erstellen, registrieren und verwalten. Sie können sich auch AWS Proton darauf verlassen, dass die eigenen Abläufe wie Speicher, Sicherheit und Bereitstellung selbst verwaltet werden. Die einzigen Kosten, die Ihnen bei der Nutzung entstehen, AWS Proton sind die folgenden.
>
> - Kosten für die Bereitstellung und Nutzung von AWS Cloud Ressourcen, die Sie in Auftrag gegeben habenAWS Proton, für Sie bereitzustellen und zu warten.
> - Kosten für die Aufrechterhaltung einer AWS CodeStar Verbindung zu Ihrem Code-Repository.
> - Kosten für die Wartung eines Amazon S3 S3-Buckets, wenn Sie einen Bucket verwenden, um Eingaben dafür bereitzustellenAWS Proton. Sie können diese Kosten vermeiden, wenn Sie auf die the section called “Konfigurationen für die Vorlagensynchronisierung” Verwendung von Git-Repositorys für Ihre the section called “Vorlagenpakete” umsteigen.

Themen

Einrichtung mit IAM

Wenn Sie sich für registrierenAWS, AWS-Konto ist Ihr automatisch für alle Dienste in angemeldetAWS, einschließlichAWS Proton. Ihnen werden nur die Dienste und Ressourcen in Rechnung gestellt, die Sie nutzen.

> **Note**
>
> Sie und Ihr Team, einschließlich Administratoren und Entwickler, müssen sich alle unter demselben Konto befinden.

Registrieren bei AWS

Wenn Sie kein AWS-Konto haben, führen Sie die folgenden Schritte zum Erstellen durch.

Anmeldung für ein AWS-Konto

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

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

   Wenn Sie sich für ein AWS-Konto anmelden, wird ein Root-Benutzer des AWS-Kontos erstellt. Der Stammbenutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Methode zur Gewährleistung der Sicherheit sollten Sie den administrativen Zugriff einem administrativen Benutzer zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, die einen Root-Benutzerzugriff erfordern.

Erstellen eines IAM-Benutzers

Wählen Sie zum Erstellen eines Administratorbenutzers eine der folgenden Optionen aus.

Wählen Sie eine Möglichkeit zur Verwaltung Ihres Administrators aus.	Bis	Von	Sie können auch
Im IAM Identity Center (Empfohlen)	Verwendung von kurzfristigen Anmeldeinformationen für den Zugriff auf AWS. Dies steht im Einklang mit den bewährten Methoden für die Sicherheit. Weitere Informationen zu bewährten Methoden finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.	Beachtung der Anweisungen unter Erste Schritte im AWS IAM Identity Center-Benutzerhandbuch.	Programmgesteuerten Zugriff unter Berücksichtigung der Informationen im Abschnitt Konfigurieren von AWS CLI für die Verwendung vonAWS IAM Identity Center im AWS Command Line Interface-Benutzerhandbuch konfigurieren.
In IAM (Nicht empfohlen)	Verwendung von langfristigen Anmeldeinformationen für den Zugriff auf AWS.	Beachtung der Anweisungen unter Erstellen Ihres ersten IAM-Administratorbenutzers und Ihrer ersten Benutzergruppe im IAM-Benutzerhandbuch.	Programmgesteuerten Zugriff unter Verwendung der Informationen unter Verwalten der Zugriffsschlüssel für IAM-Benutzer im IAM-Benutzerhandbuch konfigurieren.

AWS ProtonServicerollen einrichten

Es gibt einige IAM-Rollen, die Sie möglicherweise für verschiedene Teile Ihrer AWS Proton Lösung erstellen möchten. Sie können sie im Voraus mit der IAM-Konsole erstellen, oder Sie können die AWS Proton Konsole verwenden, um sie für Sie zu erstellen.

Erstellen Sie AWS Proton Umgebungsrollen, AWS Proton damit Sie in Ihrem Namen API-Aufrufe an andere AWS-Services AWS CloudFormationAWS CodeBuild, z. B. verschiedene Rechen- und Speicherdienste tätigen können, um Ressourcen für Sie bereitzustellen. Eine AWS-verwaltete Bereitstellungsrolle ist erforderlich, wenn eine Umgebung oder eine der darin ausgeführten Dienstinstanzen AWS-managed Provisioning verwendet. Eine CodeBuildRolle ist erforderlich, wenn eine Umgebung oder eine ihrer Dienstinstanzen Provisioning verwendet. CodeBuild Weitere Informationen zu den AWS Proton Umgebungsrollen finden Sie unterthe section called “IAM-Rollen”. Wenn Sie eine Umgebung erstellen, können Sie die AWS Proton Konsole verwenden, um eine vorhandene Rolle für eine dieser beiden Rollen auszuwählen oder eine Rolle mit Administratorrechten für Sie zu erstellen.

Erstellen Sie auf ähnliche Weise AWS Proton Pipeline-Rollen, AWS Proton damit Sie in Ihrem Namen API-Aufrufe an andere Dienste tätigen können, um eine CI/CD-Pipeline für Sie bereitzustellen. Weitere Informationen zu den AWS Proton Pipeline-Rollen finden Sie unter. the section called “Rollen im Pipeline-Dienst” Weitere Informationen zur Konfiguration der CI/CD-Einstellungen finden Sie unter. the section called “Einrichtung der CI/CD-Pipeline-Einstellungen für das Konto”

> **Note**
>
> Da wir nicht wissen, welche Ressourcen Sie in Ihren AWS Proton Vorlagen definieren werden, verfügen die Rollen, die Sie mit der Konsole erstellen, über umfassende Berechtigungen und können sowohl als AWS Proton Pipeline-Dienstrollen als auch als Servicerollen verwendet werden. AWS Proton Für Produktionsbereitstellungen empfehlen wir, die Berechtigungen auf die spezifischen Ressourcen zu beschränken, die bereitgestellt werden, indem Sie benutzerdefinierte Richtlinien sowohl für die AWS Proton Pipeline-Dienstrollen als auch für die AWS Proton Umgebungsdienstrollen erstellen. Sie können diese Rollen mithilfe von AWS CLI oder IAM erstellen und anpassen. Weitere Informationen erhalten Sie unter Servicerollen für AWS Proton und Einen Service erstellen.

Einrichten mit AWS Proton

Wenn Sie die AWS CLI zum Ausführen von AWS Proton APIs verwenden möchten, stellen Sie sicher, dass Sie sie installiert haben. Wenn Sie es nicht installiert haben, finden Sie weitere Informationen unterEinrichten von AWS CLI.

AWS Protonspezifische Konfiguration:

- Um Vorlagen zu erstellen und zu verwalten:
  - Wenn Sie Konfigurationen für die Vorlagensynchronisierung verwenden, richten Sie eine AWS CodeStarVerbindung ein.
  - Andernfalls richten Sie einen Amazon S3 S3-Bucket ein.
- So stellen Sie die Infrastruktur bereit:
  - Für die selbstverwaltete Bereitstellung müssen Sie eine AWS CodeStar Verbindung einrichten.
- (Optional) So stellen Sie Pipelines bereit:
  - Richten Sie für AWS-managed Provisioning und CodeBuildbased Provisioning Pipeline-Rollen ein.
  - Richten Sie für die selbstverwaltete Bereitstellung ein Pipeline-Repository ein.

Weitere Informationen zu Bereitstellungsmethoden finden Sie unter. the section called “AWS-verwaltete Bereitstellung”

Einen Amazon S3 S3-Bucket einrichten

Um einen S3-Bucket einzurichten, folgen Sie den Anweisungen unter Erstellen Sie Ihren ersten S3-Bucket, um einen S3-Bucket einzurichten. Platzieren Sie Ihre Eingaben AWS Proton in dem Bucket, wo AWS Proton Sie sie abrufen können. Diese Eingaben werden als Template-Bundles bezeichnet. Sie können in anderen Abschnitten dieses Handbuchs mehr über sie erfahren.

Eine AWS CodeStar Verbindung einrichten

Um eine Verbindung AWS Proton zu einem Repository herzustellen, erstellen Sie eine AWS CodeStar Verbindung, die eine Pipeline aktiviert, wenn ein neuer Commit in einem Quellcode-Repository eines Drittanbieters vorgenommen wird.

AWS Protonverwendet die Verbindung für:

- Aktiviert eine Service-Pipeline, wenn ein neuer Commit für den Quellcode Ihres Repositorys vorgenommen wird.
- Stellen Sie eine Pull-Anfrage für ein Infrastruktur-as-Code-Repository.
- Erstellen Sie immer dann eine neue Neben- oder Hauptversion einer Vorlage, wenn ein Commit in ein Template-Repository übertragen wird, das eine Ihrer Vorlagen ändert, sofern die Version noch nicht existiert.

Du kannst dich mit Bitbucket- GitHub, GitHub Enterprise- und GitHub Enterprise Server-Repositorys verbinden. CodeConnections Weitere Informationen finden Sie unter CodeConnections im AWS CodePipeline-Benutzerhandbuch.

Um eine CodeStar Verbindung einzurichten.

1. Öffnen Sie die AWS Proton-Konsole.
2. Wählen Sie im Navigationsbereich Einstellungen und dann Repository-Verbindungen aus, um zur Seite Verbindungen in den Einstellungen der Developer Tools zu gelangen. Auf der Seite wird eine Liste von Verbindungen angezeigt.
3. Wählen Sie Verbindung erstellen und folgen Sie den Anweisungen.

Einrichtung der CI/CD-Pipeline-Einstellungen für das Konto

AWS Protonkann CI/CD-Pipelines für die Bereitstellung von Anwendungscode in Ihren Serviceinstanzen bereitstellen. Die AWS Proton Einstellungen, die Sie für die Pipeline-Bereitstellung benötigen, hängen von der Bereitstellungsmethode ab, die Sie für Ihre Pipeline wählen.

AWS-verwaltete und CodeBuild basierte Bereitstellung — Richten Sie Pipeline-Rollen ein

Mit AWS-managed Provisioning und CodeBuild Provisioning werden Pipelines für Sie bereitgestellt. AWS Proton Benötigt daher eine AWS Proton Servicerolle, die Berechtigungen für die Bereitstellung von Pipelines bereitstellt. Jede dieser beiden Bereitstellungsmethoden verwendet ihre eigene Servicerolle. Diese Rollen werden von allen AWS Proton Service-Pipelines gemeinsam genutzt und Sie konfigurieren sie einmal in Ihren Kontoeinstellungen.

So erstellen Sie Pipeline-Servicerollen mithilfe der Konsole

1. Öffnen Sie die AWS Proton-Konsole.
2. Wählen Sie im Navigationsbereich Einstellungen und dann Kontoeinstellungen aus.
3. Wählen Sie auf der Seite mit den CI/CD-Einstellungen für das Konto die Option Konfigurieren aus.
4. Führen Sie eine der folgenden Aktionen aus:
   - Um eine Pipeline-Servicerolle für AWS Proton Sie erstellen zu lassen

     [Um die AWS -verwaltete Bereitstellung von Pipelines zu aktivieren] Gehen Sie auf der Seite Kontoeinstellungen konfigurieren im Abschnitt AWS-managed provisioning Pipeline-Rolle wie folgt vor:

     a. Wählen Sie Neue Servicerolle aus.
     b. Geben Sie einen Namen für die Rolle ein, zum Beispiel**`myProtonPipelineServiceRole`**.
     c. Aktivieren Sie das Kontrollkästchen, um der Erstellung einer AWS Proton Rolle mit Administratorrechten in Ihrem Konto zuzustimmen.

     [Um die CodeBuild basierte Bereitstellung von Pipelines zu aktivieren] Wählen Sie auf der Seite Kontoeinstellungen konfigurieren im Abschnitt CodeBuildPipeline-Rolle die Option Bestehende Servicerolle und wählen Sie die Servicerolle aus, die Sie im Abschnitt CloudFormation Pipeline-Rolle erstellt haben. Oder, wenn Sie keine CloudFormation Pipeline-Rolle zugewiesen haben, wiederholen Sie die vorherigen drei Schritte, um eine neue Servicerolle zu erstellen.
   - Um bestehende Pipeline-Dienstrollen auszuwählen

     [Um die AWS verwaltete Bereitstellung von Pipelines zu aktivieren] Wählen Sie auf der Seite Kontoeinstellungen konfigurieren im Abschnitt AWS-managed provisioning pipeline role die Option Existierende Servicerolle und wählen Sie eine Servicerolle in Ihrem Konto aus. AWS

     [Um die CodeBuild Bereitstellung von Pipelines zu aktivieren] Wählen Sie auf der Seite Kontoeinstellungen konfigurieren im Abschnitt CodeBuildPipeline-Bereitstellungsrolle die Option Bestehende Servicerolle und wählen Sie eine Servicerolle in Ihrem Konto aus. AWS
5. Wählen Sie Änderungen speichern aus.

   Ihre neue Pipeline-Servicerolle wird auf der Seite mit den Kontoeinstellungen angezeigt.

Selbstverwaltete Bereitstellung — Richten Sie ein Pipeline-Repository ein

AWS ProtonSendet bei der selbstverwalteten Bereitstellung eine Pull-Anfrage (PR) an ein von Ihnen eingerichtetes Provisioning-Repository, und Ihr Automatisierungscode ist für die Bereitstellung von Pipelines verantwortlich. Für die Bereitstellung von Pipelines ist daher AWS Proton keine Servicerolle erforderlich. Stattdessen benötigt es ein registriertes Provisioning-Repository. Ihr Automatisierungscode im Repository muss eine entsprechende Rolle übernehmen, die Berechtigungen für die Bereitstellung von Pipelines bereitstellt.

Um ein Pipeline-Provisioning-Repository mit der Konsole zu registrieren

1. Erstellen Sie ein CI/CD-Pipeline-Provisioning-Repository, falls Sie noch keines erstellt haben. Weitere Informationen zu Pipelines bei der selbstverwalteten Bereitstellung finden Sie unter. the section called “Selbstverwaltetes Provisioned”
2. Wählen Sie im Navigationsbereich Einstellungen und dann Kontoeinstellungen aus.
3. Wählen Sie auf der Seite mit den CI/CD-Einstellungen für das Konto die Option Konfigurieren aus.
4. Gehen Sie auf der Seite Kontoeinstellungen konfigurieren im Abschnitt CI/CD-Pipeline-Repository wie folgt vor:

   a. Wählen Sie Neues Repository und dann einen der Repository-Anbieter aus.

   b. Wählen Sie für die CodeStar Verbindung eine Ihrer Verbindungen aus.

   > **Note**
   >
   > Wenn Sie noch keine Verbindung zum entsprechenden Repository-Provider-Konto haben, wählen Sie Neue CodeStar Verbindung hinzufügen, schließen Sie den Verbindungsaufbau ab und klicken Sie dann auf die Schaltfläche „Aktualisieren“ neben dem CodeStarVerbindungsmenü. Sie sollten jetzt in der Lage sein, Ihre neue Verbindung im Menü auszuwählen.

   c. Wählen Sie als Repository-Name Ihr Pipeline-Provisioning-Repository aus. Das Drop-down-Menü zeigt die Liste der Repositorys im Anbieterkonto.

   d. Wählen Sie als Branch-Name einen der Repository-Branches aus.
5. Wählen Sie Änderungen speichern aus.

   Ihr Pipeline-Repository wird auf der Seite mit den Kontoeinstellungen angezeigt.

Einrichten von AWS CLI

Um die AWS CLI für AWS Proton API-Aufrufe zu verwenden, stellen Sie sicher, dass Sie die neueste Version von installiert habenAWS CLI. Weitere Informationen finden Sie unter Erste Schritte mit dem AWS CLI im AWS Command Line Interface-Benutzerhandbuch. Weitere Informationen zu den ersten Schritten AWS CLI mit AWS Proton finden Sie unterthe section called “Erste Schritte mit der CLI”.

Erste Schritte mit AWS Proton

Bevor Sie beginnen, sollten Sie sich für die Nutzung einrichtenAWS Proton und überprüfen, ob Sie die Voraussetzungen für die ersten Schritte erfüllt haben.

Wählen Sie AWS Proton zunächst einen oder mehrere der folgenden Pfade aus:

- Folgen Sie einem angeleiteten Beispielkonsolen- oder CLI-Workflow über Dokumentationslinks.
- Führen Sie einen angeleiteten Beispiel-Konsolen-Workflow durch.
- Führen Sie einen AWS CLIBeispiel-Workflow mit Anleitung durch.

Themen

Voraussetzungen

Bevor Sie mit der Verwendung beginnenAWS Proton, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind. Weitere Informationen finden Sie unter Einrichtung.

- Sie haben ein IAM-Konto mit Administratorrechten. Weitere Informationen finden Sie unter Einrichtung mit IAM.
- Sie haben die AWS Proton Service-Rolle und die AWS Proton Pipeline-Service-Rolle ist mit Ihrem Konto verknüpft. Weitere Informationen erhalten Sie unter AWS ProtonServicerollen einrichten und Servicerollen für AWS Proton.
- Sie haben eine AWS CodeStar Verbindung. Weitere Informationen finden Sie unter Eine AWS CodeStar Verbindung einrichten.
- Sie sind mit der Erstellung von AWS CloudFormation Vorlagen und der Jinja-Parametrisierung vertraut. Weitere Informationen finden Sie unter Was ist? AWS CloudFormation im AWS CloudFormation Benutzerhandbuch und auf der Jinja-Website.

- Sie verfügen über praktische Kenntnisse im Bereich AWS Infrastrukturdienste.
- Sie sind bei Ihrem angemeldetAWS-Konto.

Arbeitsablauf „Erste Schritte“

Erfahren Sie anhand der Beispielschritte und Links, wie Sie Vorlagenpakete erstellen, Vorlagen erstellen und registrieren und Umgebungen und Dienste erstellen.

Stellen Sie vor dem Start sicher, dass Sie eine AWS ProtonServicerolle erstellt haben.

Wenn Ihre Dienstvorlage eine AWS Proton Dienstpipeline enthält, stellen Sie sicher, dass Sie eine AWS CodeStarVerbindung und eine AWS ProtonPipeline-Servicerolle erstellt haben.

Weitere Informationen finden Sie unter Die AWS Proton Service-API-Referenz.

Beispiel: Workflow „Erste Schritte“

1. Eine allgemeine Übersicht der AWS Proton Eingaben und Ausgaben finden Sie im Funktionsweise von AWS Proton Diagramm unter.
2. Erstellen Sie ein Umgebungs- und ein Dienstvorlagenpaket.
    a. Identifizieren Sie die Eingabeparameter.
    b. Erstellen Sie eine Schemadatei.
    c. Erstellen Sie Infrastructure-as-Code-Dateien (IaC).
    d. Um Ihr Vorlagenpaket zusammenzufassen, erstellen Sie eine Manifestdatei und organisieren Sie Ihre IaC-Dateien, Manifestdateien und Schemadateien in Verzeichnissen.
    e. Machen Sie Ihr Vorlagenpaket zugänglich AWS Proton für.
3. Erstellen und registrieren Sie eine Umgebungsvorlagenversion mitAWS Proton.

    Wenn Sie die Konsole verwenden, um eine Vorlage zu erstellen und zu registrieren, wird automatisch eine Vorlagenversion erstellt.

    Wenn Sie die verwendenAWS CLI, um eine Vorlage zu erstellen und zu registrieren:

    a. Erstellen Sie eine Umgebungsvorlage.
    b. Erstellen Sie eine Version der Umgebungsvorlage.

Weitere Informationen finden Sie unter CreateEnvironmentTemplateund CreateEnvironmentTemplateVersionin der AWS ProtonAPI-Referenz.

4. Veröffentlichen Sie Ihre Umgebungsvorlage, um sie zur Verwendung verfügbar zu machen.

   Weitere Informationen finden Sie UpdateEnvironmentTemplateVersionin der AWS ProtonAPI-Referenz.

5. Um eine Umgebung zu erstellen, wählen Sie eine veröffentlichte Version der Umgebungsvorlage aus und geben Sie Werte für die erforderlichen Eingaben an.

   Weitere Informationen finden Sie CreateEnvironmentin der AWS ProtonAPI-Referenz.

6. Erstellen und registrieren Sie eine Service-Vorlagenversion mitAWS Proton.

   Wenn Sie die Konsole verwenden, um eine Vorlage zu erstellen und zu registrieren, wird automatisch eine Vorlagenversion erstellt.

   Wenn Sie die verwendenAWS CLI, um eine Vorlage zu erstellen und zu registrieren:

   a. Erstellen Sie eine Dienstvorlage.
   b. Erstellen Sie eine Version der Dienstvorlage.

   Weitere Informationen finden Sie unter CreateServiceTemplateund CreateServiceTemplateVersionin der AWS ProtonAPI-Referenz.

7. Veröffentlichen Sie Ihre Dienstvorlage, um sie für die Verwendung verfügbar zu machen.

   Weitere Informationen finden Sie UpdateServiceTemplateVersionin der AWS ProtonAPI-Referenz.

8. Um einen Service zu erstellen, wählen Sie eine veröffentlichte Service-Vorlagenversion aus und geben Sie Werte für die erforderlichen Eingaben an.

   Weitere Informationen finden Sie CreateServicein der AWS ProtonAPI-Referenz.

Erste Schritte mit AWS Management Console

Erste Schritte mit AWS Proton

- Erstellen Sie eine Umgebungsvorlage und zeigen Sie sie an.

- Erstellen, Anzeigen und Veröffentlichen einer Dienstvorlage, die die Umgebungsvorlage verwendet, die Sie gerade erstellt haben.
- Erstellen Sie eine Umgebung und einen Dienst (optional).
- Löschen Sie die Dienstvorlage, die Umgebungsvorlage, die Umgebung und den Dienst, falls sie erstellt wurden.

Schritt 1: Öffnen Sie die AWS Proton Konsole

- Öffnen Sie die AWS Proton-Konsole.

Schritt 2: Bereiten Sie sich auf die Verwendung der Beispielvorlagen vor

1. Erstellen Sie eine Codestar-Verbindung zu Github und benennen Sie die Verbindung. my-proton-connection
2. Navigieren Sie zu https://github.com/aws-samples/aws-proton-cloudformation-sample-templates
3. Erstelle einen Fork des Repositorys in deinem Github-Konto.

Schritt 3: Erstellen Sie eine Umgebungsvorlage

Wählen Sie im Navigationsbereich die Option Umgebungsvorlagen aus.

1. Wählen Sie auf der Seite Umgebungsvorlagen die Option Umgebungsvorlage erstellen aus.
2. Wählen Sie auf der Seite Umgebungsvorlage erstellen im Abschnitt Vorlagenoptionen die Option Vorlage für die Bereitstellung neuer Umgebungen erstellen aus.
3. Wählen Sie im Abschnitt Quelle des Vorlagenpakets die Option Ein Vorlagenpaket aus Git synchronisieren aus.
4. Wählen Sie im Abschnitt Repository für Vorlagendefinitionen die Option Ein verknüpftes Git-Repository auswählen aus.
5. Wählen Sie my-proton-connectionaus der Repository-Liste aus.
6. Wählen Sie main aus der Branch-Liste aus.
7. Im Abschnitt Details zur Proton-Umgebungsvorlage.
    a. Geben Sie den Vorlagennamen als **`fargate-env`** ein.
    b. Geben Sie den Anzeigenamen der Umgebungsvorlage als ein**`My Fargate Environment`**.

c. (Optional) Geben Sie eine Beschreibung für die Umgebungsvorlage ein.

8. (Optional) Wählen Sie im Abschnitt „Tags“ die Option Neues Tag hinzufügen aus und geben Sie einen Schlüssel und einen Wert ein, um ein vom Kunden verwaltetes Tag zu erstellen.
9. Wählen Sie „Umgebungsvorlage erstellen“.

   Sie befinden sich jetzt auf einer neuen Seite, auf der der Status und die Details für Ihre neue Umgebungsvorlage angezeigt werden. Zu diesen Details gehören eine Liste von AWS und vom Kunden verwaltete Tags. AWS Protongeneriert automatisch AWS verwaltete Tags für Sie, wenn Sie AWS Proton Ressourcen erstellen. Weitere Informationen finden Sie unter AWS ProtonRessourcen und Tagging.
10. Der Status einer neuen Umgebungsvorlage beginnt im Status Entwurf. Sie und andere Personen mit `proton:CreateEnvironment` entsprechenden Berechtigungen können sie anzeigen und darauf zugreifen. Folgen Sie dem nächsten Schritt, um die Vorlage für andere verfügbar zu machen.
11. Wählen Sie im Abschnitt Vorlagenversionen das Optionsfeld links neben der Nebenversion der Vorlage, die Sie gerade erstellt haben (1.0). Alternativ können Sie im Info-Banner die Option Veröffentlichen auswählen und den nächsten Schritt überspringen.
12. Wählen Sie im Abschnitt Vorlagenversionen die Option Veröffentlichen aus.
13. Der Status der Vorlage ändert sich in Veröffentlicht. Da es sich um die neueste Version der Vorlage handelt, handelt es sich um die empfohlene Version.
14. Wählen Sie im Navigationsbereich die Option Umgebungsvorlagen aus.

    Auf einer neuen Seite wird eine Liste Ihrer Umgebungsvorlagen zusammen mit Vorlagendetails angezeigt.

Schritt 4: Erstellen Sie eine Dienstvorlage

Erstellen Sie eine Dienstvorlage.

1. Wählen Sie im Navigationsbereich die Option Dienstvorlagen aus.
2. Wählen Sie auf der Seite mit den Dienstvorlagen die Option Dienstvorlage erstellen aus.
3. Wählen Sie auf der Seite Dienstvorlage erstellen im Abschnitt Quelle des Vorlagenpakets die Option Vorlagenpaket aus Git synchronisieren aus.
4. Wählen Sie im Abschnitt Vorlage die Option Ein verknüpftes Git-Repository auswählen aus.
5. Wählen Sie my-proton-connectionaus der Repository-Liste aus.

6. Wählen Sie main aus der Branch-Liste aus.
7. Im Abschnitt Details zur Proton-Servicevorlage.
   a. Geben Sie den Namen der Dienstvorlage als **`backend-fargate-svc`** ein.
   b. Geben Sie den Anzeigenamen der Dienstvorlage als ein**`My Fargate Service`**.
   c. (Optional) Geben Sie eine Beschreibung für die Dienstvorlage ein.
8. Im Abschnitt Kompatible Umgebungsvorlagen.
   - Aktivieren Sie das Kontrollkästchen links neben der Umgebungsvorlage My Fargate Environment, um die kompatible Umgebungsvorlage für die neue Dienstvorlage auszuwählen.
9. Behalten Sie für die Verschlüsselungseinstellungen die Standardeinstellungen bei.
10. Im Abschnitt Pipeline-Definition.
    - Lassen Sie die Schaltfläche Diese Vorlage enthält eine CI/CD-Pipeline ausgewählt.
11. Wählen Sie Dienstvorlage erstellen aus.

    Sie befinden sich jetzt auf einer neuen Seite, auf der der Status und die Details für Ihre neue Servicevorlage angezeigt werden, einschließlich einer Liste von AWS und vom Kunden verwalteten Tags.
12. Der Status einer neuen Servicevorlage beginnt im Status Entwurf. Nur Administratoren können sie anzeigen und darauf zugreifen. Gehen Sie wie folgt vor, um die Dienstvorlage Entwicklern zur Verfügung zu stellen.
13. Wählen Sie im Abschnitt Vorlagenversionen das Optionsfeld links neben der Nebenversion der Vorlage, die Sie gerade erstellt haben (1.0). Alternativ können Sie im Info-Banner die Option Veröffentlichen auswählen und den nächsten Schritt überspringen.
14. Wählen Sie im Abschnitt Vorlagenversionen die Option Veröffentlichen aus.
15. Der Status der Vorlage ändert sich in Veröffentlicht.

    Die erste Nebenversion Ihrer Service-Vorlage ist veröffentlicht und steht Entwicklern zur Verwendung zur Verfügung. Da es sich um die neueste Version der Vorlage handelt, handelt es sich um die empfohlene Version.
16. Wählen Sie im Navigationsbereich die Option Dienstvorlagen aus.

    Auf einer neuen Seite wird eine Liste Ihrer Dienstvorlagen und Details angezeigt.

Schritt 5: Erstellen Sie eine Umgebung

Wählen Sie im Navigationsbereich Environments (Umgebungen) aus.

1. Wählen Sie Create environment (Umgebung erstellen) aus.
2. Wählen Sie auf der Seite Umgebungsvorlage auswählen die Vorlage aus, die Sie gerade erstellt haben. Es heißt My Fargate Environment. Wählen Sie dann Configure.
3. Wählen Sie auf der Seite Umgebung konfigurieren im Abschnitt Provisioning die Option Bereitstellung durch AWS Proton aus.
4. Wählen Sie im Abschnitt Bereitstellungskonto die Option Dies AWS-Konto aus.
5. Geben Sie unter Umgebungseinstellungen den Namen der Umgebung als ein**`my-fargate-environment`**.
6. Wählen Sie im Abschnitt Umgebungsrollen die Option Neue Servicerolle oder, falls Sie bereits eine AWS Proton Servicerolle erstellt haben, die Option Bestehende Servicerolle aus.

   a. Wählen Sie Neue Servicerolle aus, um eine neue Rolle zu erstellen.

      i. Geben Sie den Namen der Umgebungsrolle als ein**`MyProtonServiceRole`**.

      ii. Aktivieren Sie das Kontrollkästchen, um der Erstellung einer AWS Proton Servicerolle mit Administratorrechten für Ihr Konto zuzustimmen.

   b. Wählen Sie Bestehende Servicerolle aus, um eine bestehende Rolle zu verwenden.

      - Wählen Sie Ihre Rolle im Dropdownfeld Name der Umgebungsrolle aus.
7. Wählen Sie Weiter aus.
8. Verwenden Sie auf der Seite Benutzerdefinierte Einstellungen konfigurieren die Standardeinstellungen.
9. Wählen Sie Weiter und überprüfen Sie Ihre Eingaben.
10. Wählen Sie Erstellen aus.

    Sehen Sie sich die Umgebungsdetails und den Status sowie die AWS verwalteten und vom Kunden verwalteten Tags für Ihre Umgebung an.
11. Wählen Sie im Navigationsbereich Environments (Umgebungen) aus.

    Auf einer neuen Seite wird eine Liste Ihrer Umgebungen zusammen mit dem Status und anderen Umgebungsdetails angezeigt.

Schritt 6: Optional — Erstellen Sie einen Dienst und stellen Sie eine Anwendung bereit

1. Öffnen Sie die AWS Proton-Konsole.
2. Wählen Sie im Navigationsbereich Dienste aus.
3. Wählen Sie auf der Seite Dienste die Option Dienst erstellen aus.
4. Wählen Sie auf der Seite Servicevorlage auswählen die Vorlage My Fargate Service aus, indem Sie auf das Optionsfeld in der oberen rechten Ecke der Vorlagenkarte klicken.
5. Wählen Sie in der unteren rechten Ecke der Seite die Option Konfigurieren aus.
6. Geben Sie auf der Seite Dienst konfigurieren im Abschnitt Diensteinstellungen den Dienstnamen ein**`my-service`**.
7. (Optional) Geben Sie eine Beschreibung für den Dienst ein.
8. Gehen Sie im Abschnitt Einstellungen für das Service-Repository wie folgt vor:
   a. Wählen Sie für die CodeStar Verbindung Ihre Verbindung aus der Liste aus.
   b. Wählen Sie unter Repository-Name den Namen Ihres Quellcode-Repositorys aus der Liste aus.
   c. Wählen Sie unter Branch-Name den Namen Ihres Quellcode-Repository-Branches aus der Liste aus.
9. (Optional) Wählen Sie im Abschnitt „Tags“ die Option Neues Tag hinzufügen aus und geben Sie einen Schlüssel und einen Wert ein, um ein vom Kunden verwaltetes Tag zu erstellen. Wählen Sie anschließend Next (Weiter).
10. Folgen Sie auf der Seite Benutzerdefinierte Einstellungen konfigurieren im Abschnitt Serviceinstanzen im Abschnitt Neue Instanz den nächsten Schritten, um benutzerdefinierte Werte für Ihre Service-Instance-Parameter anzugeben.
    a. Geben Sie den Instanznamen ein**`my-app-service`**.
    b. Wählen Sie die Umgebung **`my-fargate-environment`** für Ihre Dienstinstanz aus.
    c. Behalten Sie die Standardeinstellungen für die verbleibenden Instanzparameter bei.
    d. Behalten Sie die Standardeinstellungen für Pipeline-Eingaben bei.
    e. Wählen Sie Weiter und überprüfen Sie Ihre Eingaben.
    f. Wählen Sie Erstellen und sehen Sie sich Ihren Servicestatus und die Details an.

11. Auf der Seite mit den Servicedetails können Sie den Status Ihrer Serviceinstanz und Pipeline einsehen, indem Sie die Registerkarten Übersicht und Pipeline auswählen. Auf diesen Seiten können Sie auch Tags einsehen AWS und vom Kunden verwalten. AWS Protonerstellt automatisch AWS verwaltete Tags für Sie. Wählen Sie Tags verwalten, um vom Kunden verwaltete Tags zu erstellen und zu ändern. Weitere Informationen über das Markieren mit Tags finden Sie unter AWS ProtonRessourcen und Tagging.
12. Wenn der Service aktiv ist, wählen Sie auf der Registerkarte Overview im Abschnitt Service Instances den Namen Ihrer Dienstinstanz aus my-app-service.

    Sie befinden sich jetzt auf der Detailseite der Service-Instanz.
13. Um Ihre Anwendung anzuzeigen, kopieren Sie im Abschnitt Ausgaben den ServiceEndpointLink in Ihren Browser.

    Sie sehen eine AWS Proton Grafik auf der Webseite.
14. Nachdem der Dienst erstellt wurde, wählen Sie im Navigationsbereich Dienste aus, um eine Liste Ihrer Dienste anzuzeigen.

Schritt 7: Aufräumen.

1. Öffnen Sie die AWS Proton-Konsole.
2. Löschen Sie einen Dienst (falls Sie einen erstellt haben)
    a. Wählen Sie im Navigationsbereich Dienste aus.
    b. Wählen Sie auf der Seite Dienste den Dienstnamen my-service aus.

       Sie befinden sich jetzt auf der Seite mit den Servicedetails für my-service.
    c. Wählen Sie in der oberen rechten Ecke der Seite Aktionen und dann Löschen aus.
    d. In einem Modal werden Sie aufgefordert, die Löschaktion zu bestätigen.
    e. Folgen Sie den Anweisungen und wählen Sie Ja, löschen.
3. Lösche eine Umgebung
    a. Wählen Sie im Navigationsbereich Environments (Umgebungen) aus.
    b. Wählen Sie auf der Seite Umgebungen das Optionsfeld links neben der Umgebung aus, die Sie gerade erstellt haben.
    c. Wählen Sie „Aktionen“ und dann „Löschen“.

d. In einem Modal werden Sie aufgefordert, die Löschaktion zu bestätigen.

e. Folgen Sie den Anweisungen und wählen Sie Ja, löschen.

4. Löschen Sie eine Dienstvorlage

   a. Wählen Sie im Navigationsbereich die Option Dienstvorlagen aus.

   b. Wählen Sie auf der Seite mit den Dienstvorlagen das Optionsfeld links neben der Dienstvorlage aus my-svc-template.

   c. Wählen Sie „Aktionen“ und dann „Löschen“.

   d. In einem Modal werden Sie aufgefordert, die Löschaktion zu bestätigen.

   e. Folgen Sie den Anweisungen und wählen Sie Ja, löschen. Dadurch werden die Dienstvorlage und alle ihre Versionen gelöscht.

5. Löscht eine Umgebungsvorlage

   a. Wählen Sie im Navigationsbereich die Option Umgebungsvorlagen aus.

   b. Wählen Sie auf der Seite mit den Umgebungsvorlagen das Optionsfeld links neben aus my-env-template.

   c. Wählen Sie „Aktionen“ und dann „Löschen“.

   d. In einem Modal werden Sie aufgefordert, die Löschaktion zu bestätigen.

   e. Folgen Sie den Anweisungen und wählen Sie Ja, löschen. Dadurch werden die Umgebungsvorlage und alle ihre Versionen gelöscht.

6. Löschen Sie Ihre Codestar-Verbindung

Erste Schritte mit AWS CLI

Folgen Sie diesem TutorialAWS CLI, um mit der AWS Proton Verwendung von zu beginnen. Das Tutorial zeigt einen öffentlich zugänglichen AWS Proton Dienst mit Lastenausgleich auf der AWS Fargate Grundlage von. Das Tutorial bietet auch eine CI/CD-Pipeline, die eine statische Website mit einem angezeigten Bild bereitstellt.

Bevor Sie beginnen, stellen Sie sicher, dass Sie richtig eingerichtet sind. Details hierzu finden Sie unter the section called “Voraussetzungen”.

Schritt 1: Registrieren Sie eine Umgebungsvorlage

In diesem Schritt registrieren Sie als Administrator eine Beispielumgebungsvorlage, die einen Amazon Elastic Container Service (Amazon ECS) -Cluster und eine Amazon Virtual Private Cloud (Amazon VPC) mit zwei öffentlichen/privaten Subnetzen enthält.

Um eine Umgebungsvorlage zu registrieren

1. Ordnen Sie das AWS ProtonSample CloudFormation Templates-Repository Ihrem GitHub Konto oder Ihrer Organisation zu. Dieses Repository enthält die Umgebungs- und Dienstvorlagen, die wir in diesem Tutorial verwenden.

   Registrieren Sie dann Ihr geforktes Repository beiAWS Proton. Weitere Informationen finden Sie unter the section called “Erstellen eines Redie”.

2. Erstellen Sie eine Umgebungsvorlage.

   Die Umgebungsvorlagenressource verfolgt die Versionen der Umgebungsvorlagen.

   ```
   $ aws proton create-environment-template \
     --name "fargate-env" \
     --display-name "Public VPC Fargate" \
     --description "VPC with public access and ECS cluster"
   ```

3. Erstellen Sie eine Konfiguration für die Vorlagensynchronisierung.

   AWS Protonrichtet eine Synchronisierungsbeziehung zwischen Ihrem Repository und Ihrer Umgebungsvorlage ein. Anschließend wird die Vorlagenversion 1.0 im DRAFT Status erstellt.

   ```
   $ aws proton create-template-sync-config \
     --template-name "fargate-env" \
     --template-type "ENVIRONMENT" \
     --repository-name "your-forked-repo" \
     --repository-provider "GITHUB" \
     --branch "your-branch" \
     --subdirectory "environment-templates/fargate-env"
   ```

4. Warten Sie, bis die Version der Umgebungsvorlage erfolgreich registriert wurde.

   Wenn dieser Befehl mit dem Exit-Status von zurückkehrt0, ist die Versionsregistrierung abgeschlossen. Dies ist in Skripten nützlich, um sicherzustellen, dass Sie den Befehl im nächsten Schritt erfolgreich ausführen können.

```
$ aws proton wait environment-template-version-registered \
  --template-name "fargate-env" \
  --major-version "1" \
  --minor-version "0"
```

5. Veröffentlichen Sie die Version der Umgebungsvorlage, um sie für die Erstellung der Umgebung verfügbar zu machen.

```
$ aws proton update-environment-template-version \
  --template-name "fargate-env" \
  --major-version "1" \
  --minor-version "0" \
  --status "PUBLISHED"
```

Schritt 2: Registrieren Sie eine Dienstvorlage

In diesem Schritt registrieren Sie als Administrator eine Beispiel-Servicevorlage, die alle Ressourcen enthält, die für die Bereitstellung eines Amazon ECS Fargate-Dienstes hinter einem Load Balancer und einer CI/CD-Pipeline erforderlich sind, die verwendet. AWS CodePipeline

Um eine Service-Vorlage zu registrieren

1. Erstellen Sie eine Dienstvorlage.

   Die Dienstvorlagenressource verfolgt die Versionen der Dienstvorlagen.

```
$ aws proton create-service-template \
  --name "load-balanced-fargate-svc" \
  --display-name "Load balanced Fargate service" \
  --description "Fargate service with an application load balancer"
```

2. Erstellen Sie eine Konfiguration für die Vorlagensynchronisierung.

   AWS Protonrichtet eine Synchronisierungsbeziehung zwischen Ihrem Repository und Ihrer Service-Vorlage ein. Anschließend wird die Vorlagenversion 1.0 im `DRAFT` Status erstellt.

```
$ aws proton create-template-sync-config \
  --template-name "load-balanced-fargate-svc" \
  --template-type "SERVICE" \
  --repository-name "your-forked-repo" \
```

```
  --repository-provider "GITHUB" \
  --branch "your-branch" \
  --subdirectory "service-templates/load-balanced-fargate-svc"
```

3. Warten Sie, bis die Version der Dienstvorlage erfolgreich registriert wurde.

   Wenn dieser Befehl mit dem Exit-Status von zurückkehrt`0`, ist die Versionsregistrierung abgeschlossen. Dies ist in Skripten nützlich, um sicherzustellen, dass Sie den Befehl im nächsten Schritt erfolgreich ausführen können.

   ```
   $ aws proton wait service-template-version-registered \
     --template-name "load-balanced-fargate-svc" \
     --major-version "1" \
     --minor-version "0"
   ```

4. Veröffentlichen Sie die Version der Dienstvorlage, um sie für die Diensterstellung verfügbar zu machen.

   ```
   $ aws proton update-service-template-version \
     --template-name "load-balanced-fargate-svc" \
     --major-version "1" \
     --minor-version "0" \
     --status "PUBLISHED"
   ```

Schritt 3: Stellen Sie eine Umgebung bereit

In diesem Schritt instanziieren Sie als Administrator eine AWS Proton Umgebung anhand der Umgebungsvorlage.

Um eine Umgebung bereitzustellen

1. Holen Sie sich eine Beispielspezifikationsdatei für die Umgebungsvorlage, die Sie registriert haben.

   Sie können die Datei `environment-templates/fargate-env/spec/spec.yaml` aus dem Vorlagen-Beispiel-Repository herunterladen. Alternativ können Sie das gesamte Repository lokal abrufen und den create-environment Befehl aus dem `environment-templates/fargate-env` Verzeichnis ausführen.

2. Erstellen Sie eine Umgebung.

AWS Protonliest Eingabewerte aus Ihrer Umgebungsspezifikation, kombiniert sie mit Ihrer Umgebungsvorlage und stellt mithilfe Ihrer AWS Proton Servicerolle Umgebungsressourcen in Ihrem AWS Konto bereit.

```
$ aws proton create-environment \
  --name "fargate-env-prod" \
  --template-name "fargate-env" \
  --template-major-version 1 \
  --proton-service-role-arn "arn:aws:iam::123456789012:role/AWSProtonServiceRole" \
  --spec "file://spec/spec.yaml"
```

3. Warten Sie, bis die Umgebung erfolgreich bereitgestellt wurde.

```
$ aws proton wait environment-deployed --name "fargate-env-prod"
```

Schritt 4: Bereitstellen eines Dienstes [Anwendungsentwickler]

In den vorherigen Schritten hat ein Administrator eine Dienstvorlage registriert und veröffentlicht und eine Umgebung bereitgestellt. Als Anwendungsentwickler können Sie jetzt einen AWS Proton Dienst erstellen und ihn in der AWS Proton Umgebung bereitstellen

Um einen Dienst bereitzustellen

1. Rufen Sie eine Beispielspezifikationsdatei für die Dienstvorlage ab, die der Administrator registriert hat.

   Sie können die Datei `service-templates/load-balanced-fargate-svc/spec/spec.yaml` aus dem Vorlagen-Beispiel-Repository herunterladen. Alternativ können Sie das gesamte Repository lokal abrufen und den create-service Befehl aus dem `service-templates/load-balanced-fargate-svc` Verzeichnis ausführen.
2. Teilen Sie das AWS ProtonSample Services-Repository Ihrem GitHub Konto oder Ihrer Organisation zu. Dieses Repository enthält den Quellcode der Anwendung, den wir in diesem Tutorial verwenden.
3. Erstellen Sie einen Service.

   AWS Protonliest Eingabewerte aus Ihrer Servicespezifikation, kombiniert sie mit Ihrer Dienstvorlage und stellt Serviceressourcen in Ihrem AWS Konto in der Umgebung bereit, die in

der Spezifikation angegeben ist. Eine AWS CodePipeline Pipeline stellt Ihren Anwendungscode aus dem Repository bereit, das Sie im Befehl angeben.

```
$ aws proton create-service \
  --name "static-website" \
  --repository-connection-arn \
    "arn:aws:codestar-connections:us-east-1:123456789012:connection/your-codestar-connection-id" \
  --repository-id "your-GitHub-account/aws-proton-sample-services" \
  --branch-name "main" \
  --template-major-version 1 \
  --template-name "load-balanced-fargate-svc" \
  --spec "file://spec/spec.yaml"
```

4. Warten Sie, bis der Dienst erfolgreich bereitgestellt wurde.

```
$ aws proton wait service-created --name "static-website"
```

5. Rufen Sie die Ausgaben ab und sehen Sie sich Ihre neue Website an.

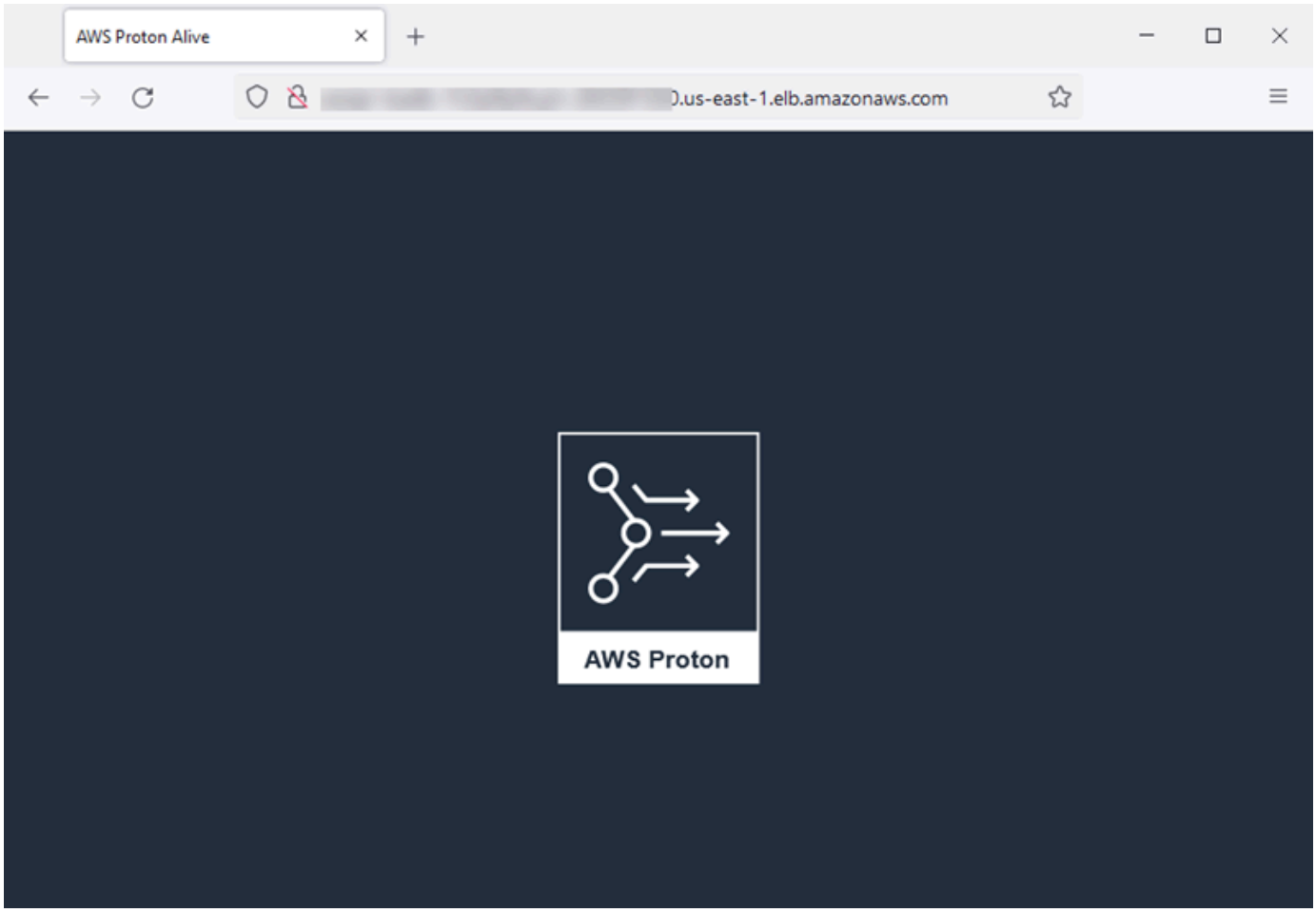
   Führen Sie den Befehl aus:

```
$ aws proton list-service-instance-outputs \
  --service-name "static-website" \
  --service-instance-name load-balanced-fargate-svc-prod
```

   Die Ausgabe des Befehls sollte der folgenden ähneln:

```
{
    "outputs": [
        {
            "key": "ServiceURL",
            "valueString": "http://your-service-endpoint.us-east-1.elb.amazonaws.com"
        }
    ]
}
```

   Der Wert der `ServiceURL` Instanzausgabe ist der Endpunkt Ihrer neuen Service-Website. Verwenden Sie Ihren Browser, um dorthin zu navigieren. Sie sollten die folgende Grafik auf einer statischen Seite sehen:



Schritt 5: Aufräumen (optional)

In diesem Schritt löschen Sie die AWS Ressourcen, die Sie im Rahmen dieses Tutorials erstellt haben, und um die mit diesen Ressourcen verbundenen Kosten zu sparen.

Um Tutorial-Ressourcen zu löschen

1. Führen Sie den folgenden Befehl aus, um den Dienst zu löschen:

```
$ aws proton delete-service --name "static-website"
```

2. Führen Sie den folgenden Befehl aus, um die Umgebung zu löschen:

```
$ aws proton delete-environment --name "fargate-env-prod"
```

3. Führen Sie die folgenden Befehle aus, um die Dienstvorlage zu löschen:

```
$ aws proton delete-template-sync-config \
  --template-name "load-balanced-fargate-svc" \
  --template-type "SERVICE"
$ aws proton delete-service-template --name "load-balanced-fargate-svc"
```

4. Führen Sie die folgenden Befehle aus, um die Umgebungsvorlage zu löschen:

```
$ aws proton delete-template-sync-config \
  --template-name "fargate-env" \
  --template-type "ENVIRONMENT"
$ aws proton delete-environment-template --name "fargate-env"
```

Die AWS Proton Vorlagenbibliothek

Das AWS Proton Team unterhält eine Bibliothek mit Vorlagenbeispielen auf GitHub. Die Bibliothek enthält Beispiele für Infrastructure-as-Code-Dateien (IaC) für viele gängige Umgebungs- und Anwendungsinfrastrukturszenarien.

Die Vorlagenbibliothek ist in zwei GitHub Repositorys gespeichert:

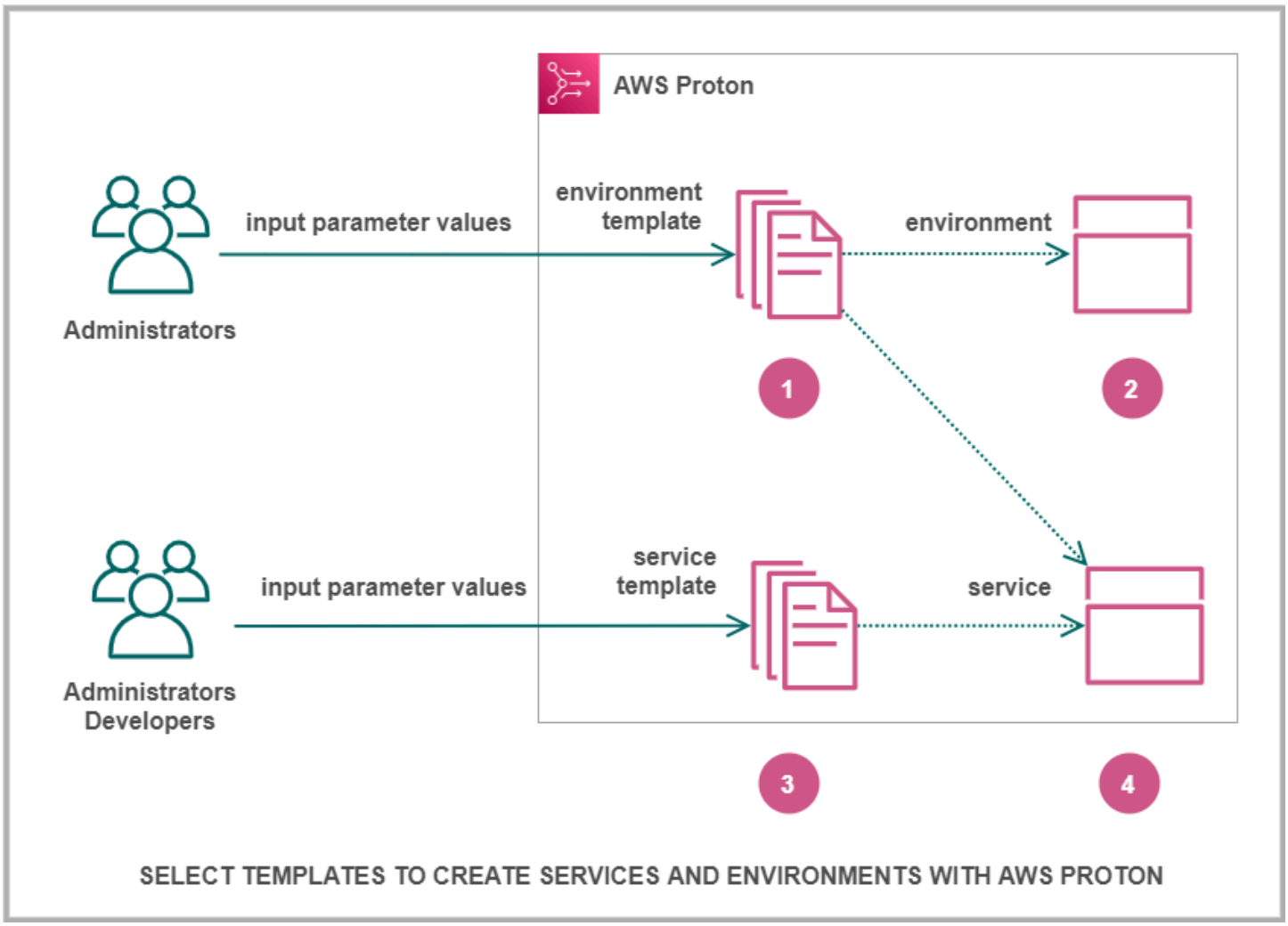
- aws-proton-cloudformation-sample-templates — Beispiele für Template-Bundles, die Jinja als AWS CloudFormationIaC-Sprache verwenden. Sie können diese Beispiele für Umgebungen verwenden. AWS-verwaltete Bereitstellung
- aws-proton-terraform-sample-templates — Beispiele für Vorlagenpakete, die Terraform als IaC-Sprache verwenden. Sie können diese Beispiele für Umgebungen verwenden. Selbstverwaltetes Provisioned

Jedes dieser Repositorien enthält eine `README` Datei mit vollständigen Informationen über den Inhalt und die Struktur des Repositorys. Jedes Beispiel enthält Informationen über den Anwendungsfall, den die Vorlage abdeckt, die Architektur des Beispiels und die Eingabeparameter, die die Vorlage verwendet.

Sie können die Vorlagen in dieser Bibliothek direkt verwenden, indem Sie eines der Repositorys der Bibliothek mit Ihrem GitHub Konto verknüpfen. Alternativ können Sie diese Beispiele als Ausgangspunkt für die Entwicklung Ihrer Umgebungs- und Dienstvorlagen verwenden.

Funktionsweise von AWS Proton

Mit AWS Proton stellen Sie Umgebungen und dann Dienste bereit, die in diesen Umgebungen ausgeführt werden. Umgebungen und Dienste basieren auf Umgebungs- bzw. Dienstvorlagen, die Sie in Ihrer AWS Proton versionierten Vorlagenbibliothek auswählen.



1 Wenn Sie als Administrator eine Umgebungsvorlage mit auswählenAWS Proton, geben Sie Werte für die erforderlichen Eingabeparameter an.

2 AWS Protonverwendet die Umgebungsvorlage und die Parameterwerte, um Ihre Umgebung bereitzustellen.

3 Wenn Sie als Entwickler oder Administrator eine Dienstvorlage mit auswählenAWS Proton, geben Sie Werte für die erforderlichen Eingabeparameter an. Sie wählen auch eine Umgebung aus, in der Sie Ihre Anwendung oder Ihren Dienst bereitstellen möchten.

4 AWS Protonverwendet die Dienstvorlage und sowohl Ihren Service als auch die ausgewählten Umgebungsparameterwerte, um Ihren Service bereitzustellen.

Sie geben Werte für die Eingabeparameter an, um Ihre Vorlage für die Wiederverwendung und für mehrere Anwendungsfälle, Anwendungen oder Dienste anzupassen.

Damit dies funktioniert, erstellen Sie Umgebungs- oder Dienstvorlagenpakete und laden sie in registrierte Umgebungs- bzw. Dienstvorlagen hoch.

Vorlagenpakete enthalten alles, was Sie für die Bereitstellung von Umgebungen oder Diensten AWS Proton benötigen.

Wenn Sie eine Umgebungs- oder Dienstvorlage erstellen, laden Sie ein Vorlagenpaket hoch, das die parametrisierte Infrastruktur als Codedateien (IaC) enthält, die zur Bereitstellung von Umgebungen oder Diensten AWS Proton verwendet werden.

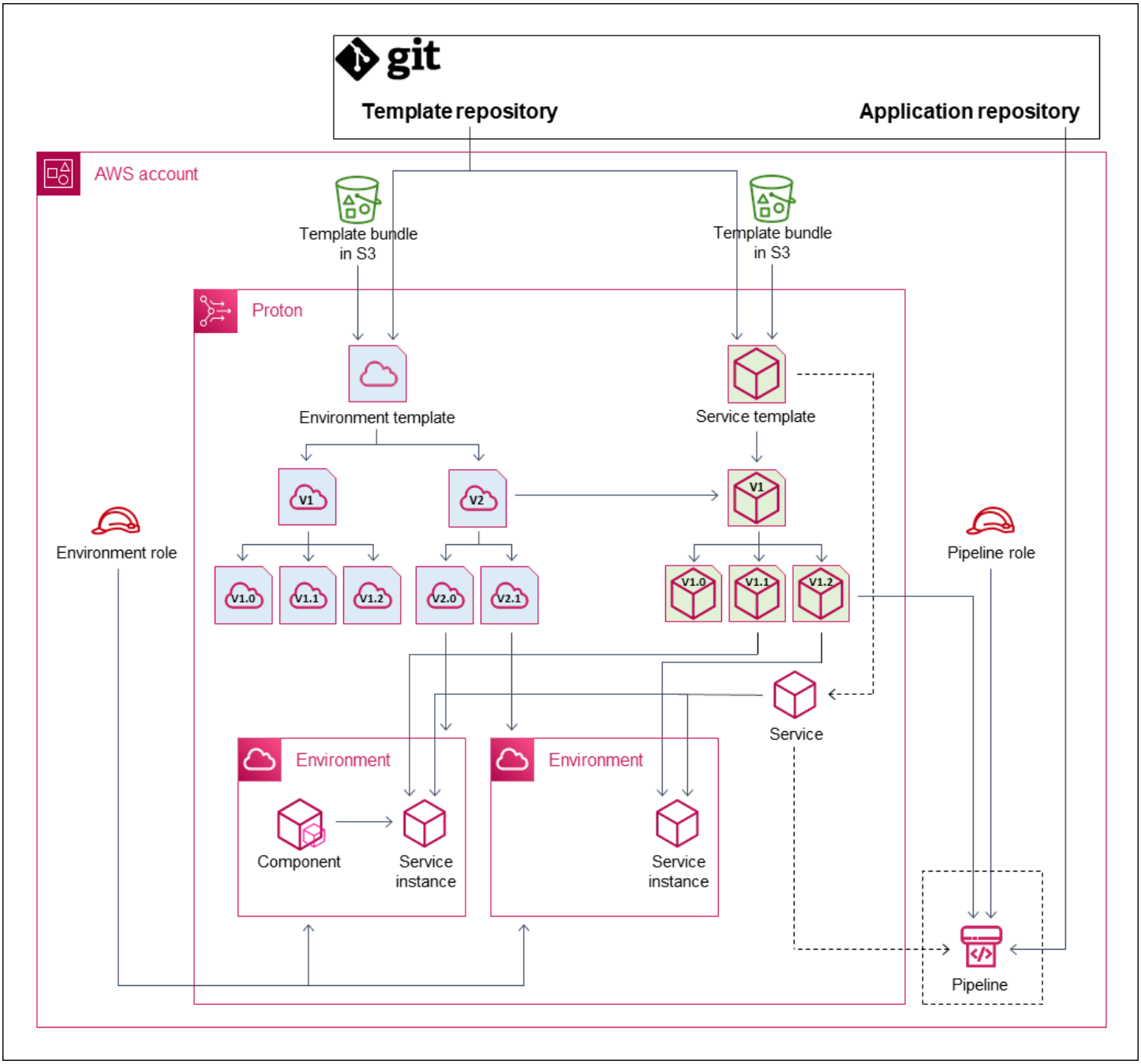
Wenn Sie eine Umgebungs- oder Dienstvorlage auswählen, um eine Umgebung oder einen Dienst zu erstellen oder zu aktualisieren, geben Sie Werte für die IaC-Dateiparameter des Vorlagenpakets an.

Themen

AWS Protonobjekte

Das folgende Diagramm zeigt die AWS Proton Hauptobjekte und ihre Beziehung zu anderen Objekten AWS und Objekten von Drittanbietern. Die Pfeile stellen die Richtung des Datenflusses dar (die umgekehrte Richtung der Abhängigkeit).

Wir folgen dem Diagramm mit kurzen Beschreibungen und Referenzlinks für diese AWS Proton Objekte.



- Umgebungsvorlage — Eine Sammlung von Umgebungsvorlagenversionen, die zum Erstellen von AWS Proton Umgebungen verwendet werden können.

  Weitere Informationen erhalten Sie unter Vorlagenerstellung und Pakete und Vorlagen.
- Version der Umgebungsvorlage — Eine bestimmte Version einer Umgebungsvorlage. Nimmt ein Vorlagenpaket als Eingabe, entweder aus einem S3-Bucket oder aus einem Git-Repository. Das Paket spezifiziert Infrastructure as Code (IaC) und zugehörige Eingabeparameter für eine AWS Proton Umgebung.

Weitere Informationen finden Sie unter the section called “Versionen”, the section called “Veröffentlichen” und the section called “Konfigurationen für die Vorlagensynchronisierung”.

- Umgebung — Der Satz gemeinsam genutzter AWS Infrastrukturressourcen und Zugriffsrichtlinien, in denen AWS Proton Dienste bereitgestellt werden. AWSRessourcen werden mithilfe einer Umgebungsvorlagenversion bereitgestellt, die mit bestimmten Parameterwerten aufgerufen wird. Zugriffsrichtlinien werden in einer Servicerolle bereitgestellt.

  Weitere Informationen finden Sie unter Umgebungen.

- Dienstvorlage — Eine Sammlung von Dienstvorlagenversionen, die zum Erstellen von AWS Proton Diensten verwendet werden können.

  Weitere Informationen erhalten Sie unter Vorlagenerstellung und Pakete und Vorlagen.

- Version der Dienstvorlage — Eine bestimmte Version einer Dienstvorlage. Nimmt ein Vorlagenpaket als Eingabe, entweder aus einem S3-Bucket oder aus einem Git-Repository. Das Paket spezifiziert Infrastructure as Code (IaC) und zugehörige Eingabeparameter für einen AWS Proton Dienst.

  Eine Version der Dienstvorlage spezifiziert außerdem diese Einschränkungen für Dienstinstanzen, die auf der Version basieren:

  - Kompatible Umgebungsvorlagen — Instances können nur in Umgebungen ausgeführt werden, die auf diesen kompatiblen Umgebungsvorlagen basieren.
  - Unterstützte Komponentenquellen — Die Komponententypen, die Entwickler Instanzen zuordnen können.

  Weitere Informationen finden Sie unter the section called “Versionen”, the section called “Veröffentlichen” und the section called “Konfigurationen für die Vorlagensynchronisierung”.

- Service — Eine Sammlung von Dienstinstanzen, die eine Anwendung mithilfe der in einer Dienstvorlage angegebenen Ressourcen ausführen, und optional eine CI/CD-Pipeline, die den Anwendungscode in diesen Instanzen bereitstellt.

  Im Diagramm bedeutet die gestrichelte Linie von der Dienstvorlage, dass der Service die Vorlage an die Dienstinstanzen und die Pipeline weiterleitet.

  Weitere Informationen finden Sie unter Dienstleistungen.

- Dienstinstanz — Die Gruppe von AWS Infrastrukturressourcen, die eine Anwendung in einer bestimmten AWS Proton Umgebung ausführen. AWSRessourcen werden mithilfe einer Dienstvorlagenversion bereitgestellt, die mit bestimmten Parameterwerten aufgerufen wird.

  Weitere Informationen erhalten Sie unter Dienstleistungen und the section called “Aktualisierung der Instance”.
- Pipeline — Eine optionale CI/CD-Pipeline, die eine Anwendung in den Instanzen eines Dienstes bereitstellt, mit Zugriffsrichtlinien zur Bereitstellung dieser Pipeline. Zugriffsrichtlinien werden in einer Servicerolle bereitgestellt. Ein Service hat nicht immer eine zugehörige AWS Proton Pipeline. Sie können sich dafür entscheiden, Ihre App-Code-Bereitstellungen außerhalb von zu verwalten. AWS Proton

  In der Abbildung bedeuten die gestrichelte Linie von Service und das gestrichelte Feld rund um die Pipeline, dass, wenn Sie sich dafür entscheiden, Ihre CI/CD-Bereitstellungen selbst zu verwalten, die AWS Proton Pipeline möglicherweise nicht erstellt wird und Ihre eigene Pipeline möglicherweise nicht in Ihrem Konto vorhanden ist. AWS

  Weitere Informationen erhalten Sie unter Dienstleistungen und the section called “Aktualisierung der Pipeline”.
- Komponente — Eine vom Entwickler definierte Erweiterung einer Serviceinstanz. Gibt zusätzliche AWS Infrastrukturressourcen an, die eine bestimmte Anwendung zusätzlich zu den von der Umgebung und der Dienstinstanz bereitgestellten Ressourcen benötigt. Plattformteams kontrollieren die Infrastruktur, die eine Komponente bereitstellen kann, indem sie der Umgebung eine Komponentenrolle zuweisen.

  Weitere Informationen finden Sie unter Komponenten.

Wie stellt AWS Proton die Infrastruktur bereit

AWS Protonkann die Infrastruktur auf eine von mehreren Arten bereitstellen:

- AWS-managed Provisioning — AWS Proton ruft die Provisioning Engine in Ihrem Namen auf. Diese Methode unterstützt nur AWS CloudFormation Vorlagenpakete. Weitere Informationen finden Sie unter the section called “AWS CloudFormation IaC-Dateien”.
- CodeBuildBereitstellung — AWS Proton wird verwendetAWS CodeBuild, um Shell-Befehle auszuführen, die Sie bereitstellen. Ihre Befehle können Eingaben lesen, die die Infrastruktur AWS Proton bereitstellen, und sind dafür verantwortlich, die Infrastruktur bereitzustellen oder

sie aufzuheben und Ausgabewerte zu generieren. Ein Vorlagenpaket für diese Methode enthält Ihre Befehle in einer Manifestdatei und alle Programme, Skripts oder anderen Dateien, die diese Befehle möglicherweise benötigen.

Als Beispiel für die Verwendung von CodeBuild Provisioning können Sie Code hinzufügen, der die AWS Ressourcen AWS Cloud Development Kit (AWS CDK) zur Bereitstellung verwendet, und ein Manifest, das das CDK installiert und Ihren CDK-Code ausführt.

Weitere Informationen finden Sie unter the section called “CodeBuild -Paket”.

> **Note**
>
> Sie können die CodeBuild Bereitstellung mit Umgebungen und Diensten verwenden. Derzeit können Sie auf diese Weise keine Komponenten bereitstellen.

- Selbstverwaltete Bereitstellung — sendet eine AWS Proton Pull-Anfrage (PR) an ein von Ihnen bereitgestelltes Repository, in dem Ihr eigenes Infrastrukturbereitstellungssystem den Bereitstellungsprozess durchführt. Diese Methode unterstützt nur Terraform-Vorlagenpakete. Weitere Informationen finden Sie unter the section called “Terraform-IaC-Dateien”.

AWS Protonbestimmt und legt die Bereitstellungsmethode für jede Umgebung und jeden Dienst separat fest. Wenn Sie eine Umgebung oder einen Dienst erstellen oder aktualisieren, AWS Proton untersucht er das von Ihnen bereitgestellte Vorlagenpaket und bestimmt die im Vorlagenpaket angegebene Bereitstellungsmethode. Auf Umgebungsebene geben Sie die Parameter an, die die Umgebung und ihre potenziellen Dienste möglicherweise für ihre Bereitstellungsmethoden benötigen — AWS Identity and Access Management (IAM) -Rollen, eine Verbindung mit einem Umgebungskonto oder ein Infrastruktur-Repository.

Entwickler, die einen Dienst bereitstellen, haben unabhängig von der Bereitstellungsmethode die gleiche Erfahrung. AWS Proton Entwickler müssen sich der Bereitstellungsmethode nicht bewusst sein und müssen nichts am Servicebereitstellungsprozess ändern. Die Dienstvorlage legt die Bereitstellungsmethode fest, und jede Umgebung, in der ein Entwickler den Service bereitstellt, stellt die erforderlichen Parameter für die Bereitstellung von Serviceinstanzen bereit.

Das folgende Diagramm fasst einige Hauptmerkmale der verschiedenen Bereitstellungsmethoden zusammen. Die Abschnitte, die der Tabelle folgen, enthalten Einzelheiten zu den einzelnen Methoden.

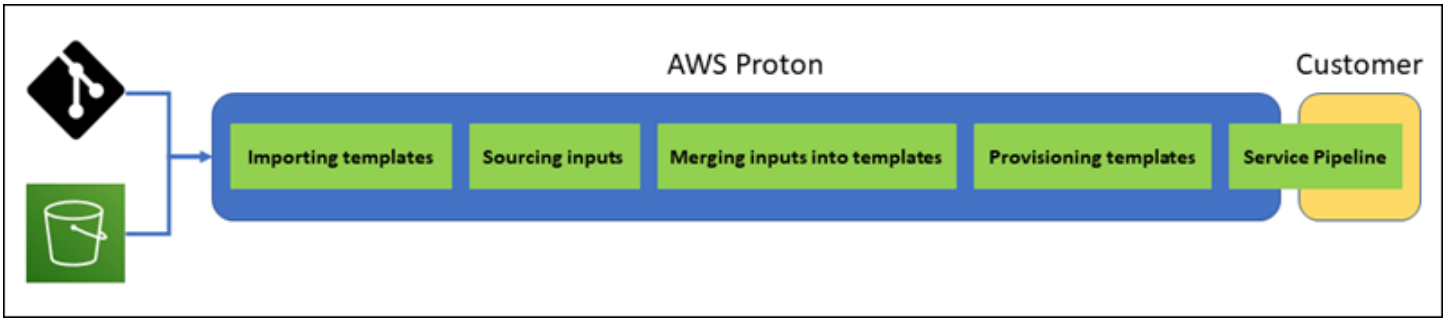
Provisioned	Vorlagen	Provisioned von	Status verfolgt von
AWS-verwaltet	Manifest, Schema, IaC-Datei () CloudFormation	AWS Proton(durchCloudFormation)	AWS Proton(durchCloudFormation)
CodeBuild	Manifest (mit Befehlen), Schema, Befehlsabhängigkeiten (z. B. AWS CDK Code)	AWS Proton(durchCodeBuild)	AWS Proton(Ihre Befehle geben den Status zurück durchCodeBuild)
selbstverwaltet	Manifest, Schema, IaC-Dateien (Terraform)	Dein Code (durch Git-Aktionen)	Ihr Code (AWSper API-Aufruf übergeben)

So funktioniert AWS Managed Provisioning

Wenn eine Umgebung oder ein Dienst AWS verwaltetes Provisioning verwendet, wird die Infrastruktur wie folgt bereitgestellt:

1. Ein AWS Proton Kunde (ein Administrator oder ein Entwickler) erstellt die AWS Proton Ressource (eine Umgebung oder einen Service). Der Kunde wählt eine Vorlage für die Ressource aus und stellt die erforderlichen Parameter bereit. Weitere Informationen finden Sie im folgenden Abschnittthe section called “Überlegungen zur AWS verwalteten Bereitstellung”.
2. AWS Protonrendert eine vollständige AWS CloudFormation Vorlage für die Bereitstellung der Ressource.
3. AWS Protonruft AWS CloudFormation auf, um mit der Bereitstellung mithilfe der gerenderten Vorlage zu beginnen.
4. AWS Protonüberwacht kontinuierlich den AWS CloudFormation Einsatz.
5. Wenn die Bereitstellung abgeschlossen ist, werden im Falle eines Fehlers Fehler AWS Proton gemeldet und im Erfolgsfall werden die Bereitstellungsausgaben wie die Amazon VPC-ID erfasst.

Das folgende Diagramm zeigt, dass die AWS Proton meisten dieser Schritte direkt erledigt werden.



Überlegungen zur AWS verwalteten Bereitstellung

- Rolle zur Infrastrukturbereitstellung — Wenn eine Umgebung oder eine der darin ausgeführten Dienstinstanzen möglicherweise AWS verwaltetes Provisioning verwendet, muss ein Administrator eine IAM-Rolle konfigurieren (entweder direkt oder als Teil einer AWS Proton Umgebungskontoverbindung). AWS Protonverwendet diese Rolle, um die Infrastruktur dieser AWS verwalteten Bereitstellungsressourcen bereitzustellen. Die Rolle sollte über Berechtigungen verfügen, mit AWS CloudFormation denen sie alle Ressourcen erstellen kann, die in den Vorlagen dieser Ressourcen enthalten sind.

  Weitere Informationen erhalten Sie unter the section called “IAM-Rollen” und the section called “Beispiele für Richtlinien für Servicerollen”.
- Servicebereitstellung — Wenn ein Entwickler eine Dienstinstanz bereitstellt, die AWS verwaltete Bereitstellung für die Umgebung verwendet, AWS Proton verwendet er die dieser Umgebung bereitgestellte Rolle, um die Infrastruktur für die Dienstinstanz bereitzustellen. Entwickler sehen diese Rolle nicht und können sie nicht ändern.
- Service mit Pipeline — Eine Dienstvorlage, die AWS verwaltete Bereitstellung verwendet, kann eine im AWS CloudFormation YAML-Schema geschriebene Pipeline-Definition enthalten. AWS Protonerstellt die Pipeline auch durch einen AufrufAWS CloudFormation. Die Rolle, die zum Erstellen einer Pipeline AWS Proton verwendet wird, ist von der Rolle für jede einzelne Umgebung getrennt. Diese Rolle wird AWS Proton separat, nur einmal auf AWS Kontoebene, bereitgestellt und dient der Bereitstellung und Verwaltung aller AWS verwalteten Pipelines. Diese Rolle sollte über Berechtigungen zum Erstellen von Pipelines und anderen Ressourcen verfügen, die Ihre Pipelines benötigen.

  Im folgenden Verfahren wird beschrieben, wie Sie die Pipeline anAWS Proton.

AWS Proton console

Um die Pipeline-Rolle bereitzustellen

1. Wählen Sie in der AWS ProtonKonsole im Navigationsbereich Einstellungen > Kontoeinstellungen und dann Konfigurieren aus.
2. Verwenden Sie den Abschnitt „Mit AWSPipeline verwaltete Rolle“, um eine neue oder bestehende Pipelinerolle für die AWS verwaltete Bereitstellung zu konfigurieren.

AWS Proton API

Um die Pipeline-Rolle bereitzustellen

1. Verwenden Sie die UpdateAccountSettingsAPI-Aktion.
2. Sie müssen für den Amazon-Ressourcennamen (ARN) Ihrer Pipeline `pipelineServiceRoleArn` an.

AWS CLI

Um die Pipeline-Rolle bereitzustellen

Führen Sie den Befehl aus:

```
$ aws proton update-account-settings \
    --pipeline-service-role-arn \
        "arn:aws:iam::123456789012:role/my-pipeline-role"
```

So CodeBuild funktioniert die Bereitstellung

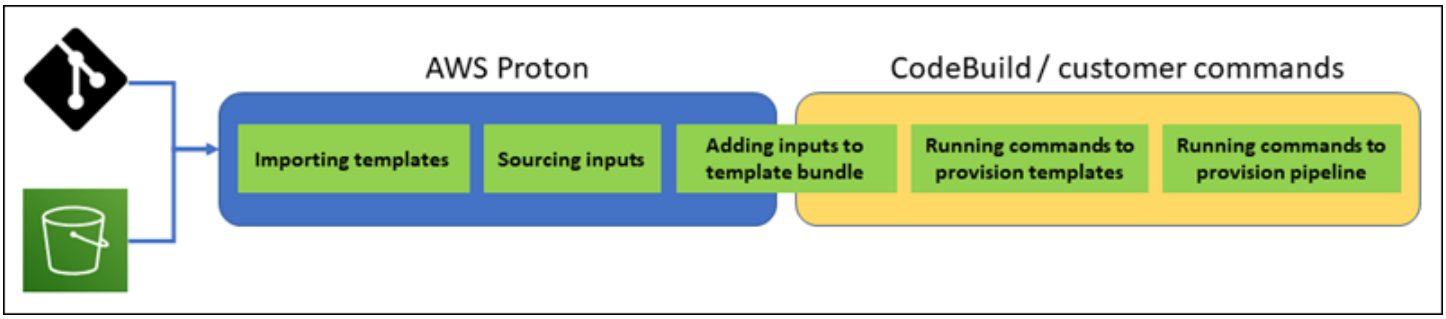
Wenn eine Umgebung oder ein Service CodeBuild Provisioning verwendet, wird die Infrastruktur wie folgt bereitgestellt:

1. Ein AWS Proton Kunde (ein Administrator oder ein Entwickler) erstellt die AWS Proton Ressource (eine Umgebung oder einen Service). Der Kunde wählt eine Vorlage für die Ressource aus und stellt die erforderlichen Parameter bereit. Weitere Informationen finden Sie im folgenden Abschnittthe section called “Überlegungen zur CodeBuild Bereitstellung”.

2. AWS Protonrendert eine Eingabedatei mit Eingabeparameterwerten für die Bereitstellung der Ressource.
3. AWS Protonruft CodeBuild an, um einen Job zu beginnen. Der CodeBuild Job führt die in der Vorlage angegebenen Customer-Shell-Befehle aus. Diese Befehle stellen die gewünschte Infrastruktur bereit und lesen optional Eingabewerte.
4. Wenn die Bereitstellung abgeschlossen ist, gibt der Befehl final customer den Bereitstellungsstatus an zurück CodeBuild und ruft die NotifyResourceDeploymentStatusChangeAWS ProtonAPI-Aktion auf, um Ausgaben wie die Amazon VPC-ID bereitzustellen, falls vorhanden.

> **Important**
>
> Stellen Sie sicher, dass Ihre Befehle den Bereitstellungsstatus korrekt an zurückgeben CodeBuild und die Ausgaben bereitstellen. Wenn sie dies nicht tun, AWS Proton können sie den Bereitstellungsstatus nicht richtig verfolgen und den Service-Instances keine korrekten Ausgaben bereitstellen.

Das folgende Diagramm veranschaulicht die Schritte, die AWS Proton ausgeführt werden, und die Schritte, die Ihre Befehle innerhalb eines CodeBuild Jobs ausführen.



Überlegungen zur CodeBuild Bereitstellung

- Rolle zur Infrastrukturbereitstellung — Wenn eine Umgebung oder eine der darin ausgeführten Dienstinstanzen möglicherweise CodeBuild basiertes Provisioning verwendet, muss ein Administrator eine IAM-Rolle konfigurieren (entweder direkt oder als Teil einer AWS Proton Umgebungskontoverbindung). AWS Protonverwendet diese Rolle, um die Infrastruktur dieser CodeBuild Bereitstellungsressourcen bereitzustellen. Die Rolle sollte über Berechtigungen verfügen, mit denen CodeBuild Sie alle Ressourcen erstellen können, die Ihre Befehle in den Vorlagen dieser Ressourcen bereitstellen.

Weitere Informationen erhalten Sie unter the section called “IAM-Rollen” und the section called “Beispiele für Richtlinien für Servicerollen”.

- Servicebereitstellung — Wenn ein Entwickler eine Dienstinstanz bereitstellt, die CodeBuild Provisioning für die Umgebung verwendet, AWS Proton verwendet er die dieser Umgebung bereitgestellte Rolle, um die Infrastruktur für die Dienstinstanz bereitzustellen. Entwickler sehen diese Rolle nicht und können sie nicht ändern.
- Service mit Pipeline — Eine Dienstvorlage, die CodeBuild Provisioning verwendet, kann Befehle zur Bereitstellung einer Pipeline enthalten. AWS Protonerstellt die Pipeline auch durch einen AufrufCodeBuild. Die Rolle, die zum Erstellen einer Pipeline AWS Proton verwendet wird, ist von der Rolle für jede einzelne Umgebung getrennt. Diese Rolle wird AWS Proton separat, nur einmal auf AWS Kontoebene, bereitgestellt und dient der Bereitstellung und Verwaltung aller CodeBuild basierten Pipelines. Diese Rolle sollte über Berechtigungen zum Erstellen von Pipelines und anderen Ressourcen verfügen, die Ihre Pipelines benötigen.

  Im folgenden Verfahren wird beschrieben, wie Sie die Pipeline anAWS Proton.

  AWS Proton console

  Um die Pipeline-Rolle bereitzustellen

  1. Wählen Sie in der AWS ProtonKonsole im Navigationsbereich Einstellungen > Kontoeinstellungen und dann Konfigurieren aus.
  2. Verwenden Sie den Abschnitt Codebuild-Pipeline-Bereitstellungsrolle, um eine neue oder bestehende Pipelinerolle für CodeBuild die Bereitstellung zu konfigurieren.

  AWS Proton API

  Um die Pipeline-Rolle bereitzustellen

  1. Verwenden Sie die UpdateAccountSettingsAPI-Aktion.
  2. Sie müssen für den Amazon-Ressourcennamen (ARN) Ihrer Pipeline `pipelineCodebuildRoleArn` an.

  AWS CLI

  Um die Pipeline-Rolle bereitzustellen

Führen Sie den Befehl aus:

```
$ aws proton update-account-settings \
    --pipeline-codebuild-role-arn \
        "arn:aws:iam::123456789012:role/my-pipeline-role"
```

So funktioniert Selbstverwaltetes Provisioning

Wenn eine Umgebung so konfiguriert ist, dass sie selbstverwaltete Bereitstellung verwendet, wird die Infrastruktur wie folgt bereitgestellt:

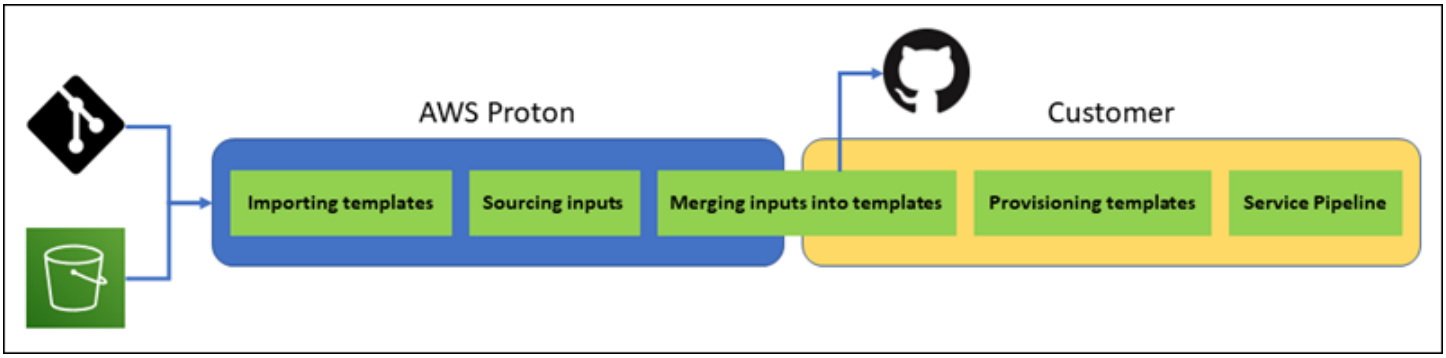
1. Ein AWS Proton Kunde (ein Administrator oder ein Entwickler) erstellt die AWS Proton Ressource (eine Umgebung oder einen Service). Der Kunde wählt eine Vorlage für die Ressource aus und stellt die erforderlichen Parameter bereit. Für eine Umgebung stellt der Kunde auch ein verknüpftes Infrastruktur-Repository bereit. Weitere Informationen finden Sie im folgenden Abschnittthe section called “Überlegungen zur Selbstverwalteten Provisioned”.
2. AWS Protonrendert eine vollständige Terraform-Vorlage. Es besteht aus einer oder mehreren Terraform-Dateien, möglicherweise in mehreren Ordnern, und einer `.tfvars` Variablendatei. AWS Protonschreibt die beim Aufruf zur Ressourcenerstellung bereitgestellten Parameterwerte in diese Variablendatei.
3. AWS Protonübermittelt eine PR mit der gerenderten Terraform-Vorlage an das Infrastruktur-Repository.
4. Wenn der Kunde (Administrator oder Entwickler) die PR zusammenführt, veranlasst die Automatisierung des Kunden die Provisioning Engine, mit der Bereitstellung der Infrastruktur unter Verwendung der zusammengeführten Vorlage zu beginnen.

   > **Note**
   >
   > Wenn der Kunde (Administrator oder Entwickler) die PR schließt, AWS Proton erkennt er die PR als abgeschlossen an und markiert die Bereitstellung als storniert.

5. Wenn die Bereitstellung abgeschlossen ist, ruft die Automatisierung des Kunden die NotifyResourceDeploymentStatusChangeAWS ProtonAPI-Aktion auf, um den Abschluss anzuzeigen, den Status (Erfolg oder Misserfolg) bereitzustellen und gegebenenfalls Ausgaben wie die Amazon VPC-ID bereitzustellen.

> **Important**
>
> Stellen Sie sicher, dass Ihr Automatisierungscode AWS Proton mit dem Bereitstellungsstatus und den Ausgaben zurückruft. Ist dies nicht der Fall, wird die Bereitstellung AWS Proton möglicherweise länger als ausstehend angesehen, als sie sollte, und zeigt weiterhin den Status In Bearbeitung an.

Das folgende Diagramm veranschaulicht die Schritte, die AWS Proton ausgeführt werden, und die Schritte, die Ihr eigenes Provisioningsystem ausführt.



Überlegungen zur Selbstverwalteten Provisioned

- Infrastruktur-Repository — Wenn ein Administrator eine Umgebung für die selbstverwaltete Bereitstellung konfiguriert, muss er ein verknüpftes Infrastruktur-Repository bereitstellen. AWS Protonübermittelt PRs an dieses Repository, um die Infrastruktur der Umgebung und alle dort bereitgestellten Serviceinstanzen bereitzustellen. Die kundeneigene Automatisierungsaktion im Repository sollte eine IAM-Rolle übernehmen und über Berechtigungen zum Erstellen aller Ressourcen verfügen, die Ihre Umgebung und Servicevorlagen enthalten, sowie eine Identität, die das AWS Zielkonto widerspiegelt. Ein Beispiel für eine GitHub Aktion, die eine Rolle annimmt, finden Sie unter Eine Rolle annehmen in der Dokumentation zur Aktion „AWSAnmeldeinformationen konfigurieren“ für GitHub Aktionen.
- Berechtigungen — Ihr Bereitstellungscode muss sich bei Bedarf mit einem Konto authentifizieren (z. B. bei einem AWS Konto authentifizieren) und eine Autorisierung für die Ressourcenbereitstellung bereitstellen (z. B. eine Rolle angeben).
- Servicebereitstellung — Wenn ein Entwickler eine Serviceinstanz bereitstellt, die selbstverwaltete Bereitstellung für die Umgebung verwendet, AWS Proton übermittelt er eine PR an das Repository,

das der Umgebung zugeordnet ist, um die Infrastruktur für die Dienstinstanz bereitzustellen. Entwickler sehen das Repository nicht und können es nicht ändern.

> **Note**
>
> Entwickler, die Dienste erstellen, verwenden unabhängig von der Bereitstellungsmethode denselben Prozess, und der Unterschied wird von ihnen abstrahiert. Bei selbstverwalteter Bereitstellung reagieren Entwickler jedoch möglicherweise langsamer, da sie warten müssen, bis jemand (der möglicherweise nicht sie selbst ist) die PR im Infrastruktur-Repository zusammenführt, bevor die Bereitstellung beginnen kann.

- Service mit Pipeline — Eine Dienstvorlage für eine Umgebung mit selbstverwalteter Bereitstellung kann eine in Terraform HCL geschriebene Pipeline-Definition (z. B. eine AWS CodePipeline Pipeline) enthalten. Um die Bereitstellung dieser Pipelines AWS Proton zu ermöglichen, stellt ein Administrator ein verknüpftes Pipeline-Repository bereitAWS Proton. Bei der Bereitstellung einer Pipeline sollte die kundeneigene Automatisierungsaktion im Repository eine IAM-Rolle mit Berechtigungen zur Bereitstellung der Pipeline und einer Identität übernehmen, die das Zielkonto widerspiegelt. AWS Das Pipeline-Repository und die Rolle unterscheiden sich von denen, die für jede einzelne Umgebung verwendet werden. Das verknüpfte Repository wird AWS Proton separat bereitgestellt, nur einmal auf AWS Kontoebene, und es wird zur Bereitstellung und Verwaltung aller Pipelines verwendet. Die Rolle sollte über Berechtigungen zum Erstellen von Pipelines und anderen Ressourcen verfügen, die Ihre Pipelines benötigen.

  Im folgenden Verfahren wird beschrieben, wie Sie das Pipeline-Repository und die Rolle anAWS Proton.

  AWS Proton console

  Um die Pipeline-Rolle bereitzustellen

  1. Wählen Sie in der AWS ProtonKonsole im Navigationsbereich Einstellungen > Kontoeinstellungen und dann Konfigurieren aus.
  2. Verwenden Sie den Abschnitt CI/CD-Pipeline-Repository, um einen neuen oder vorhandenen Repository-Link zu konfigurieren.

AWS Proton API

Um die Pipeline-Rolle bereitzustellen

1. Verwenden Sie die UpdateAccountSettingsAPI-Aktion.
2. Geben Sie den Anbieter, den Namen und den Zweig Ihres Pipeline-Repositorys im `pipelineProvisioningRepository` Parameter an.

AWS CLI

Um die Pipeline-Rolle bereitzustellen

Führen Sie den Befehl aus:

```
$ aws proton update-account-settings \
    --pipeline-provisioning-repository \
        "provider=GITHUB,name=my-pipeline-repo-name,branch=my-branch"
```

- Löschen von selbst verwalteten bereitgestellten Ressourcen — Terraform-Module können neben Ressourcendefinitionen auch Konfigurationselemente enthalten, die für den Terraform-Betrieb erforderlich sind. Daher AWS Proton können nicht alle Terraform-Dateien für eine Umgebung oder Dienstinstanz gelöscht werden. AWS ProtonMarkiert stattdessen die Dateien zum Löschen und aktualisiert eine Markierung in den PR-Metadaten. Ihre Automatisierung kann diese Flagge lesen und sie verwenden, um einen Terraform-Zerstörungsbefehl auszulösen.

AWS Proton-Terminologie

Vorlage „Umgebung“

Definiert eine gemeinsam genutzte Infrastruktur, z. B. eine VPC oder einen Cluster, die von mehreren Anwendungen oder Ressourcen verwendet wird.

Paket mit Umgebungsvorlagen

Eine Sammlung von Dateien, die Sie hochladen, um eine Umgebungsvorlage zu erstellen und zu registrierenAWS Proton. Ein Paket mit Umgebungsvorlagen enthält Folgendes:

1. Eine Schemadatei, die Infrastruktur als Codeeingabeparameter definiert.

2. Eine IaC-Datei (Infrastructure as Code), die eine gemeinsam genutzte Infrastruktur wie eine VPC oder einen Cluster definiert, die von mehreren Anwendungen oder Ressourcen verwendet wird.
3. Eine Manifestdatei, die die IaC-Datei auflistet.

Umgebung

Bereitgestellte gemeinsam genutzte Infrastruktur, z. B. eine VPC oder ein Cluster, die von mehreren Anwendungen oder Ressourcen verwendet wird.

Servicevorlage

Definiert die Art der Infrastruktur, die für die Bereitstellung und Wartung einer Anwendung oder eines Microservices in einer Umgebung erforderlich ist.

Servicevorlagenpaket

Eine Sammlung von Dateien, die Sie hochladen, um eine Dienstvorlage zu erstellen und zu registrierenAWS Proton. Ein Service-Vorlagenpaket enthält Folgendes:

1. Eine Schemadatei, die Eingabeparameter für Infrastruktur als Code (IaC) definiert.
2. Eine IaC-Datei, die die Infrastruktur definiert, die für die Bereitstellung und Wartung einer Anwendung oder eines Microservices in einer Umgebung erforderlich ist.
3. Eine Manifestdatei, die die IaC-Datei auflistet.
4. Optional
   a. Eine IaC-Datei, die die Infrastruktur der Service Pipeline definiert.
   b. Eine Manifestdatei, die die IaC-Datei auflistet.

Service

Bereitgestellte Infrastruktur, die für die Bereitstellung und Wartung einer Anwendung oder eines Microservices in einer Umgebung erforderlich ist.

Service-Instance

Bereitgestellte Infrastruktur, die eine Anwendung oder einen Microservice in einer Umgebung unterstützt.

Service-Pipeline

Bereitgestellte Infrastruktur, die eine Pipeline unterstützt.

Vorlagenversion

Eine Haupt- oder Nebenversion einer Vorlage. Weitere Informationen finden Sie unter Versionierte Vorlagen.

Eingabeparameter

In einer Schemadatei definiert und in einer Infrastruktur als Codedatei (IaC) verwendet, sodass die IaC-Datei wiederholt und für eine Vielzahl von Anwendungsfällen verwendet werden kann.

Schema-Datei

Definiert Infrastruktur als Eingabeparameter für Codedateien.

Spezifikationsdatei

Gibt Werte für die Infrastruktur als Codedatei-Eingabeparameter an, wie sie in einer Schemadatei definiert sind.

Manifestdatei

Listet eine Infrastruktur als Codedatei auf.

Erstellen von Vorlagen und Erstellen von Paketen für AWS Proton

AWS Proton stellt Ressourcen basierend auf Infrastructure as Code (IaC)-Dateien für Sie bereit. Sie beschreiben die Infrastruktur in wiederverwendbaren IaC-Dateien. Um die Dateien für verschiedene Umgebungen und Anwendungen wiederverwendbar zu machen, erstellen Sie sie als Vorlagen, definieren Eingabeparameter und verwenden diese Parameter in IaC-Definitionen. Wenn Sie später eine Bereitstellungsressource (Umgebung, Service-Instance oder Komponente) erstellen, AWS Proton verwendet eine Rendering-Engine, die Eingabewerte mit einer Vorlage kombiniert, um eine IaC-Datei zu erstellen, die bereit für die Bereitstellung ist.

Administratoren erstellen die meisten Vorlagen als Vorlagenpakete und laden sie dann hoch und registrieren sie in AWS Proton. Der Rest dieser Seite behandelt diese AWS Proton Vorlagenpakete. Direkt definierte Komponenten sind eine Ausnahme – Entwickler erstellen sie und stellen IaC-Vorlagendateien direkt bereit. Weitere Informationen zu Komponenten finden Sie unter Komponenten.

Themen

Vorlagenpakete

Als Administrator erstellen und registrieren Sie Vorlagen bei AWS Proton. Sie verwenden diese Vorlagen, um Umgebungen und Services zu erstellen. Wenn Sie einen Service erstellen, stellt Service-Instances AWS Proton bereit und stellt sie in ausgewählten Umgebungen bereit. Weitere Informationen finden Sie unter AWS Protonfür Plattformteams.

Um eine Vorlage in zu erstellen und zu registrieren AWS Proton, laden Sie ein Vorlagenpaket hoch, das die Infrastructure as Code (IaC)-Dateien enthält, die bereitstellen und die Umgebung oder den Service bereitstellen AWS Proton müssen.

Ein Vorlagenpaket enthält Folgendes:

- Eine Infrastructure as Code (IaC)-Datei mit einer YAML-Manifestdatei, die die IaC-Datei auflistet.
- Eine Schema-YAML-Datei für Ihre Parameterdefinitionen für die IaC-Dateieingabe.

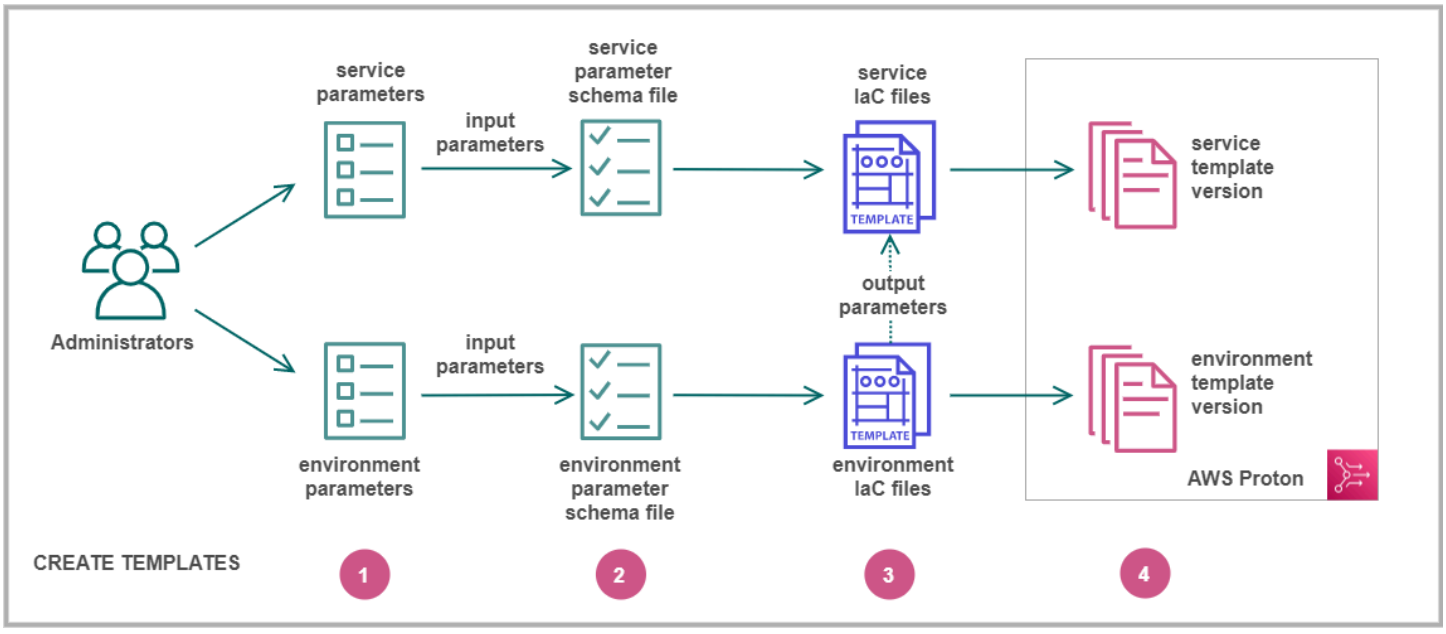
Ein CloudFormation Umgebungsvorlagenpaket enthält eine IaC-Datei.

Ein CloudFormation Servicevorlagenpaket enthält eine IaC-Datei für Service-Instance-Definitionen und eine weitere optionale IaC-Datei für eine Pipeline-Definition.

Pakete für Terraform-Umgebungen und -Servicevorlagen können jeweils mehrere IaC-Dateien enthalten.

AWS Proton erfordert eine Eingabeparameter-Schemadatei. Wenn Sie AWS CloudFormation zum Erstellen Ihrer IaC-Dateien verwenden, verwenden Sie die Jinja-Syntax, um auf Ihre Eingabeparameter zu verweisen. AWS Proton stellt Parameter-Namespaces bereit, mit denen Sie auf Parameter in Ihren IaC-Dateien verweisen können.

Das folgende Diagramm zeigt ein Beispiel für Schritte, die Sie ausführen können, um eine Vorlage für zu erstellen AWS Proton.



1

Identifizieren Sie die Eingabeparameter .

2

Erstellen Sie eine Schemadatei, um Ihre Eingabeparameter zu definieren.

3

Erstellen Sie IaC-Dateien, die auf Ihre Eingabeparameter verweisen. Sie können auf UmgebungsIaC-Dateiausgaben als Eingaben für Ihre Service-IaC-Dateien verweisen.

4

Registrieren Sie eine Vorlagenversion bei AWS Proton und laden Sie Ihr Vorlagenpaket hoch.

AWS Proton -Parameter

Sie können Parameter in Ihren Infrastructure as Code (IaC)-Dateien definieren und verwenden, um sie flexibel und wiederverwendbar zu machen. Sie lesen einen Parameterwert in Ihren IaC-Dateien, indem Sie auf den Namen des Parameters im AWS Proton Parameter-Namespace verweisen. AWS Proton Injects Parameterwerte in die gerenderten IaC-Dateien, die während der Ressourcenbereitstellung generiert werden. Um AWS CloudFormation IaC-Parameter zu verarbeiten, AWS Proton verwendet Jinja . Um Terraform-IaC-Parameter zu verarbeiten, AWS Proton generiert eine Terraform-Parameterwertdatei und stützt sich auf die in HCL integrierten Parametrisierungsfunktionen.

Mit AWS Proton generiert eine EingabedateiCodeBuildBereitstellung, die Ihr Code importieren kann. Die Datei ist eine JSON- oder HCL-Datei, abhängig von einer Eigenschaft im Manifest Ihrer Vorlage. Weitere Informationen finden Sie unter the section called “CodeBuild Bereitstellungsparameter”.

Sie können mit den folgenden Anforderungen auf Parameter in Ihren IaC-Dateien oder Komponenten verweisen:

- Die Länge der einzelnen Parameternamen darf 100 Zeichen nicht überschreiten.
- Die Länge des Parameter-Namespaces und des Ressourcennamens zusammengenommen überschreitet das Zeichenlimit für den Ressourcennamen nicht.

AWS Proton Die Bereitstellung schlägt fehl, wenn diese Kontingente überschritten werden.

Parametertypen

Die folgenden Parametertypen stehen Ihnen als Referenz in AWS Proton IaC-Dateien zur Verfügung:

Eingabeparameter

Umgebungen und Service-Instances können Eingabeparameter übernehmen, die Sie in einer Schemadatei definieren, die Sie der Umgebung oder Servicevorlage zuordnen. Sie können auf die Eingabeparameter einer Ressource in der IaC-Datei der Ressource verweisen. Komponenten-IaC-Dateien können sich auf Eingabeparameter der Service-Instance beziehen, an die die Komponente angefügt ist.

AWS Proton überprüft die Namen der Eingabeparameter anhand Ihrer Schemadatei und gleicht sie mit den Parametern ab, auf die in Ihren IaC-Dateien verwiesen wird, um die Eingabewerte einzufügen, die Sie während der Ressourcenbereitstellung in einer Spezifikationsdatei angeben.

Ausgabeparameter

Sie können Ausgaben in jeder Ihrer IaC-Dateien definieren. Eine Ausgabe kann beispielsweise ein Name, eine ID oder ein ARN einer der Ressourcen sein, die die Vorlage bereitstellt, oder sie kann eine Möglichkeit sein, eine der Eingaben der Vorlage zu durchlaufen. Sie können auf diese Ausgaben in IaC-Dateien anderer Ressourcen verweisen.

Definieren Sie in CloudFormation IaC-Dateien Ausgabeparameter im -`Outputs:`Block. Definieren Sie in einer Terraform-IaC-Datei jeden Ausgabeparameter mithilfe einer -`output`Anweisung.

Ressourcenparameter

AWS Proton erstellt automatisch AWS Proton Ressourcenparameter. Diese Parameter stellen Eigenschaften des AWS Proton Ressourcenobjekts bereit. Ein Beispiel für einen Ressourcenparameter ist `environment.name`.

Verwenden von AWS Proton Parametern in Ihren IaC-Dateien

Um einen Parameterwert in einer IaC-Datei zu lesen, verweisen Sie auf den Namen des Parameters im AWS Proton Parameter-Namespace. Für AWS CloudFormation IaC-Dateien verwenden Sie die Jinja-Syntax und umgeben den Parameter mit Paaren von geschweiften Klammern und Anführungszeichen.

Die folgende Tabelle zeigt die Referenzsyntax für jede unterstützte Vorlagensprache, mit einem Beispiel.

Vorlagensprache	Syntax	Beispiel: Umgebungseingabe mit dem Namen „VPC“
CloudFormation	`"{{ parameter-name }}"`	`"{{ environment.inputs.VPC }}"`
Terraform	`var.parameter-name`	`var.environment.inputs.VPC` Generierte Terraform-Variablendefinitionen

> **Note**
>
> Wenn Sie CloudFormation dynamische Parameter in Ihrer IaC-Datei verwenden, müssen Sie sie mit Escape-Zeichen versehen, um Jinja-Fehler bei der Fehlinterpretation zu vermeiden. Weitere Informationen finden Sie unter Fehlerbehebung für AWS Proton.

In der folgenden Tabelle sind Namespace-Namen für alle AWS Proton Ressourcenparameter aufgeführt. Jeder Vorlagendateityp kann eine andere Teilmenge des Parameter-Namespace verwenden.

Vorlagendatei	Parametertyp	Parametername	Beschreibung
Umgebung	Ressourc	`environment.` **`name`**	Environment name
	input	`environment.inputs.` *`input-name`*	Schemadefinierte Umgebungseingaben
Service	Ressourc	`environment.` **`name`** `environment.` **`account_id`**	Name und AWS-Konto ID der Umgebung
	output	`environment.outputs.` *`output-name`*	Umgebungs-IaC-Dateiausgaben
	Ressourc	`service.`**`branch_name`**	Servicename und Code-Repository

Vorlagendatei	Parametertyp	Parametername	Beschreibung
		`service.`**`name`** `service.`**`repository_connection_arn`** `service.`**`repository_id`**	
	Ressourc	`service_instance.` **`name`**	Name der Service-Instance
	input	`service_instance.inputs.` *`input-name`*	Schemadefinierte Service-Instance-Eingaben
	Ressourc	`service_instance.components.default.` **`name`**	Angefügter Standardkomponentenname
	output	`service_instance.components.default.outputs.` *`output-name`*	Angefügte IaC-Standarddateiausgaben der Komponente
Pipeline	Ressourc	`service_instance.environment.` **`name`** `service_instance.environment.` **`account_id`**	Name und AWS-Konto ID der Service-Instance-Umgebung
	output	`service_instance.environment.outputs.` *`output-name`*	IaC-Dateiausgaben der Service-Instance-Umgebung
	input	`pipeline.inputs.` *`input-name`*	Schemadefinierte Pipeline-Eingaben

Vorlagendatei	Parametertyp	Parametername	Beschreibung
	Ressourc	`service.`**`branch_name`** `service.`**`name`** `service.`**`repository_connection_arn`** `service.`**`repository_id`**	Servicename und Code-Repository
	input	`service_instance.inputs.` *`input-name`*	Schemadefinierte Service-Instance-Eingaben
	collection	`{% for service_instance in` **`service_instances`** `%}...{% endfor %}`	Eine Sammlung von Service-Instances, die Sie durchlaufen können
Komponente	Ressourc	`environment.` **`name`** `environment.` **`account_id`**	Umgebungsname und AWS-Konto Konto-ID
	output	`environment.outputs.` *`output-name`*	Umgebungs-IaC-Dateiausgaben
	Ressourc	`service.`**`branch_name`** `service.`**`name`** `service.`**`repository_connection_arn`** `service.`**`repository_id`**	Servicename und Code-Repository (angefügte Komponenten)
	Ressourc	`service_instance.` **`name`**	Name der Service-Instance (angefügte Komponenten)

Vorlagendatei	Parametertyp	Parametername	Beschreibung
	input	`service_instance.inputs.` *`input-name`*	Schemadefinierte Service-Instance-Eingaben (angefügte Komponenten)
	Ressourc	`component.` **`name`**	Name der Komponente

Weitere Informationen und Beispiele finden Sie in den Unterthemen zu Parametern in IaC-Vorlagendateien für verschiedene Ressourcentypen und Vorlagensprachen.

Themen

- Details und Beispiele für Umgebungs- CloudFormation IaC-Dateiparameter
- Details und Beispiele für Service- CloudFormation IaC-Dateiparameter
- Details und Beispiele für Komponenten- CloudFormation IaC-Dateiparameter
- Parameterfilter für CloudFormation IaC-Dateien
- CodeBuild Details und Beispiele für Bereitstellungsparameter
- Details und Beispiele für Terraform Infrastructure as Code (IaC)-Dateiparameter

Details und Beispiele für Umgebungs- CloudFormation IaC-Dateiparameter

Sie können Parameter in Ihren IaC-Dateien (Environment Infrastructure as Code) definieren und referenzieren. Eine detaillierte Beschreibung der AWS Proton Parameter, Parametertypen, des Parameter-Namespace und der Verwendung von Parametern in Ihren IaC-Dateien finden Sie unter the section called “Parameter”.

Definieren von Umgebungsparametern

Sie können sowohl Eingabe- als auch Ausgabeparameter für Umgebungs-IaC-Dateien definieren.

- Eingabeparameter – Definieren Sie Umgebungseingabeparameter in Ihrer Schemadatei .

  Die folgende Liste enthält Beispiele für Umgebungseingabeparameter für typische Anwendungsfälle.

- VPC-CIDR-Werte
- Load Balancer-Einstellungen
- Datenbankeinstellungen
- Ein Timeout für die Zustandsprüfung

Als Administrator können Sie Werte für Eingabeparameter angeben, wenn Sie eine Umgebung erstellen:

- Verwenden Sie die -Konsole, um ein schemabasiertes Formular auszufüllen, das AWS Proton bereitstellt.
- Verwenden Sie die CLI, um eine Spezifikation bereitzustellen, die die Werte enthält.

- Ausgabeparameter – Definieren Sie Umgebungsausgaben in Ihren IaC-Dateien der Umgebung. Sie können dann in IaC-Dateien anderer Ressourcen auf diese Ausgaben verweisen.

Lesen von Parameterwerten in Umgebungs-IaC-Dateien

Sie können Parameter im Zusammenhang mit der Umgebung in IaC-Dateien der Umgebung lesen. Sie lesen einen Parameterwert, indem Sie auf den Namen des Parameters im AWS Proton Parameter-Namespace verweisen.

- Eingabeparameter – Lesen Sie einen Umgebungseingabewert, indem Sie auf verweisen`environment.inputs.`*`input-name`*.
- Ressourcenparameter – Lesen Sie AWS Proton Ressourcenparameter, indem Sie auf Namen wie verweisen`environment.name`.

> **Note**
>
> Für Umgebungs-IaC-Dateien sind keine Ausgabeparameter anderer Ressourcen verfügbar.

Beispiel für Umgebungs- und ServiceIaC-Dateien mit Parametern

Das folgende Beispiel zeigt die Parameterdefinition und -referenz in einer IaC-Datei. Das Beispiel zeigt dann, wie in der IaC-Umgebungsdatei definierte Umgebungsausgabeparameter in einer Service-IaC-Datei referenziert werden können.

Example Umgebungs- CloudFormation IaC-Datei

Beachten Sie in diesem Beispiel Folgendes:

- Der `environment.inputs.` Namespace bezieht sich auf Umgebungseingabeparameter.
- Der Amazon EC2 Systems Manager (SSM)-Parameter `StoreInputValue` verkettet die Umgebungseingaben.
- Die `MyEnvParameterValue` Ausgabe stellt dieselbe Eingabeparameterverkettung wie ein Ausgabeparameter bereit. Drei zusätzliche Ausgabeparameter stellen die Eingabeparameter auch einzeln bereit.
- Sechs zusätzliche Ausgabeparameter stellen Ressourcen bereit, die die Umgebung bereitstellt.

```
Resources:
  StoreInputValue:
    Type: AWS::SSM::Parameter
    Properties:
      Type: String
      Value: "{{ environment.inputs.my_sample_input }}
 {{ environment.inputs.my_other_sample_input}}
 {{ environment.inputs.another_optional_input }}"
              # input parameter references

# These output values are available to service infrastructure as code files as outputs,
 when given the
# the 'environment.outputs' namespace, for example,
 service_instance.environment.outputs.ClusterName.
Outputs:
  MyEnvParameterValue:                                    # output definition
    Value: !GetAtt StoreInputValue.Value
  MySampleInputValue:                                     # output definition
    Value: "{{ environment.inputs.my_sample_input }}"         #   input parameter
 reference
  MyOtherSampleInputValue:                                # output definition
    Value: "{{ environment.inputs.my_other_sample_input }}"   #   input parameter
 reference
  AnotherOptionalInputValue:                              # output definition
    Value: "{{ environment.inputs.another_optional_input }}"  #   input parameter
 reference
  ClusterName:                                            # output definition
    Description: The name of the ECS cluster
    Value: !Ref 'ECSCluster'                              #   provisioned resource
```

```
  ECSTaskExecutionRole:                                    # output definition
    Description: The ARN of the ECS role
    Value: !GetAtt 'ECSTaskExecutionRole.Arn'              #   provisioned resource
  VpcId:                                                   # output definition
    Description: The ID of the VPC that this stack is deployed in
    Value: !Ref 'VPC'                                      #   provisioned resource
  PublicSubnetOne:                                         # output definition
    Description: Public subnet one
    Value: !Ref 'PublicSubnetOne'                          #   provisioned resource
  PublicSubnetTwo:                                         # output definition
    Description: Public subnet two
    Value: !Ref 'PublicSubnetTwo'                          #   provisioned resource
  ContainerSecurityGroup:                                  # output definition
    Description: A security group used to allow Fargate containers to receive traffic
    Value: !Ref 'ContainerSecurityGroup'                   #   provisioned resource
```

Example Service CloudFormation IaC-Datei

Der `environment.outputs.` Namespace bezieht sich auf Umgebungsausgaben aus einer IaC-Datei. Der Name `environment.outputs.ClusterName` liest beispielsweise den Wert des `ClusterName` Umgebungsausgabeparameters.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Deploy a service on AWS Fargate, hosted in a public subnet, and accessible
 via a public load balancer.
Mappings:
  TaskSize:
    x-small:
      cpu: 256
      memory: 512
    small:
      cpu: 512
      memory: 1024
    medium:
      cpu: 1024
      memory: 2048
    large:
      cpu: 2048
      memory: 4096
    x-large:
      cpu: 4096
      memory: 8192
Resources:
```

```
  # A log group for storing the stdout logs from this service's containers
  LogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: '{{service_instance.name}}' # resource parameter

  # The task definition. This is a simple metadata description of what
  # container to run, and what resource requirements it has.
  TaskDefinition:
    Type: AWS::ECS::TaskDefinition
    Properties:
      Family: '{{service_instance.name}}' # resource parameter
      Cpu: !FindInMap [TaskSize, {{service_instance.inputs.task_size}}, cpu] # input
parameter
      Memory: !FindInMap [TaskSize, {{service_instance.inputs.task_size}}, memory]
      NetworkMode: awsvpc
      RequiresCompatibilities:
        - FARGATE
      ExecutionRoleArn: '{{environment.outputs.ECSTaskExecutionRole}}'  # output
reference to an environment infrastructure code file
      TaskRoleArn: !Ref "AWS::NoValue"
      ContainerDefinitions:
        - Name: '{{service_instance.name}}'  # resource parameter
          Cpu: !FindInMap [TaskSize, {{service_instance.inputs.task_size}}, cpu]
          Memory: !FindInMap [TaskSize, {{service_instance.inputs.task_size}}, memory]
          Image: '{{service_instance.inputs.image}}'
          PortMappings:
            - ContainerPort: '{{service_instance.inputs.port}}' # input parameter
          LogConfiguration:
            LogDriver: 'awslogs'
            Options:
              awslogs-group: '{{service_instance.name}}' # resource parameter
              awslogs-region: !Ref 'AWS::Region'
              awslogs-stream-prefix: '{{service_instance.name}}' # resource parameter

  # The service_instance. The service is a resource which allows you to run multiple
  # copies of a type of task, and gather up their logs and metrics, as well
  # as monitor the number of running tasks and replace any that have crashed
  Service:
    Type: AWS::ECS::Service
    DependsOn: LoadBalancerRule
    Properties:
      ServiceName: '{{service_instance.name}}'  # resource parameter
```

```
      Cluster: '{{environment.outputs.ClusterName}}' # output reference to an
 environment infrastructure as code file
      LaunchType: FARGATE
      DeploymentConfiguration:
        MaximumPercent: 200
        MinimumHealthyPercent: 75
      DesiredCount: '{{service_instance.inputs.desired_count}}'# input parameter
      NetworkConfiguration:
        AwsvpcConfiguration:
          AssignPublicIp: ENABLED
          SecurityGroups:
            - '{{environment.outputs.ContainerSecurityGroup}}' # output reference to an
 environment infrastructure as code file
          Subnets:
            - '{{environment.outputs.PublicSubnetOne}}' # output reference to an
 environment infrastructure as code file
            - '{{environment.outputs.PublicSubnetTwo}}' # output reference to an
 environment infrastructure as code file
      TaskDefinition: !Ref 'TaskDefinition'
      LoadBalancers:
        - ContainerName: '{{service_instance.name}}'  # resource parameter
          ContainerPort: '{{service_instance.inputs.port}}' # input parameter
          TargetGroupArn: !Ref 'TargetGroup'
[...]
```

Details und Beispiele für Service- CloudFormation IaC-Dateiparameter

Sie können Parameter in Ihren Service- und Pipeline-Infrastruktur-as-Code (IaC)-Dateien definieren und referenzieren. Eine detaillierte Beschreibung der AWS Proton Parameter, Parametertypen, des Parameter-Namespace und der Verwendung von Parametern in Ihren IaC-Dateien finden Sie unter the section called “Parameter”.

Definieren von Serviceparametern

Sie können sowohl Eingabe- als auch Ausgabeparameter für Service-IaC-Dateien definieren.

- Eingabeparameter – Definieren Sie Eingabeparameter der Service-Instance in Ihrer Schemadatei .

  Die folgende Liste enthält Beispiele für Serviceeingabeparameter für typische Anwendungsfälle.

  - Port
  - Aufgabengröße

- Image
- Gewünschte Anzahl
- Docker-Datei
- Einheitentestbefehl

Sie geben Werte für Eingabeparameter an, wenn Sie einen Service erstellen:

- Verwenden Sie die -Konsole, um ein schemabasiertes Formular auszufüllen, das AWS Proton bereitstellt.
- Verwenden Sie die CLI, um eine Spezifikation bereitzustellen, die die Werte enthält.

- Ausgabeparameter – Definieren Sie Service-Instance-Ausgaben in Ihren Service-IaC-Dateien. Sie können dann in IaC-Dateien anderer Ressourcen auf diese Ausgaben verweisen.

Lesen von Parameterwerten in Service-IaC-Dateien

Sie können Parameter im Zusammenhang mit dem Service und anderen Ressourcen in Service-IaC-Dateien lesen. Sie lesen einen Parameterwert, indem Sie im AWS Proton Parameter-Namespace auf den Namen des Parameters verweisen.

- Eingabeparameter – Lesen Sie einen Service-Instance-Eingabewert, indem Sie auf verweisen`service_instance.inputs.`*`input-name`*.
- Ressourcenparameter – Lesen Sie AWS Proton Ressourcenparameter`service_instance.name`, indem Sie auf Namen wie `service.name`, und verweisen`environment.name`.
- Ausgabeparameter – Lesen Sie Ausgaben anderer Ressourcen, indem Sie auf `environment.outputs.`*`output-name`* oder verweisen`service_instance.components.default.outputs.`*`output-name`*.

Beispiel für eine ServiceIaC-Datei mit Parametern

Das folgende Beispiel ist ein Ausschnitt aus einer CloudFormation IaC-Datei. Der `environment.outputs.` Namespace bezieht sich auf Ausgaben aus der IaC-Datei der Umgebung. Der `service_instance.inputs.` Namespace bezieht sich auf Eingabeparameter der Service-Instance. Die -`service_instance.name`Eigenschaft bezieht sich auf einen - AWS Proton Ressourcenparameter.

```
Resources:
  StoreServiceInstanceInputValue:
    Type: AWS::SSM::Parameter
    Properties:
      Type: String
      Value: "{{ service.name }} {{ service_instance.name }}
 {{ service_instance.inputs.my_sample_service_instance_required_input }}
 {{ service_instance.inputs.my_sample_service_instance_optional_input }}
 {{ environment.outputs.MySampleInputValue }}
 {{ environment.outputs.MyOtherSampleInputValue }}"
              #  resource parameter references               # input parameter
 references
                                          # output references to an environment
 infrastructure as code file
Outputs:
  MyServiceInstanceParameter:                                                  #
 output definition
    Value: !Ref StoreServiceInstanceInputValue
  MyServiceInstanceRequiredInputValue:                                         #
 output definition
    Value: "{{ service_instance.inputs.my_sample_service_instance_required_input }}"  #
 input parameter reference
  MyServiceInstanceOptionalInputValue:                                         #
 output definition
    Value: "{{ service_instance.inputs.my_sample_service_instance_optional_input }}"  #
 input parameter reference
  MyServiceInstancesEnvironmentSampleOutputValue:                              #
 output definition
    Value: "{{ environment.outputs.MySampleInputValue }}"                      #
 output reference to an environment IaC file
  MyServiceInstancesEnvironmentOtherSampleOutputValue:                         #
 output definition
    Value: "{{ environment.outputs.MyOtherSampleInputValue }}"                 #
 output reference to an environment IaC file
```

Details und Beispiele für Komponenten- CloudFormation IaC-Dateiparameter

Sie können Parameter in Ihrer Komponenteninfrastruktur als Codedateien (IaC) definieren und referenzieren. Eine detaillierte Beschreibung der AWS Proton Parameter, Parametertypen, des Parameter-Namespace und der Verwendung von Parametern in Ihren IaC-Dateien finden Sie

unter the section called “Parameter”. Weitere Informationen zu -Komponenten finden Sie unter Komponenten.

Definieren von Komponentenausgabeparametern

Sie können Ausgabeparameter in Ihren IaC-Komponentendateien definieren. Sie können dann in Service-IaC-Dateien auf diese Ausgaben verweisen.

> **Note**
>
> Sie können keine Eingaben für Komponenten-IaC-Dateien definieren. Angefügte Komponenten können Eingaben von der Service-Instance abrufen, an die sie angehängt sind. Trennte Komponenten haben keine Eingaben.

Lesen von Parameterwerten in Komponenten-IaC-Dateien

Sie können Parameter im Zusammenhang mit der Komponente und anderen Ressourcen in Komponenten-IaC-Dateien lesen. Sie lesen einen Parameterwert, indem Sie im AWS Proton Parameter-Namespace auf den Namen des Parameters verweisen.

- Eingabeparameter – Lesen Sie einen angehängten Service-Instance-Eingabewert, indem Sie auf verweisen`service_instance.inputs.`*`input-name`*.
- Ressourcenparameter – Lesen Sie AWS Proton Ressourcenparameter, indem Sie auf Namen wie `component.name`, `service.name`service_instance.name, und verweisen`environment.name`.
- Ausgabeparameter – Lesen Sie Umgebungsausgaben, indem Sie auf verweisen`environment.outputs.`*`output-name`*.

Beispiel für Komponenten- und ServiceIaC-Dateien mit Parametern

Das folgende Beispiel zeigt eine Komponente, die einen Amazon Simple Storage Service (Amazon S3)-Bucket und eine zugehörige Zugriffsrichtlinie bereitstellt und die Amazon-Ressourcennamen (ARNs) beider Ressourcen als Komponentenausgaben bereitstellt. Eine ServiceIaC-Vorlage fügt die Komponentenausgaben als Containerumgebungsvariablen einer Amazon Elastic Container Service (Amazon ECS)-Aufgabe hinzu, um die Ausgaben für Code verfügbar zu machen, der im Container ausgeführt wird, und fügt die Bucket-Zugriffsrichtlinie zur Rolle der Aufgabe hinzu. Der Bucket-Name basiert auf den Namen der Umgebung, des Services, der Service-Instance und der Komponente,

was bedeutet, dass der Bucket mit einer bestimmten Instance der Komponentenvorlage gekoppelt ist, die eine bestimmte Service-Instance erweitert. Entwickler können mehrere benutzerdefinierte Komponenten basierend auf dieser Komponentenvorlage erstellen, um Amazon S3-Buckets für verschiedene Service-Instances und funktionale Anforderungen bereitzustellen.

Das Beispiel zeigt, wie Sie die Jinja`{{ ... }}`-Syntax verwenden, um auf Komponenten- und andere Ressourcenparameter in Ihrer IaC-Datei zu verweisen. Sie können -`{% if ... %}`Anweisungen verwenden, um Blöcke von Anweisungen nur hinzuzufügen, wenn eine Komponente an die Service-Instance angefügt ist. Die `proton_cfn_*` Schlüsselwörter sind Filter, mit denen Sie Ausgabeparameterwerte bereinigen und formatieren können. Weitere Informationen zu Filtern finden Sie unter the section called “CloudFormation Parameterfilter”.

Als Administrator erstellen Sie die IaC-Vorlagendatei.

Example -Service CloudFormation IaC-Datei mit einer Komponente

```
# service/instance_infrastructure/cloudformation.yaml

Resources:
  TaskDefinition:
    Type: AWS::ECS::TaskDefinition
    Properties:
      TaskRoleArn: !Ref TaskRole
      ContainerDefinitions:
        - Name: '{{service_instance.name}}'
          # ...
          {% if service_instance.components.default.outputs | length > 0 %}
          Environment:
            {{ service_instance.components.default.outputs |
                proton_cfn_ecs_task_definition_formatted_env_vars }}
          {% endif %}

  # ...

  TaskRole:
    Type: AWS::IAM::Role
    Properties:
      # ...
      ManagedPolicyArns:
        - !Ref BaseTaskRoleManagedPolicy
        {{ service_instance.components.default.outputs
            | proton_cfn_iam_policy_arns }}
```

```
  # Basic permissions for the task
  BaseTaskRoleManagedPolicy:
    Type: AWS::IAM::ManagedPolicy
    Properties:
      # ...
```

Als Entwickler erstellen Sie die IaC-Vorlagendatei der Komponente.

Example CloudFormation IaC-Komponentendatei

```
# cloudformation.yaml

# A component that defines an S3 bucket and a policy for accessing the bucket.
Resources:
  S3Bucket:
    Type: 'AWS::S3::Bucket'
    Properties:
      BucketName: '{{environment.name}}-{{service.name}}-{{service_instance.name}}-
{{component.name}}'
  S3BucketAccessPolicy:
    Type: AWS::IAM::ManagedPolicy
    Properties:
      PolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Action:
              - 's3:Get*'
              - 's3:List*'
              - 's3:PutObject'
            Resource: !GetAtt S3Bucket.Arn
Outputs:
  BucketName:
    Description: "Bucket to access"
    Value: !GetAtt S3Bucket.Arn
  BucketAccessPolicyArn:
    Value: !Ref S3BucketAccessPolicy
```

Wenn eine - AWS CloudFormation Vorlage für Ihre Service-Instance AWS Proton wiedergibt und alle Parameter durch tatsächliche Werte ersetzt, könnte die Vorlage wie die folgende Datei aussehen.

Example -Service-Instance CloudFormation gerenderte IaC-Datei

```
Resources:
  TaskDefinition:
    Type: AWS::ECS::TaskDefinition
    Properties:
      TaskRoleArn: !Ref TaskRole
      ContainerDefinitions:
        - Name: '{{service_instance.name}}'
          # ...
          Environment:
            - Name: BucketName
              Value: arn:aws:s3:us-
east-1:123456789012:environment_name-service_name-service_instance_name-component_name
            - Name: BucketAccessPolicyArn
              Value: arn:aws:iam::123456789012:policy/cfn-generated-policy-name
  # ...

  TaskRole:
    Type: AWS::IAM::Role
    Properties:
      # ...
      ManagedPolicyArns:
        - !Ref BaseTaskRoleManagedPolicy
        - arn:aws:iam::123456789012:policy/cfn-generated-policy-name

  # Basic permissions for the task
  BaseTaskRoleManagedPolicy:
    Type: AWS::IAM::ManagedPolicy
    Properties:
      # ...
```

Parameterfilter für CloudFormation IaC-Dateien

Wenn Sie Verweise auf AWS Proton Parameter in Ihren AWS CloudFormation IaC-Dateien vornehmen, können Sie Jinja-Modifikatoren verwenden, die als Filter bezeichnet werden, um Parameterwerte zu validieren, zu filtern und zu formatieren, bevor sie in die gerenderte Vorlage eingefügt werden. Filtervalidierungen sind besonders nützlich, wenn sie auf Komponentenausgabeparameter verweisen, da die Erstellung und Anfügung von Komponenten von Entwicklern durchgeführt werden und ein Administrator, der Komponentenausgaben in einer Service-Instance-Vorlage verwendet, möglicherweise überprüfen möchte, ob sie vorhanden und gültig sind. Sie können jedoch Filter in jeder Jinja-IaC-Datei verwenden.

In den folgenden Abschnitten werden die verfügbaren Parameterfilter beschrieben und definiert und Beispiele bereitgestellt. AWS Proton definiert die meisten dieser Filter. Der `default` Filter ist ein integrierter Jinja-Filter.

Formatieren von Umgebungseigenschaften für Amazon-ECS-Aufgaben

Deklaration

```
dict # proton_cfn_ecs_task_definition_formatted_env_vars (raw: boolean = True) # YAML
 list of dicts
```

Beschreibung

Dieser Filter formatiert eine Liste von Ausgaben, die in einer Umgebungseigenschaft im -`ContainerDefinition`Abschnitt einer Amazon Elastic Container Service (Amazon ECS)-Aufgabendefinition verwendet werden sollen.

Setzen Sie diesen Wert `raw` auf `False`, um auch den Parameterwert zu validieren. In diesem Fall muss der Wert mit dem regulären Ausdruck übereinstimmen`^[a-zA-Z0-9_-]*$`. Wenn der Wert diese Validierung nicht besteht, schlägt das Rendern der Vorlage fehl.

Beispiel

Mit der folgenden benutzerdefinierten Komponentenvorlage:

```
Resources:
  # ...
Outputs:
  Output1:
    Description: "Example component output 1"
    Value: hello
  Output2:
    Description: "Example component output 2"
    Value: world
```

Und die folgende Servicevorlage:

```
Resources:
  TaskDefinition:
    Type: AWS::ECS::TaskDefinition
    Properties:
```

```
      # ...
      ContainerDefinitions:
        - Name: MyServiceName
          # ...
          Environment:
            {{ service_instance.components.default.outputs
              | proton_cfn_ecs_task_definition_formatted_env_vars }}
```

Die gerenderte Servicevorlage lautet wie folgt:

```
Resources:
  TaskDefinition:
    Type: AWS::ECS::TaskDefinition
    Properties:
      # ...
      ContainerDefinitions:
        - Name: MyServiceName
          # ...
          Environment:
            - Name: Output1
              Value: hello
            - Name: Output2
              Value: world
```

Formatieren von Umgebungseigenschaften für Lambda-Funktionen

Deklaration

```
dict # proton_cfn_lambda_function_formatted_env_vars (raw: boolean = True) # YAML dict
```

Beschreibung

Dieser Filter formatiert eine Liste von Ausgaben, die in einer Umgebungseigenschaft im -`Properties`Abschnitt einer - AWS Lambda Funktionsdefinition verwendet werden sollen.

Setzen Sie diesen Wert `raw` auf `False`, um auch den Parameterwert zu validieren. In diesem Fall muss der Wert mit dem regulären Ausdruck übereinstimmen`^[a-zA-Z0-9_-]*$`. Wenn der Wert diese Validierung nicht besteht, schlägt das Rendern der Vorlage fehl.

Beispiel

Mit der folgenden benutzerdefinierten Komponentenvorlage:

```
Resources:
  # ...
Outputs:
  Output1:
    Description: "Example component output 1"
    Value: hello
  Output2:
    Description: "Example component output 2"
    Value: world
```

Und die folgende Servicevorlage:

```
Resources:
  Lambda:
    Type: AWS::Lambda::Function
    Properties:
      Environment:
        Variables:
          {{ service_instance.components.default.outputs
            | proton_cfn_lambda_function_formatted_env_vars }}
```

Die gerenderte Servicevorlage lautet wie folgt:

```
Resources:
  Lambda:
    Type: AWS::Lambda::Function
    Properties:
      Environment:
        Variables:
          Output1: hello
          Output2: world
```

Extrahieren von IAM-Richtlinien-ARNs, die in IAM-Rollen aufgenommen werden sollen

Deklaration

```
dict # proton_cfn_iam_policy_arns # YAML list
```

Beschreibung

Dieser Filter formatiert eine Liste von Ausgaben, die in einer ManagedPolicyArns Eigenschaft im -`Properties`Abschnitt einer AWS Identity and Access Management (IAM)-Rollendefinition verwendet werden sollen. Der Filter verwendet den regulären Ausdruck`^arn:[a-zA-Z-]+:iam::\d{12}:policy/`, um gültige IAM-Richtlinien-ARNs aus der Liste der Ausgabeparameter zu extrahieren. Sie können diesen Filter verwenden, um Richtlinien in Ausgabeparameterwerten an eine IAM-Rollendefinition in einer Servicevorlage anzuhängen.

Beispiel

Mit der folgenden benutzerdefinierten Komponentenvorlage:

```
Resources:
  # ...
  ExamplePolicy1:
    Type: AWS::IAM::ManagedPolicy
    Properties:
      # ...
  ExamplePolicy2:
    Type: AWS::IAM::ManagedPolicy
    Properties:
      # ...

  # ...

Outputs:
  Output1:
    Description: "Example component output 1"
    Value: hello
  Output2:
    Description: "Example component output 2"
    Value: world
  PolicyArn1:
    Description: "ARN of policy 1"
    Value: !Ref ExamplePolicy1
  PolicyArn2:
    Description: "ARN of policy 2"
    Value: !Ref ExamplePolicy2
```

Und die folgende Servicevorlage:

```
Resources:
```

```
  # ...

  TaskRole:
    Type: AWS::IAM::Role
    Properties:
      # ...
      ManagedPolicyArns:
        - !Ref BaseTaskRoleManagedPolicy
        {{ service_instance.components.default.outputs
            | proton_cfn_iam_policy_arns }}

  # Basic permissions for the task
  BaseTaskRoleManagedPolicy:
    Type: AWS::IAM::ManagedPolicy
    Properties:
      # ...
```

Die gerenderte Servicevorlage lautet wie folgt:

```
Resources:

  # ...

  TaskRole:
    Type: AWS::IAM::Role
    Properties:
      # ...
      ManagedPolicyArns:
        - !Ref BaseTaskRoleManagedPolicy
        - arn:aws:iam::123456789012:policy/cfn-generated-policy-name-1
        - arn:aws:iam::123456789012:policy/cfn-generated-policy-name-2

  # Basic permissions for the task
  BaseTaskRoleManagedPolicy:
    Type: AWS::IAM::ManagedPolicy
    Properties:
      # ...
```

Eigenschaftswerte bereinigen

Deklaration

```
string # proton_cfn_sanitize # string
```

Beschreibung

Dies ist ein Allzweckfilter. Verwenden Sie sie, um die Sicherheit eines Parameterwerts zu überprüfen. Der Filter überprüft, ob der Wert entweder mit dem regulären Ausdruck übereinstimmt `^[a-zA-Z0-9_-]*$` oder ein gültiger Amazon-Ressourcenname (ARN) ist. Wenn der Wert diese Validierung nicht besteht, schlägt das Rendern der Vorlage fehl.

Beispiel

Mit der folgenden benutzerdefinierten Komponentenvorlage:

```
Resources:
  # ...
Outputs:
  Output1:
    Description: "Example of valid output"
    Value: "This-is_valid_37"
  Output2:
    Description: "Example incorrect output"
    Value: "this::is::incorrect"
  SomeArn:
    Description: "Example ARN"
    Value: arn:aws:some-service::123456789012:some-resource/resource-name
```

- Die folgende Referenz in einer Servicevorlage:

  ```
  # ...
    {{ service_instance.components.default.outputs.Output1
      | proton_cfn_sanitize }}
  ```

  Rendern Sie wie folgt:

  ```
  # ...
    This-is_valid_37
  ```

- Die folgende Referenz in einer Servicevorlage:

  ```
  # ...
    {{ service_instance.components.default.outputs.Output2
  ```

```
    | proton_cfn_sanitize }}
```

Ergebnisse mit dem folgenden Rendering-Fehler:

```
Illegal character(s) detected in "this::is::incorrect". Must match regex ^[a-zA-
Z0-9_-]*$ or be a valid ARN
```

- Die folgende Referenz in einer Servicevorlage:

```
# ...
  {{ service_instance.components.default.outputs.SomeArn
    | proton_cfn_sanitize }}
```

Rendern Sie wie folgt:

```
# ...
  arn:aws:some-service::123456789012:some-resource/resource-name
```

Geben Sie Standardwerte für nicht vorhandene Referenzen an

Beschreibung

Der `default` Filter stellt einen Standardwert bereit, wenn keine Namespace-Referenz vorhanden ist. Verwenden Sie sie, um robuste Vorlagen zu schreiben, die ohne Fehler rendern können, auch wenn der Parameter, auf den Sie verweisen, fehlt.

Beispiel

Die folgende Referenz in einer Servicevorlage führt dazu, dass das Rendern von Vorlagen fehlschlägt, wenn der Service-Instance keine direkt definierte (Standard-)Komponente angefügt ist oder wenn die angefügte Komponente keine Ausgabe mit dem Namen hat`test`.

```
# ...
  {{ service_instance.components.default.outputs.test }}
```

Um dieses Problem zu vermeiden, fügen Sie den `default` Filter hinzu.

```
# ...
  {{ service_instance.components.default.outputs.test | default("[optional-value]") }}
```

CodeBuild Details und Beispiele für Bereitstellungsparameter

Sie können Parameter in Ihren Vorlagen für CodeBuild-basierte AWS Proton Ressourcen definieren und diese Parameter in Ihrem Bereitstellungscode referenzieren. Eine detaillierte Beschreibung der AWS Proton Parameter, Parametertypen, des Parameter-Namespace und der Verwendung von Parametern in Ihren IaC-Dateien finden Sie unter the section called “Parameter”.

> **Note**
>
> Sie können die CodeBuild Bereitstellung mit Umgebungen und Services verwenden. Derzeit können Sie Komponenten nicht auf diese Weise bereitstellen.

Eingabeparameter

Wenn Sie eine - AWS Proton Ressource erstellen, z. B. eine Umgebung oder einen Service, geben Sie Werte für Eingabeparameter an, die in der Schemadatei Ihrer Vorlage definiert sind. Wenn die von Ihnen erstellte Ressource verwendetCodeBuildBereitstellung, AWS Proton stellt diese Eingabewerte in einer Eingabedatei wieder her. Ihr Bereitstellungscode kann Parameterwerte aus dieser Datei importieren und abrufen.

Ein Beispiel für eine - CodeBuild Vorlage finden Sie unter the section called “CodeBuild -Paket”. Weitere Informationen zu Manifestdateien finden Sie unter the section called “Manifest und Wrapup”.

Das folgende Beispiel ist eine JSON-Eingabedatei, die während der CodeBuild-basierten Bereitstellung einer Service-Instance generiert wurde.

Beispiel: Verwenden der AWS CDK mit CodeBuild Bereitstellung

```
{
  "service_instance": {
    "name": "my-service-staging",
    "inputs": {
      "port": "8080",
      "task_size": "medium"
    }
  },
  "service": {
    "name": "my-service"
  },
```

```
  "environment": {
    "account_id": "123456789012",
    "name": "my-env-staging",
    "outputs": {
      "vpc-id": "hdh2323423"
    }
  }
}
```

Ausgabeparameter

Um Ausgaben für die Ressourcenbereitstellung zurück an zu übermitteln AWS Proton, kann Ihr Bereitstellungscode eine JSON-Datei `proton-outputs.json` mit dem Namen und Werten für Ausgabeparameter generieren, die in der Schemadatei Ihrer Vorlage definiert sind. Der `cdk deploy` Befehl hat beispielsweise das Argument `--outputs-file` , das anweist, eine JSON-Datei mit Bereitstellungsausgaben AWS CDK zu generieren. Wenn Ihre Ressource die verwendet AWS CDK, geben Sie den folgenden Befehl in Ihrem CodeBuild Vorlagenmanifest an:

```
aws proton notify-resource-deployment-status-change
```

AWS Proton sucht nach dieser JSON-Datei. Wenn die Datei vorhanden ist, nachdem Ihr Bereitstellungscode erfolgreich abgeschlossen wurde, AWS Proton liest die Ausgabeparameterwerte aus ihr.

Details und Beispiele für Terraform Infrastructure as Code (IaC)-Dateiparameter

Sie können Terraform-Eingabevariablen in `variable.tf` Dateien in Ihr Vorlagenpaket aufnehmen. Sie können auch ein Schema erstellen, um verwaltete Variablen zu erstellen AWS Proton . AWS Proton erstellt Variablen `.tf files` aus Ihrer Schemadatei. Weitere Informationen finden Sie unter the section called “Terraform-IaC-Dateien”.

Um auf Ihre schemadefinierten AWS Proton Variablen in Ihrer Infrastruktur zu verweisen`.tf files`, verwenden Sie die AWS Proton Namespaces, die in der Tabelle Parameter und Namespaces für Terraform IaC angezeigt werden. Sie können beispielsweise die Datei `var.environment.inputs.vpc_cidr` verwenden. Setzen Sie diese Variablen in Anführungszeichen in einzelne Klammern und fügen Sie ein Dollarzeichen vor der ersten Klammer hinzu (z. B. “`${var.environment.inputs.vpc_cidr}`”).

Das folgende Beispiel zeigt, wie Sie Namespaces verwenden, um AWS Proton Parameter in eine Umgebung aufzunehmen `.tf file`.

```
terraform {
  required_providers {
    aws = {
      source  = "hashicorp/aws"
      version = "~> 3.0"
    }
  }
  // This tells terraform to store the state file in s3 at the location
  // s3://terraform-state-bucket/tf-os-sample/terraform.tfstate
  backend "s3" {
    bucket = "terraform-state-bucket"
    key    = "tf-os-sample/terraform.tfstate"
    region = "us-east-1"
  }
}

// Configure the AWS Provider
provider "aws" {
  region = "us-east-1"
  default_tags {
    tags = var.proton_tags
  }
}

resource "aws_ssm_parameter" "my_ssm_parameter" {
  name  = "my_ssm_parameter"
  type  = "String"
  // Use the Proton environment.inputs. namespace
  value = var.environment.inputs.ssm_parameter_value
}
```

AWS Proton Infrastructure as Code-Dateien

Die Hauptbestandteile des Vorlagenpakets sind Infrastructure as Code (IaC)-Dateien, die die Infrastrukturressourcen und Eigenschaften definieren, die Sie bereitstellen möchten. AWS CloudFormation und andere Infrastrukturen als Code-Engines verwenden diese Arten von Dateien zur Bereitstellung von Infrastrukturressourcen.

> **Note**
>
> Eine IaC-Datei kann auch unabhängig von Vorlagenpaketen als direkte Eingabe für direkt definierte Komponenten verwendet werden. Weitere Informationen zu Komponenten finden Sie unter Komponenten.

AWS Proton unterstützt derzeit zwei Arten von IaC-Dateien:

- -CloudFormationDateien – Wird für die von verwaltete Bereitstellung verwendet. AWS Proton verwendet Jinja zusätzlich zum CloudFormation Vorlagendateiformat für die Parametrisierung. AWS
- Terraform-HCL-Dateien – Wird für die selbstverwaltete Bereitstellung von verwendet. HCL unterstützt nativ die Parametrisierung.

Sie können AWS Proton Ressourcen nicht mit einer Kombination von Bereitstellungsmethoden bereitstellen. Sie müssen die eine oder andere verwenden. Sie können einen AWS von verwalteten Bereitstellungsservice nicht in einer selbstverwalteten Bereitstellungsumgebung oder umgekehrt bereitstellen.

Weitere Informationen dazu finden Sie unter the section called “Methoden der Provisioned”, Umgebungen, Dienstleistungen und Komponenten.

AWS CloudFormation IaC-Dateien

Erfahren Sie, wie Sie AWS CloudFormation Infrastruktur als Codedateien mit verwenden AWS Proton. AWS CloudFormation ist ein Infrastructure as Code (IaC)-Service, der Sie bei der Modellierung und Einrichtung Ihrer - AWS Ressourcen unterstützt. Sie definieren Ihre Infrastrukturressourcen in Vorlagen und verwenden Jinja zusätzlich zum CloudFormation Vorlagendateiformat für parametrization. AWS Proton expands-Parameter und rendert die vollständige CloudFormation Vorlage. CloudFormation stellt die definierten Ressourcen als CloudFormation Stack bereit. Weitere Informationen finden Sie unter Was ist AWS CloudFormation im AWS CloudFormation -Benutzerhandbuch.

AWS Proton unterstützt die von AWS verwaltete Bereitstellung für CloudFormation IaC .

Beginnen Sie mit Ihrer eigenen vorhandenen Infrastruktur als Codedateien

Sie können Ihre eigenen vorhandenen Infrastructure as Code (IaC)-Dateien für die Verwendung mit anpassen AWS Proton.

Die folgenden AWS CloudFormation Beispiele, Beispiel 1 und Beispiel 2, stellen Ihre eigenen vorhandenen CloudFormation IaC-Dateien dar. CloudFormation kann diese Dateien verwenden, um zwei verschiedene CloudFormation Stacks zu erstellen.

In Beispiel 1 ist die CloudFormation IaC-Datei so konfiguriert, dass sie Infrastruktur bereitstellt, die von Container-Anwendungen gemeinsam genutzt werden kann. In diesem Beispiel werden Eingabeparameter hinzugefügt, sodass Sie dieselbe IaC-Datei verwenden können, um mehrere Sätze bereitgestellter Infrastruktur zu erstellen. Jeder Satz kann unterschiedliche Namen zusammen mit einem anderen Satz von VPC- und Subnetz-CIDR-Werten haben. Als Administrator oder Entwickler geben Sie Werte für diese Parameter an, wenn Sie eine IaC-Datei verwenden, um Infrastrukturressourcen mit bereitzustellen CloudFormation. Der Einfachheit halber werden diese Eingabeparameter im Beispiel mit Kommentaren markiert und mehrmals referenziert. Die Ausgaben werden am Ende der Vorlage definiert. Sie können in anderen CloudFormation IaC-Dateien referenziert werden.

In Beispiel 2 ist die CloudFormation IaC-Datei so konfiguriert, dass eine Anwendung in der Infrastruktur bereitgestellt wird, die aus Beispiel 1 bereitgestellt wird. Die Parameter werden zu Ihrer Bequemlichkeit kommentiert.

Beispiel 1: CloudFormation IaC-Datei

```
AWSTemplateFormatVersion: '2010-09-09'
Description: AWS Fargate cluster running containers in a public subnet. Only supports
             public facing load balancer, and public service discovery namespaces.
Parameters:
   VpcCIDR:       # input parameter
        Description: CIDR for VPC
        Type: String
        Default: "10.0.0.0/16"
   SubnetOneCIDR: # input parameter
        Description: CIDR for SubnetOne
        Type: String
        Default: "10.0.0.0/24"
   SubnetTwoCIDR: # input parameters
        Description: CIDR for SubnetTwo
        Type: String
```

```
        Default: "10.0.1.0/24"
Resources:
  VPC:
    Type: AWS::EC2::VPC
    Properties:
      EnableDnsSupport: true
      EnableDnsHostnames: true
      CidrBlock:
        Ref: 'VpcCIDR'

  # Two public subnets, where containers will have public IP addresses
  PublicSubnetOne:
    Type: AWS::EC2::Subnet
    Properties:
      AvailabilityZone:
         Fn::Select:
         - 0
         - Fn::GetAZs: {Ref: 'AWS::Region'}
      VpcId: !Ref 'VPC'
      CidrBlock:
         Ref: 'SubnetOneCIDR'
      MapPublicIpOnLaunch: true

  PublicSubnetTwo:
    Type: AWS::EC2::Subnet
    Properties:
      AvailabilityZone:
         Fn::Select:
         - 1
         - Fn::GetAZs: {Ref: 'AWS::Region'}
      VpcId: !Ref 'VPC'
      CidrBlock:
        Ref: 'SubnetTwoCIDR'
      MapPublicIpOnLaunch: true

  # Setup networking resources for the public subnets. Containers
  # in the public subnets have public IP addresses and the routing table
  # sends network traffic via the internet gateway.
  InternetGateway:
    Type: AWS::EC2::InternetGateway
  GatewayAttachement:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      VpcId: !Ref 'VPC'
```

```
      InternetGatewayId: !Ref 'InternetGateway'
  PublicRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref 'VPC'
  PublicRoute:
    Type: AWS::EC2::Route
    DependsOn: GatewayAttachement
    Properties:
      RouteTableId: !Ref 'PublicRouteTable'
      DestinationCidrBlock: '0.0.0.0/0'
      GatewayId: !Ref 'InternetGateway'
  PublicSubnetOneRouteTableAssociation:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      SubnetId: !Ref PublicSubnetOne
      RouteTableId: !Ref PublicRouteTable
  PublicSubnetTwoRouteTableAssociation:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      SubnetId: !Ref PublicSubnetTwo
      RouteTableId: !Ref PublicRouteTable

  # ECS Resources
  ECSCluster:
    Type: AWS::ECS::Cluster

  # A security group for the containers we will run in Fargate.
  # Rules are added to this security group based on what ingress you
  # add for the cluster.
  ContainerSecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: Access to the Fargate containers
      VpcId: !Ref 'VPC'

  # This is a role which is used by the ECS tasks themselves.
  ECSTaskExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Statement:
        - Effect: Allow
          Principal:
```

```
            Service: [ecs-tasks.amazonaws.com]
          Action: ['sts:AssumeRole']
      Path: /
      ManagedPolicyArns:
        - 'arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy'

# These output values will be available to other templates to use.
Outputs:
  ClusterName:                                          # output
    Description: The name of the ECS cluster
    Value: !Ref 'ECSCluster'
    Export:
      Name:
        Fn::Sub: "${AWS::StackName}-ECSCluster"
  ECSTaskExecutionRole:                                  # output
    Description: The ARN of the ECS role
    Value: !GetAtt 'ECSTaskExecutionRole.Arn'
    Export:
      Name:
        Fn::Sub: "${AWS::StackName}-ECSTaskExecutionRole"
  VpcId:                                                 # output
    Description: The ID of the VPC that this stack is deployed in
    Value: !Ref 'VPC'
    Export:
      Name:
        Fn::Sub: "${AWS::StackName}-VPC"
  PublicSubnetOne:                                       # output
    Description: Public subnet one
    Value: !Ref 'PublicSubnetOne'
    Export:
      Name:
        Fn::Sub: "${AWS::StackName}-PublicSubnetOne"
  PublicSubnetTwo:                                       # output
    Description: Public subnet two
    Value: !Ref 'PublicSubnetTwo'
    Export:
      Name:
        Fn::Sub: "${AWS::StackName}-PublicSubnetTwo"
  ContainerSecurityGroup:                                # output
    Description: A security group used to allow Fargate containers to receive traffic
    Value: !Ref 'ContainerSecurityGroup'
    Export:
      Name:
```

```
        Fn::Sub: "${AWS::StackName}-ContainerSecurityGroup"
```

Beispiel 2: CloudFormation IaC-Datei

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Deploy a service on AWS Fargate, hosted in a public subnet, and accessible
 via a public load balancer.
Parameters:
    ContainerPortInput:  # input parameter
        Description: The port to route traffic to
        Type: Number
        Default: 80
    TaskCountInput:      # input parameter
        Description: The default number of Fargate tasks you want running
        Type: Number
        Default: 1
    TaskSizeInput:       # input parameter
        Description: The size of the task you want to run
        Type: String
        Default: x-small
    ContainerImageInput: # input parameter
        Description: The name/url of the container image
        Type: String
        Default: "public.ecr.aws/z9d2n7e1/nginx:1.19.5"
    TaskNameInput:       # input parameter
        Description: Name for your task
        Type: String
        Default: "my-fargate-instance"
    StackName:           # input parameter
        Description: Name of the environment stack to deploy to
        Type: String
        Default: "my-fargate-environment"
Mappings:
  TaskSizeMap:
    x-small:
      cpu: 256
      memory: 512
    small:
      cpu: 512
      memory: 1024
    medium:
      cpu: 1024
      memory: 2048
```

```
    large:
      cpu: 2048
      memory: 4096
    x-large:
      cpu: 4096
      memory: 8192
Resources:
  # A log group for storing the stdout logs from this service's containers
  LogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName:
        Ref: 'TaskNameInput' # input parameter

  # The task definition. This is a simple metadata description of what
  # container to run, and what resource requirements it has.
  TaskDefinition:
    Type: AWS::ECS::TaskDefinition
    Properties:
      Family: !Ref 'TaskNameInput'
      Cpu: !FindInMap [TaskSizeMap, !Ref 'TaskSizeInput', cpu]
      Memory: !FindInMap [TaskSizeMap, !Ref 'TaskSizeInput', memory]
      NetworkMode: awsvpc
      RequiresCompatibilities:
        - FARGATE
      ExecutionRoleArn:
        Fn::ImportValue:
          !Sub "${StackName}-ECSTaskExecutionRole"    # output parameter from another
 CloudFormation template
              awslogs-region: !Ref 'AWS::Region'
              awslogs-stream-prefix: !Ref 'TaskNameInput'


  # The service_instance. The service is a resource which allows you to run multiple
  # copies of a type of task, and gather up their logs and metrics, as well
  # as monitor the number of running tasks and replace any that have crashed
  Service:
    Type: AWS::ECS::Service
    DependsOn: LoadBalancerRule
    Properties:
      ServiceName: !Ref 'TaskNameInput'
      Cluster:
        Fn::ImportValue:
```

```
          !Sub "${StackName}-ECSCluster"  # output parameter from another
CloudFormation template
     LaunchType: FARGATE
     DeploymentConfiguration:
       MaximumPercent: 200
       MinimumHealthyPercent: 75
     DesiredCount: !Ref 'TaskCountInput'
     NetworkConfiguration:
       AwsvpcConfiguration:
         AssignPublicIp: ENABLED
         SecurityGroups:
           - Fn::ImportValue:
               !Sub "${StackName}-ContainerSecurityGroup"    # output parameter from
another CloudFormation template
         Subnets:
           - Fn::ImportValue:r CloudFormation template
     TaskRoleArn: !Ref "AWS::NoValue"
     ContainerDefinitions:
       - Name: !Ref 'TaskNameInput'
         Cpu: !FindInMap [TaskSizeMap, !Ref 'TaskSizeInput', cpu]
         Memory: !FindInMap [TaskSizeMap, !Ref 'TaskSizeInput', memory]
         Image: !Ref 'ContainerImageInput'             # input parameter
         PortMappings:
           - ContainerPort: !Ref 'ContainerPortInput'  # input parameter

         LogConfiguration:
           LogDriver: 'awslogs'
           Options:
             awslogs-group: !Ref 'TaskNameInput'
               !Sub "${StackName}-PublicSubnetOne"    # output parameter from another
CloudFormation template
           - Fn::ImportValue:
               !Sub "${StackName}-PublicSubnetTwo"    # output parameter from another
CloudFormation template
     TaskDefinition: !Ref 'TaskDefinition'
     LoadBalancers:
       - ContainerName: !Ref 'TaskNameInput'
         ContainerPort: !Ref 'ContainerPortInput'  # input parameter
         TargetGroupArn: !Ref 'TargetGroup'

 # A target group. This is used for keeping track of all the tasks, and
 # what IP addresses / port numbers they have. You can query it yourself,
 # to use the addresses yourself, but most often this target group is just
 # connected to an application load balancer, or network load balancer, so
```

```
  # it can automatically distribute traffic across all the targets.
  TargetGroup:
    Type: AWS::ElasticLoadBalancingV2::TargetGroup
    Properties:
      HealthCheckIntervalSeconds: 6
      HealthCheckPath: /
      HealthCheckProtocol: HTTP
      HealthCheckTimeoutSeconds: 5
      HealthyThresholdCount: 2
      TargetType: ip
      Name: !Ref 'TaskNameInput'
      Port: !Ref 'ContainerPortInput'
      Protocol: HTTP
      UnhealthyThresholdCount: 2
      VpcId:
        Fn::ImportValue:
          !Sub "${StackName}-VPC"    # output parameter from another CloudFormation
template

  # Create a rule on the load balancer for routing traffic to the target group
  LoadBalancerRule:
    Type: AWS::ElasticLoadBalancingV2::ListenerRule
    Properties:
      Actions:
        - TargetGroupArn: !Ref 'TargetGroup'
          Type: 'forward'
      Conditions:
        - Field: path-pattern
          Values:
            - '*'
      ListenerArn: !Ref PublicLoadBalancerListener
      Priority: 1

  # Enable autoscaling for this service
  ScalableTarget:
    Type: AWS::ApplicationAutoScaling::ScalableTarget
    DependsOn: Service
    Properties:
      ServiceNamespace: 'ecs'
      ScalableDimension: 'ecs:service:DesiredCount'
      ResourceId:
        Fn::Join:
          - '/'
          - - service
```

```
            - Fn::ImportValue:
                !Sub "${StackName}-ECSCluster"
            - !Ref 'TaskNameInput'
      MinCapacity: 1
      MaxCapacity: 10
      RoleARN: !Sub arn:aws:iam::${AWS::AccountId}:role/
aws-service-role/ecs.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_ECSService

  # Create scaling policies for the service
  ScaleDownPolicy:
    Type: AWS::ApplicationAutoScaling::ScalingPolicy
    DependsOn: ScalableTarget
    Properties:
      PolicyName:
        Fn::Join:
          - '/'
          - - scale
            - !Ref 'TaskNameInput'
            - down
      PolicyType: StepScaling
      ResourceId:
        Fn::Join:
          - '/'
          - - service
            - Fn::ImportValue:
                !Sub "${StackName}-ECSCluster"  # output parameter from another
 CloudFormation template
            - !Ref 'TaskNameInput'
      ScalableDimension: 'ecs:service:DesiredCount'
      ServiceNamespace: 'ecs'
      StepScalingPolicyConfiguration:
        AdjustmentType: 'ChangeInCapacity'
        StepAdjustments:
          - MetricIntervalUpperBound: 0
            ScalingAdjustment: -1
        MetricAggregationType: 'Average'
        Cooldown: 60

  ScaleUpPolicy:
    Type: AWS::ApplicationAutoScaling::ScalingPolicy
    DependsOn: ScalableTarget
    Properties:
      PolicyName:
```

```
        Fn::Join:
          - '/'
          - - scale
            - !Ref 'TaskNameInput'
            - up
      PolicyType: StepScaling
      ResourceId:
        Fn::Join:
          - '/'
          - - service
            - Fn::ImportValue:
                !Sub "${StackName}-ECSCluster"
            - !Ref 'TaskNameInput'
      ScalableDimension: 'ecs:service:DesiredCount'
      ServiceNamespace: 'ecs'
      StepScalingPolicyConfiguration:
        AdjustmentType: 'ChangeInCapacity'
        StepAdjustments:
          - MetricIntervalLowerBound: 0
            MetricIntervalUpperBound: 15
            ScalingAdjustment: 1
          - MetricIntervalLowerBound: 15
            MetricIntervalUpperBound: 25
            ScalingAdjustment: 2
          - MetricIntervalLowerBound: 25
            ScalingAdjustment: 3
        MetricAggregationType: 'Average'
        Cooldown: 60

  # Create alarms to trigger these policies
  LowCpuUsageAlarm:
    Type: AWS::CloudWatch::Alarm
    Properties:
      AlarmName:
        Fn::Join:
          - '-'
          - - low-cpu
            - !Ref 'TaskNameInput'
      AlarmDescription:
        Fn::Join:
          - ' '
          - - "Low CPU utilization for service"
            - !Ref 'TaskNameInput'
      MetricName: CPUUtilization
```

```
      Namespace: AWS/ECS
      Dimensions:
        - Name: ServiceName
          Value: !Ref 'TaskNameInput'
        - Name: ClusterName
          Value:
            Fn::ImportValue:
              !Sub "${StackName}-ECSCluster"
      Statistic: Average
      Period: 60
      EvaluationPeriods: 1
      Threshold: 20
      ComparisonOperator: LessThanOrEqualToThreshold
      AlarmActions:
        - !Ref ScaleDownPolicy

  HighCpuUsageAlarm:
    Type: AWS::CloudWatch::Alarm
    Properties:
      AlarmName:
        Fn::Join:
          - '-'
          - - high-cpu
            - !Ref 'TaskNameInput'
      AlarmDescription:
        Fn::Join:
          - ' '
          - - "High CPU utilization for service"
            - !Ref 'TaskNameInput'
      MetricName: CPUUtilization
      Namespace: AWS/ECS
      Dimensions:
        - Name: ServiceName
          Value: !Ref 'TaskNameInput'
        - Name: ClusterName
          Value:
            Fn::ImportValue:
              !Sub "${StackName}-ECSCluster"
      Statistic: Average
      Period: 60
      EvaluationPeriods: 1
      Threshold: 70
      ComparisonOperator: GreaterThanOrEqualToThreshold
      AlarmActions:
```

```
        - !Ref ScaleUpPolicy

  EcsSecurityGroupIngressFromPublicALB:
    Type: AWS::EC2::SecurityGroupIngress
    Properties:
      Description: Ingress from the public ALB
      GroupId:
        Fn::ImportValue:
          !Sub "${StackName}-ContainerSecurityGroup"
      IpProtocol: -1
      SourceSecurityGroupId: !Ref 'PublicLoadBalancerSG'

  # Public load balancer, hosted in public subnets that is accessible
  # to the public, and is intended to route traffic to one or more public
  # facing services. This is used for accepting traffic from the public
  # internet and directing it to public facing microservices
  PublicLoadBalancerSG:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: Access to the public facing load balancer
      VpcId:
        Fn::ImportValue:
          !Sub "${StackName}-VPC"
      SecurityGroupIngress:
          # Allow access to ALB from anywhere on the internet
          - CidrIp: 0.0.0.0/0
            IpProtocol: -1

  PublicLoadBalancer:
    Type: AWS::ElasticLoadBalancingV2::LoadBalancer
    Properties:
      Scheme: internet-facing
      LoadBalancerAttributes:
      - Key: idle_timeout.timeout_seconds
        Value: '30'
      Subnets:
        # The load balancer is placed into the public subnets, so that traffic
        # from the internet can reach the load balancer directly via the internet
gateway
        - Fn::ImportValue:
            !Sub "${StackName}-PublicSubnetOne"
        - Fn::ImportValue:
            !Sub "${StackName}-PublicSubnetTwo"
      SecurityGroups: [!Ref 'PublicLoadBalancerSG']
```

```
  PublicLoadBalancerListener:
    Type: AWS::ElasticLoadBalancingV2::Listener
    DependsOn:
      - PublicLoadBalancer
    Properties:
      DefaultActions:
        - TargetGroupArn: !Ref 'TargetGroup'
          Type: 'forward'
      LoadBalancerArn: !Ref 'PublicLoadBalancer'
      Port: 80
      Protocol: HTTP
# These output values will be available to other templates to use.
Outputs:
  ServiceEndpoint:        # output
    Description: The URL to access the service
    Value: !Sub "http://${PublicLoadBalancer.DNSName}"
```

Sie können diese Dateien für die Verwendung mit anpassen AWS Proton.

Bringen Sie Ihre Infrastruktur als Code in AWS Proton

Mit leichten Änderungen können Sie Beispiel 1 als Infrastructure as Code (IaC)-Datei für ein Umgebungsvorlagenpaket verwenden, das AWS Proton verwendet, um eine Umgebung bereitzustellen (wie in Beispiel 3 gezeigt).

Anstatt die CloudFormation Parameter zu verwenden, verwenden Sie die Jinja-Syntax, um Parameter zu referenzieren, die Sie in einer Open API-basierten Schemadatei definiert haben. ??? Diese Eingabeparameter werden zu Ihrer Bequemlichkeit kommentiert und in der IaC-Datei mehrfach referenziert. Auf diese Weise AWS Proton kann Parameterwerte prüfen und überprüfen. Es kann auch Ausgabeparameterwerte in einer IaC-Datei abgleichen und Parametern in einer anderen IaC-Datei hinzufügen.

Als Administrator können Sie den AWS Proton `environment.inputs.` Namespace zu den Eingabeparametern hinzufügen. Wenn Sie in einer Service-IaC-Datei auf Umgebungs-IaC-Dateiausgaben verweisen, können Sie den `environment.outputs.` Namespace zu den Ausgaben hinzufügen (z. B. `environment.outputs.ClusterName`). Zuletzt umgeben Sie sie mit geschweiften Klammern und Anführungszeichen.

Mit diesen Änderungen können Ihre CloudFormation IaC-Dateien von verwendet werden AWS Proton.

Beispiel 3: AWS Proton Umgebungsinfrastruktur als Codedatei

```
AWSTemplateFormatVersion: '2010-09-09'
Description: AWS Fargate cluster running containers in a public subnet. Only supports
             public facing load balancer, and public service discovery prefixes.
Mappings:
  # The VPC and subnet configuration is passed in via the environment spec.
  SubnetConfig:
    VPC:
      CIDR: '{{ environment.inputs.vpc_cidr}}'        # input parameter
    PublicOne:
      CIDR: '{{ environment.inputs.subnet_one_cidr}}' # input parameter
    PublicTwo:
      CIDR: '{{ environment.inputs.subnet_two_cidr}}' # input parameter
Resources:
  VPC:
    Type: AWS::EC2::VPC
    Properties:
      EnableDnsSupport: true
      EnableDnsHostnames: true
      CidrBlock: !FindInMap ['SubnetConfig', 'VPC', 'CIDR']

  # Two public subnets, where containers will have public IP addresses
  PublicSubnetOne:
    Type: AWS::EC2::Subnet
    Properties:
      AvailabilityZone:
         Fn::Select:
         - 0
         - Fn::GetAZs: {Ref: 'AWS::Region'}
      VpcId: !Ref 'VPC'
      CidrBlock: !FindInMap ['SubnetConfig', 'PublicOne', 'CIDR']
      MapPublicIpOnLaunch: true

  PublicSubnetTwo:
    Type: AWS::EC2::Subnet
    Properties:
      AvailabilityZone:
         Fn::Select:
         - 1
         - Fn::GetAZs: {Ref: 'AWS::Region'}
      VpcId: !Ref 'VPC'
      CidrBlock: !FindInMap ['SubnetConfig', 'PublicTwo', 'CIDR']
      MapPublicIpOnLaunch: true
```

```
  # Setup networking resources for the public subnets. Containers
  # in the public subnets have public IP addresses and the routing table
  # sends network traffic via the internet gateway.
  InternetGateway:
    Type: AWS::EC2::InternetGateway
  GatewayAttachement:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      VpcId: !Ref 'VPC'
      InternetGatewayId: !Ref 'InternetGateway'
  PublicRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref 'VPC'
  PublicRoute:
    Type: AWS::EC2::Route
    DependsOn: GatewayAttachement
    Properties:
      RouteTableId: !Ref 'PublicRouteTable'
      DestinationCidrBlock: '0.0.0.0/0'
      GatewayId: !Ref 'InternetGateway'
  PublicSubnetOneRouteTableAssociation:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      SubnetId: !Ref PublicSubnetOne
      RouteTableId: !Ref PublicRouteTable
  PublicSubnetTwoRouteTableAssociation:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      SubnetId: !Ref PublicSubnetTwo
      RouteTableId: !Ref PublicRouteTable

  # ECS Resources
  ECSCluster:
    Type: AWS::ECS::Cluster

  # A security group for the containers we will run in Fargate.
  # Rules are added to this security group based on what ingress you
  # add for the cluster.
  ContainerSecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: Access to the Fargate containers
```

```
      VpcId: !Ref 'VPC'

  # This is a role which is used by the ECS tasks themselves.
  ECSTaskExecutionRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Statement:
        - Effect: Allow
          Principal:
            Service: [ecs-tasks.amazonaws.com]
          Action: ['sts:AssumeRole']
      Path: /
      ManagedPolicyArns:
        - 'arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy'

# These output values are available to service infrastructure as code files as outputs,
 when given the
# the 'service_instance.environment.outputs.' namespace, for example,
 service_instance.environment.outputs.ClusterName.

Outputs:
  ClusterName:                                          # output
    Description: The name of the ECS cluster
    Value: !Ref 'ECSCluster'
  ECSTaskExecutionRole:                                 # output
    Description: The ARN of the ECS role
    Value: !GetAtt 'ECSTaskExecutionRole.Arn'
  VpcId:                                                # output
    Description: The ID of the VPC that this stack is deployed in
    Value: !Ref 'VPC'
  PublicSubnetOne:                                      # output
    Description: Public subnet one
    Value: !Ref 'PublicSubnetOne'
  PublicSubnetTwo:                                      # output
    Description: Public subnet two
    Value: !Ref 'PublicSubnetTwo'
  ContainerSecurityGroup:                               # output
    Description: A security group used to allow Fargate containers to receive traffic
    Value: !Ref 'ContainerSecurityGroup'
```

Die IaC-Dateien in Beispiel 1 und Beispiel 3 erzeugen etwas unterschiedliche CloudFormation Stacks. Parameter werden in den Stack-Vorlagendateien unterschiedlich angezeigt. Die Stack-

Vorlagendatei von Beispiel 1 CloudFormation zeigt die Parameterbezeichnungen (Schlüssel) in der Stack-Vorlagenansicht an. In der Infrastruktur-Stack-Vorlagendatei von Beispiel 3 AWS Proton CloudFormation werden die Parameterwerte angezeigt. Die AWS Proton Eingabeparameter werden nicht in der Stack-Parameteransicht der Konsole CloudFormation angezeigt.

In Beispiel 4 entspricht die AWS Proton IaC-Datei Beispiel 2.

Beispiel 4: AWS Proton Service-InstanceIaC-Datei

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Deploy a service on AWS Fargate, hosted in a public subnet, and accessible
 via a public load balancer.
Mappings:
  TaskSize:
    x-small:
      cpu: 256
      memory: 512
    small:
      cpu: 512
      memory: 1024
    medium:
      cpu: 1024
      memory: 2048
    large:
      cpu: 2048
      memory: 4096
    x-large:
      cpu: 4096
      memory: 8192
Resources:
  # A log group for storing the stdout logs from this service's containers
  LogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: '{{service_instance.name}}' # resource parameter

  # The task definition. This is a simple metadata description of what
  # container to run, and what resource requirements it has.
  TaskDefinition:
    Type: AWS::ECS::TaskDefinition
    Properties:
      Family: '{{service_instance.name}}'
```

```
      Cpu: !FindInMap [TaskSize, {{service_instance.inputs.task_size}}, cpu] # input
parameter
      Memory: !FindInMap [TaskSize, {{service_instance.inputs.task_size}}, memory]
      NetworkMode: awsvpc
      RequiresCompatibilities:
        - FARGATE
      ExecutionRoleArn: '{{environment.outputs.ECSTaskExecutionRole}}' # output from an
environment infrastructure as code file
      TaskRoleArn: !Ref "AWS::NoValue"
      ContainerDefinitions:
        - Name: '{{service_instance.name}}'
          Cpu: !FindInMap [TaskSize, {{service_instance.inputs.task_size}}, cpu]
          Memory: !FindInMap [TaskSize, {{service_instance.inputs.task_size}}, memory]
          Image: '{{service_instance.inputs.image}}'
          PortMappings:
            - ContainerPort: '{{service_instance.inputs.port}}' # input parameter
          LogConfiguration:
            LogDriver: 'awslogs'
            Options:
              awslogs-group: '{{service_instance.name}}'
              awslogs-region: !Ref 'AWS::Region'
              awslogs-stream-prefix: '{{service_instance.name}}'

  # The service_instance. The service is a resource which allows you to run multiple
  # copies of a type of task, and gather up their logs and metrics, as well
  # as monitor the number of running tasks and replace any that have crashed
  Service:
    Type: AWS::ECS::Service
    DependsOn: LoadBalancerRule
    Properties:
      ServiceName: '{{service_instance.name}}'
      Cluster: '{{environment.outputs.ClusterName}}' # output from an environment
infrastructure as code file
      LaunchType: FARGATE
      DeploymentConfiguration:
        MaximumPercent: 200
        MinimumHealthyPercent: 75
      DesiredCount: '{{service_instance.inputs.desired_count}}'       # input parameter
      NetworkConfiguration:
        AwsvpcConfiguration:
          AssignPublicIp: ENABLED
          SecurityGroups:
            - '{{environment.outputs.ContainerSecurityGroup}}' # output from an
environment infrastructure as code file
```

```
          Subnets:
            - '{{environment.outputs.PublicSubnetOne}}'        # output from an
environment infrastructure as code file
            - '{{environment.outputs.PublicSubnetTwo}}'
      TaskDefinition: !Ref 'TaskDefinition'
      LoadBalancers:
        - ContainerName: '{{service_instance.name}}'
          ContainerPort: '{{service_instance.inputs.port}}'
          TargetGroupArn: !Ref 'TargetGroup'

  # A target group. This is used for keeping track of all the tasks, and
  # what IP addresses / port numbers they have. You can query it yourself,
  # to use the addresses yourself, but most often this target group is just
  # connected to an application load balancer, or network load balancer, so
  # it can automatically distribute traffic across all the targets.
  TargetGroup:
    Type: AWS::ElasticLoadBalancingV2::TargetGroup
    Properties:
      HealthCheckIntervalSeconds: 6
      HealthCheckPath: /
      HealthCheckProtocol: HTTP
      HealthCheckTimeoutSeconds: 5
      HealthyThresholdCount: 2
      TargetType: ip
      Name: '{{service_instance.name}}'
      Port: '{{service_instance.inputs.port}}'
      Protocol: HTTP
      UnhealthyThresholdCount: 2
      VpcId: '{{environment.outputs.VpcId}}' # output from an environment
infrastructure as code file

  # Create a rule on the load balancer for routing traffic to the target group
  LoadBalancerRule:
    Type: AWS::ElasticLoadBalancingV2::ListenerRule
    Properties:
      Actions:
        - TargetGroupArn: !Ref 'TargetGroup'
          Type: 'forward'
      Conditions:
        - Field: path-pattern
          Values:
            - '*'
      ListenerArn: !Ref PublicLoadBalancerListener
      Priority: 1
```

```
  # Enable autoscaling for this service
  ScalableTarget:
    Type: AWS::ApplicationAutoScaling::ScalableTarget
    DependsOn: Service
    Properties:
      ServiceNamespace: 'ecs'
      ScalableDimension: 'ecs:service:DesiredCount'
      ResourceId:
        Fn::Join:
          - '/'
          - - service
            - '{{environment.outputs.ClusterName}}' # output from an environment
 infrastructure as code file
            - '{{service_instance.name}}'
      MinCapacity: 1
      MaxCapacity: 10
      RoleARN: !Sub arn:aws:iam::${AWS::AccountId}:role/
aws-service-role/ecs.application-autoscaling.amazonaws.com/
AWSServiceRoleForApplicationAutoScaling_ECSService

  # Create scaling policies for the service
  ScaleDownPolicy:
    Type: AWS::ApplicationAutoScaling::ScalingPolicy
    DependsOn: ScalableTarget
    Properties:
      PolicyName:
        Fn::Join:
          - '/'
          - - scale
            - '{{service_instance.name}}'
            - down
      PolicyType: StepScaling
      ResourceId:
        Fn::Join:
          - '/'
          - - service
            - '{{environment.outputs.ClusterName}}'
            - '{{service_instance.name}}'
      ScalableDimension: 'ecs:service:DesiredCount'
      ServiceNamespace: 'ecs'
      StepScalingPolicyConfiguration:
        AdjustmentType: 'ChangeInCapacity'
        StepAdjustments:
```

```
        - MetricIntervalUpperBound: 0
          ScalingAdjustment: -1
      MetricAggregationType: 'Average'
      Cooldown: 60

ScaleUpPolicy:
  Type: AWS::ApplicationAutoScaling::ScalingPolicy
  DependsOn: ScalableTarget
  Properties:
    PolicyName:
      Fn::Join:
        - '/'
        - - scale
          - '{{service_instance.name}}'
          - up
    PolicyType: StepScaling
    ResourceId:
      Fn::Join:
        - '/'
        - - service
          - '{{environment.outputs.ClusterName}}'
          - '{{service_instance.name}}'
    ScalableDimension: 'ecs:service:DesiredCount'
    ServiceNamespace: 'ecs'
    StepScalingPolicyConfiguration:
      AdjustmentType: 'ChangeInCapacity'
      StepAdjustments:
        - MetricIntervalLowerBound: 0
          MetricIntervalUpperBound: 15
          ScalingAdjustment: 1
        - MetricIntervalLowerBound: 15
          MetricIntervalUpperBound: 25
          ScalingAdjustment: 2
        - MetricIntervalLowerBound: 25
          ScalingAdjustment: 3
      MetricAggregationType: 'Average'
      Cooldown: 60

# Create alarms to trigger these policies
LowCpuUsageAlarm:
  Type: AWS::CloudWatch::Alarm
  Properties:
    AlarmName:
      Fn::Join:
```

```
          - '-'
          - - low-cpu
            - '{{service_instance.name}}'
      AlarmDescription:
        Fn::Join:
          - ' '
          - - "Low CPU utilization for service"
            - '{{service_instance.name}}'
      MetricName: CPUUtilization
      Namespace: AWS/ECS
      Dimensions:
        - Name: ServiceName
          Value: '{{service_instance.name}}'
        - Name: ClusterName
          Value:
            '{{environment.outputs.ClusterName}}'
      Statistic: Average
      Period: 60
      EvaluationPeriods: 1
      Threshold: 20
      ComparisonOperator: LessThanOrEqualToThreshold
      AlarmActions:
        - !Ref ScaleDownPolicy

  HighCpuUsageAlarm:
    Type: AWS::CloudWatch::Alarm
    Properties:
      AlarmName:
        Fn::Join:
          - '-'
          - - high-cpu
            - '{{service_instance.name}}'
      AlarmDescription:
        Fn::Join:
          - ' '
          - - "High CPU utilization for service"
            - '{{service_instance.name}}'
      MetricName: CPUUtilization
      Namespace: AWS/ECS
      Dimensions:
        - Name: ServiceName
          Value: '{{service_instance.name}}'
        - Name: ClusterName
          Value:
```

```
            '{{environment.outputs.ClusterName}}'
      Statistic: Average
      Period: 60
      EvaluationPeriods: 1
      Threshold: 70
      ComparisonOperator: GreaterThanOrEqualToThreshold
      AlarmActions:
        - !Ref ScaleUpPolicy

  EcsSecurityGroupIngressFromPublicALB:
    Type: AWS::EC2::SecurityGroupIngress
    Properties:
      Description: Ingress from the public ALB
      GroupId: '{{environment.outputs.ContainerSecurityGroup}}'
      IpProtocol: -1
      SourceSecurityGroupId: !Ref 'PublicLoadBalancerSG'

  # Public load balancer, hosted in public subnets that is accessible
  # to the public, and is intended to route traffic to one or more public
  # facing services. This is used for accepting traffic from the public
  # internet and directing it to public facing microservices
  PublicLoadBalancerSG:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: Access to the public facing load balancer
      VpcId: '{{environment.outputs.VpcId}}'
      SecurityGroupIngress:
          # Allow access to ALB from anywhere on the internet
          - CidrIp: 0.0.0.0/0
            IpProtocol: -1

  PublicLoadBalancer:
    Type: AWS::ElasticLoadBalancingV2::LoadBalancer
    Properties:
      Scheme: internet-facing
      LoadBalancerAttributes:
      - Key: idle_timeout.timeout_seconds
        Value: '30'
      Subnets:
        # The load balancer is placed into the public subnets, so that traffic
        # from the internet can reach the load balancer directly via the internet
gateway
        - '{{environment.outputs.PublicSubnetOne}}'
        - '{{environment.outputs.PublicSubnetTwo}}'
```

```
      SecurityGroups: [!Ref 'PublicLoadBalancerSG']

  PublicLoadBalancerListener:
    Type: AWS::ElasticLoadBalancingV2::Listener
    DependsOn:
      - PublicLoadBalancer
    Properties:
      DefaultActions:
        - TargetGroupArn: !Ref 'TargetGroup'
          Type: 'forward'
      LoadBalancerArn: !Ref 'PublicLoadBalancer'
      Port: 80
      Protocol: HTTP
Outputs:
  ServiceEndpoint:         # output
    Description: The URL to access the service
    Value: !Sub "http://${PublicLoadBalancer.DNSName}"
```

In Beispiel 5 stellt die AWS Proton Pipeline-IaC-Datei die Pipeline-Infrastruktur zur Unterstützung der von Beispiel 4 bereitgestellten Service-Instances bereit.

Beispiel 5: AWS Proton Service-PipelineIaC-Datei

```
Resources:
  ECRRepo:
    Type: AWS::ECR::Repository
    DeletionPolicy: Retain
  BuildProject:
    Type: AWS::CodeBuild::Project
    Properties:
      Artifacts:
        Type: CODEPIPELINE
      Environment:
        ComputeType: BUILD_GENERAL1_SMALL
        Image: aws/codebuild/amazonlinux2-x86_64-standard:3.0
        PrivilegedMode: true
        Type: LINUX_CONTAINER
        EnvironmentVariables:
        - Name: repo_name
          Type: PLAINTEXT
          Value: !Ref ECRRepo
        - Name: service_name
          Type: PLAINTEXT
```

```
          Value: '{{ service.name }}'    # resource parameter
      ServiceRole:
        Fn::GetAtt:
          - PublishRole
          - Arn
      Source:
        BuildSpec:
          Fn::Join:
            - ""
            - - >-
                {
                  "version": "0.2",
                  "phases": {
                    "install": {
                      "runtime-versions": {
                        "docker": 18
                      },
                      "commands": [
                        "pip3 install --upgrade --user awscli",
                        "echo
 'f6bd1536a743ab170b35c94ed4c7c4479763356bd543af5d391122f4af852460  yq_linux_amd64' >
 yq_linux_amd64.sha",
                        "wget https://github.com/mikefarah/yq/releases/download/3.4.0/
yq_linux_amd64",
                        "sha256sum -c yq_linux_amd64.sha",
                        "mv yq_linux_amd64 /usr/bin/yq",
                        "chmod +x /usr/bin/yq"
                      ]
                    },
                    "pre_build": {
                      "commands": [
                        "cd $CODEBUILD_SRC_DIR",
                        "$(aws ecr get-login --no-include-email --region
 $AWS_DEFAULT_REGION)",
                        "{{ pipeline.inputs.unit_test_command }}",    # input parameter
                      ]
                    },
                    "build": {
                      "commands": [
                        "IMAGE_REPO_NAME=$repo_name",
                        "IMAGE_TAG=$CODEBUILD_BUILD_NUMBER",
                        "IMAGE_ID=
              - Ref: AWS::AccountId
              - >-
```

```
                .dkr.ecr.$AWS_DEFAULT_REGION.amazonaws.com/$IMAGE_REPO_NAME:
$IMAGE_TAG",
                        "docker build -t $IMAGE_REPO_NAME:$IMAGE_TAG -f
 {{ pipeline.inputs.dockerfile }} .",     # input parameter
                        "docker tag $IMAGE_REPO_NAME:$IMAGE_TAG $IMAGE_ID;",
                        "docker push $IMAGE_ID"
                      ]
                    },
                    "post_build": {
                      "commands": [
                        "aws proton --region $AWS_DEFAULT_REGION get-service --name
 $service_name | jq -r .service.spec > service.yaml",
                        "yq w service.yaml 'instances[*].spec.image' \"$IMAGE_ID\" >
 rendered_service.yaml"
                      ]
                    }
                  },
                  "artifacts": {
                    "files": [
                      "rendered_service.yaml"
                    ]
                  }
                }
        Type: CODEPIPELINE
      EncryptionKey:
        Fn::GetAtt:
          - PipelineArtifactsBucketEncryptionKey
          - Arn
{% for service_instance in service_instances %}
  Deploy{{loop.index}}Project:
    Type: AWS::CodeBuild::Project
    Properties:
      Artifacts:
        Type: CODEPIPELINE
      Environment:
        ComputeType: BUILD_GENERAL1_SMALL
        Image: aws/codebuild/amazonlinux2-x86_64-standard:3.0
        PrivilegedMode: false
        Type: LINUX_CONTAINER
        EnvironmentVariables:
        - Name: service_name
          Type: PLAINTEXT
          Value:  '{{service.name}}'          # resource parameter
        - Name: service_instance_name
```

```
          Type: PLAINTEXT
          Value: '{{service_instance.name}}'  # resource parameter
      ServiceRole:
        Fn::GetAtt:
          - DeploymentRole
          - Arn
      Source:
        BuildSpec: >-
          {
            "version": "0.2",
            "phases": {
              "build": {
                "commands": [
                  "pip3 install --upgrade --user awscli",
                  "aws proton --region $AWS_DEFAULT_REGION update-service-instance
 --deployment-type CURRENT_VERSION --name $service_instance_name --service-name
 $service_name --spec file://rendered_service.yaml",
                  "aws proton --region $AWS_DEFAULT_REGION wait service-instance-
deployed --name $service_instance_name --service-name $service_name"
                ]
              }
            }
          }
        Type: CODEPIPELINE
      EncryptionKey:
        Fn::GetAtt:
          - PipelineArtifactsBucketEncryptionKey
          - Arn
{% endfor %}
  # This role is used to build and publish an image to ECR
  PublishRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Statement:
          - Action: sts:AssumeRole
            Effect: Allow
            Principal:
              Service: codebuild.amazonaws.com
        Version: "2012-10-17"
  PublishRoleDefaultPolicy:
    Type: AWS::IAM::Policy
    Properties:
      PolicyDocument:
```

```
        Statement:
          - Action:
              - logs:CreateLogGroup
              - logs:CreateLogStream
              - logs:PutLogEvents
            Effect: Allow
            Resource:
              - Fn::Join:
                  - ""
                  - - "arn:"
                    - Ref: AWS::Partition
                    - ":logs:"
                    - Ref: AWS::Region
                    - ":"
                    - Ref: AWS::AccountId
                    - :log-group:/aws/codebuild/
                    - Ref: BuildProject
              - Fn::Join:
                  - ""
                  - - "arn:"
                    - Ref: AWS::Partition
                    - ":logs:"
                    - Ref: AWS::Region
                    - ":"
                    - Ref: AWS::AccountId
                    - :log-group:/aws/codebuild/
                    - Ref: BuildProject
                    - :*
          - Action:
              - codebuild:CreateReportGroup
              - codebuild:CreateReport
              - codebuild:UpdateReport
              - codebuild:BatchPutTestCases
            Effect: Allow
            Resource:
              Fn::Join:
                - ""
                - - "arn:"
                  - Ref: AWS::Partition
                  - ":codebuild:"
                  - Ref: AWS::Region
                  - ":"
                  - Ref: AWS::AccountId
                  - :report-group/
```

```
                - Ref: BuildProject
                - -*
          - Action:
              - ecr:GetAuthorizationToken
            Effect: Allow
            Resource: "*"
          - Action:
              - ecr:BatchCheckLayerAvailability
              - ecr:CompleteLayerUpload
              - ecr:GetAuthorizationToken
              - ecr:InitiateLayerUpload
              - ecr:PutImage
              - ecr:UploadLayerPart
            Effect: Allow
            Resource:
              Fn::GetAtt:
                - ECRRepo
                - Arn
          - Action:
              - proton:GetService
            Effect: Allow
            Resource: "*"
          - Action:
              - s3:GetObject*
              - s3:GetBucket*
              - s3:List*
              - s3:DeleteObject*
              - s3:PutObject*
              - s3:Abort*
            Effect: Allow
            Resource:
              - Fn::GetAtt:
                  - PipelineArtifactsBucket
                  - Arn
              - Fn::Join:
                  - ""
                  - - Fn::GetAtt:
                        - PipelineArtifactsBucket
                        - Arn
                    - /*
          - Action:
              - kms:Decrypt
              - kms:DescribeKey
              - kms:Encrypt
```

```
            - kms:ReEncrypt*
            - kms:GenerateDataKey*
          Effect: Allow
          Resource:
            Fn::GetAtt:
              - PipelineArtifactsBucketEncryptionKey
              - Arn
        - Action:
            - kms:Decrypt
            - kms:Encrypt
            - kms:ReEncrypt*
            - kms:GenerateDataKey*
          Effect: Allow
          Resource:
            Fn::GetAtt:
              - PipelineArtifactsBucketEncryptionKey
              - Arn
      Version: "2012-10-17"
    PolicyName: PublishRoleDefaultPolicy
    Roles:
      - Ref: PublishRole

DeploymentRole:
  Type: AWS::IAM::Role
  Properties:
    AssumeRolePolicyDocument:
      Statement:
        - Action: sts:AssumeRole
          Effect: Allow
          Principal:
            Service: codebuild.amazonaws.com
      Version: "2012-10-17"
DeploymentRoleDefaultPolicy:
  Type: AWS::IAM::Policy
  Properties:
    PolicyDocument:
      Statement:
        - Action:
            - logs:CreateLogGroup
            - logs:CreateLogStream
            - logs:PutLogEvents
          Effect: Allow
          Resource:
            - Fn::Join:
```

```
                - ""
                - - "arn:"
                  - Ref: AWS::Partition
                  - ":logs:"
                  - Ref: AWS::Region
                  - ":"
                  - Ref: AWS::AccountId
                  - :log-group:/aws/codebuild/Deploy*Project*
              - Fn::Join:
                - ""
                - - "arn:"
                  - Ref: AWS::Partition
                  - ":logs:"
                  - Ref: AWS::Region
                  - ":"
                  - Ref: AWS::AccountId
                  - :log-group:/aws/codebuild/Deploy*Project:*
          - Action:
              - codebuild:CreateReportGroup
              - codebuild:CreateReport
              - codebuild:UpdateReport
              - codebuild:BatchPutTestCases
            Effect: Allow
            Resource:
              Fn::Join:
                - ""
                - - "arn:"
                  - Ref: AWS::Partition
                  - ":codebuild:"
                  - Ref: AWS::Region
                  - ":"
                  - Ref: AWS::AccountId
                  - :report-group/Deploy*Project
                  - -*
          - Action:
              - proton:UpdateServiceInstance
              - proton:GetServiceInstance
            Effect: Allow
            Resource: "*"
          - Action:
              - s3:GetObject*
              - s3:GetBucket*
              - s3:List*
            Effect: Allow
```

```
            Resource:
              - Fn::GetAtt:
                  - PipelineArtifactsBucket
                  - Arn
              - Fn::Join:
                  - ""
                  - - Fn::GetAtt:
                        - PipelineArtifactsBucket
                        - Arn
                    - /*
          - Action:
              - kms:Decrypt
              - kms:DescribeKey
            Effect: Allow
            Resource:
              Fn::GetAtt:
                - PipelineArtifactsBucketEncryptionKey
                - Arn
          - Action:
              - kms:Decrypt
              - kms:Encrypt
              - kms:ReEncrypt*
              - kms:GenerateDataKey*
            Effect: Allow
            Resource:
              Fn::GetAtt:
                - PipelineArtifactsBucketEncryptionKey
                - Arn
        Version: "2012-10-17"
      PolicyName: DeploymentRoleDefaultPolicy
      Roles:
        - Ref: DeploymentRole
  PipelineArtifactsBucketEncryptionKey:
    Type: AWS::KMS::Key
    Properties:
      KeyPolicy:
        Statement:
          - Action:
              - kms:Create*
              - kms:Describe*
              - kms:Enable*
              - kms:List*
              - kms:Put*
              - kms:Update*
```

```
            - kms:Revoke*
            - kms:Disable*
            - kms:Get*
            - kms:Delete*
            - kms:ScheduleKeyDeletion
            - kms:CancelKeyDeletion
            - kms:GenerateDataKey
            - kms:TagResource
            - kms:UntagResource
          Effect: Allow
          Principal:
            AWS:
              Fn::Join:
                - ""
                - - "arn:"
                  - Ref: AWS::Partition
                  - ":iam::"
                  - Ref: AWS::AccountId
                  - :root
          Resource: "*"
        - Action:
            - kms:Decrypt
            - kms:DescribeKey
            - kms:Encrypt
            - kms:ReEncrypt*
            - kms:GenerateDataKey*
          Effect: Allow
          Principal:
            AWS:
              Fn::GetAtt:
                - PipelineRole
                - Arn
          Resource: "*"
        - Action:
            - kms:Decrypt
            - kms:DescribeKey
            - kms:Encrypt
            - kms:ReEncrypt*
            - kms:GenerateDataKey*
          Effect: Allow
          Principal:
            AWS:
              Fn::GetAtt:
                - PublishRole
```

```
                - Arn
          Resource: "*"
        - Action:
            - kms:Decrypt
            - kms:Encrypt
            - kms:ReEncrypt*
            - kms:GenerateDataKey*
          Effect: Allow
          Principal:
            AWS:
              Fn::GetAtt:
                - PublishRole
                - Arn
          Resource: "*"
        - Action:
            - kms:Decrypt
            - kms:DescribeKey
          Effect: Allow
          Principal:
            AWS:
              Fn::GetAtt:
                - DeploymentRole
                - Arn
          Resource: "*"
        - Action:
            - kms:Decrypt
            - kms:Encrypt
            - kms:ReEncrypt*
            - kms:GenerateDataKey*
          Effect: Allow
          Principal:
            AWS:
              Fn::GetAtt:
                - DeploymentRole
                - Arn
          Resource: "*"
      Version: "2012-10-17"
  UpdateReplacePolicy: Delete
  DeletionPolicy: Delete
PipelineArtifactsBucket:
  Type: AWS::S3::Bucket
  Properties:
    VersioningConfiguration:
      Status: Enabled
```

```
      BucketEncryption:
        ServerSideEncryptionConfiguration:
          - ServerSideEncryptionByDefault:
              KMSMasterKeyID:
                Fn::GetAtt:
                  - PipelineArtifactsBucketEncryptionKey
                  - Arn
              SSEAlgorithm: aws:kms
      PublicAccessBlockConfiguration:
        BlockPublicAcls: true
        BlockPublicPolicy: true
        IgnorePublicAcls: true
        RestrictPublicBuckets: true
    UpdateReplacePolicy: Retain
    DeletionPolicy: Retain
  PipelineArtifactsBucketEncryptionKeyAlias:
    Type: AWS::KMS::Alias
    Properties:
      AliasName: 'alias/codepipeline-encryption-key-{{ service.name }}'
      TargetKeyId:
        Fn::GetAtt:
          - PipelineArtifactsBucketEncryptionKey
          - Arn
    UpdateReplacePolicy: Delete
    DeletionPolicy: Delete
  PipelineRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Statement:
          - Action: sts:AssumeRole
            Effect: Allow
            Principal:
              Service: codepipeline.amazonaws.com
        Version: "2012-10-17"
  PipelineRoleDefaultPolicy:
    Type: AWS::IAM::Policy
    Properties:
      PolicyDocument:
        Statement:
          - Action:
              - s3:GetObject*
              - s3:GetBucket*
              - s3:List*
```

```
            - s3:DeleteObject*
            - s3:PutObject*
            - s3:Abort*
          Effect: Allow
          Resource:
            - Fn::GetAtt:
                - PipelineArtifactsBucket
                - Arn
            - Fn::Join:
                - ""
                - - Fn::GetAtt:
                      - PipelineArtifactsBucket
                      - Arn
                  - /*
        - Action:
            - kms:Decrypt
            - kms:DescribeKey
            - kms:Encrypt
            - kms:ReEncrypt*
            - kms:GenerateDataKey*
          Effect: Allow
          Resource:
            Fn::GetAtt:
              - PipelineArtifactsBucketEncryptionKey
              - Arn
        - Action: codestar-connections:*
          Effect: Allow
          Resource: "*"
        - Action: sts:AssumeRole
          Effect: Allow
          Resource:
            Fn::GetAtt:
              - PipelineBuildCodePipelineActionRole
              - Arn
        - Action: sts:AssumeRole
          Effect: Allow
          Resource:
            Fn::GetAtt:
              - PipelineDeployCodePipelineActionRole
              - Arn
      Version: "2012-10-17"
    PolicyName: PipelineRoleDefaultPolicy
    Roles:
      - Ref: PipelineRole
```

```
  Pipeline:
    Type: AWS::CodePipeline::Pipeline
    Properties:
      RoleArn:
        Fn::GetAtt:
          - PipelineRole
          - Arn
      Stages:
        - Actions:
            - ActionTypeId:
                Category: Source
                Owner: AWS
                Provider: CodeStarSourceConnection
                Version: "1"
              Configuration:
                ConnectionArn: '{{ service.repository_connection_arn }}'
                FullRepositoryId: '{{ service.repository_id }}'
                BranchName: '{{ service.branch_name }}'
              Name: Checkout
              OutputArtifacts:
                - Name: Artifact_Source_Checkout
              RunOrder: 1
          Name: Source
        - Actions:
            - ActionTypeId:
                Category: Build
                Owner: AWS
                Provider: CodeBuild
                Version: "1"
              Configuration:
                ProjectName:
                  Ref: BuildProject
              InputArtifacts:
                - Name: Artifact_Source_Checkout
              Name: Build
              OutputArtifacts:
                - Name: BuildOutput
              RoleArn:
                Fn::GetAtt:
                  - PipelineBuildCodePipelineActionRole
                  - Arn
              RunOrder: 1
          Name: Build {%- for service_instance in service_instances %}
        - Actions:
```

```
            - ActionTypeId:
                Category: Build
                Owner: AWS
                Provider: CodeBuild
                Version: "1"
              Configuration:
                ProjectName:
                  Ref: Deploy{{loop.index}}Project
              InputArtifacts:
                - Name: BuildOutput
              Name: Deploy
              RoleArn:
                Fn::GetAtt:
                  - PipelineDeployCodePipelineActionRole
                  - Arn
              RunOrder: 1
          Name: 'Deploy{{service_instance.name}}'
{%- endfor %}
      ArtifactStore:
        EncryptionKey:
          Id:
            Fn::GetAtt:
              - PipelineArtifactsBucketEncryptionKey
              - Arn
          Type: KMS
        Location:
          Ref: PipelineArtifactsBucket
        Type: S3
    DependsOn:
      - PipelineRoleDefaultPolicy
      - PipelineRole
  PipelineBuildCodePipelineActionRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Statement:
          - Action: sts:AssumeRole
            Effect: Allow
            Principal:
              AWS:
                Fn::Join:
                  - ""
                  - - "arn:"
                    - Ref: AWS::Partition
```

```
                  - ":iam::"
                  - Ref: AWS::AccountId
                  - :root
      Version: "2012-10-17"
  PipelineBuildCodePipelineActionRoleDefaultPolicy:
    Type: AWS::IAM::Policy
    Properties:
      PolicyDocument:
        Statement:
          - Action:
              - codebuild:BatchGetBuilds
              - codebuild:StartBuild
              - codebuild:StopBuild
            Effect: Allow
            Resource:
              Fn::GetAtt:
                - BuildProject
                - Arn
        Version: "2012-10-17"
      PolicyName: PipelineBuildCodePipelineActionRoleDefaultPolicy
      Roles:
        - Ref: PipelineBuildCodePipelineActionRole
  PipelineDeployCodePipelineActionRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Statement:
          - Action: sts:AssumeRole
            Effect: Allow
            Principal:
              AWS:
                Fn::Join:
                  - ""
                  - - "arn:"
                    - Ref: AWS::Partition
                    - ":iam::"
                    - Ref: AWS::AccountId
                    - :root
        Version: "2012-10-17"
  PipelineDeployCodePipelineActionRoleDefaultPolicy:
    Type: AWS::IAM::Policy
    Properties:
      PolicyDocument:
        Statement:
```

```
          - Action:
              - codebuild:BatchGetBuilds
              - codebuild:StartBuild
              - codebuild:StopBuild
            Effect: Allow
            Resource:
              Fn::Join:
                - ""
                - - "arn:"
                  - Ref: AWS::Partition
                  - ":codebuild:"
                  - Ref: AWS::Region
                  - ":"
                  - Ref: AWS::AccountId
                  - ":project/Deploy*"
        Version: "2012-10-17"
      PolicyName: PipelineDeployCodePipelineActionRoleDefaultPolicy
      Roles:
        - Ref: PipelineDeployCodePipelineActionRole
Outputs:
  PipelineEndpoint:
    Description: The URL to access the pipeline
    Value: !Sub "https://${AWS::Region}.console.aws.amazon.com/codesuite/codepipeline/
pipelines/${Pipeline}/view?region=${AWS::Region}"

                ]
              }
            }
          }
        Type: CODEPIPELINE
      EncryptionKey:
        Fn::GetAtt:
          - PipelineArtifactsBucketEncryptionKey
          - Arn
{% endfor %}
  # This role is used to build and publish an image to ECR
  PublishRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Statement:
          - Action: sts:AssumeRole
            Effect: Allow
            Principal:
```

```
            Service: codebuild.amazonaws.com
      Version: "2012-10-17"
  PublishRoleDefaultPolicy:
    Type: AWS::IAM::Policy
    Properties:
      PolicyDocument:
        Statement:
          - Action:
              - logs:CreateLogGroup
              - logs:CreateLogStream
              - logs:PutLogEvents
            Effect: Allow
            Resource:
              - Fn::Join:
                  - ""
                  - - "arn:"
                    - Ref: AWS::Partition
                    - ":logs:"
                    - Ref: AWS::Region
                    - ":"
                    - Ref: AWS::AccountId
                    - :log-group:/aws/codebuild/
                    - Ref: BuildProject
              - Fn::Join:
                  - ""
                  - - "arn:"
                    - Ref: AWS::Partition
                    - ":logs:"
                    - Ref: AWS::Region
                    - ":"
                    - Ref: AWS::AccountId
                    - :log-group:/aws/codebuild/
                    - Ref: BuildProject
                    - :*
          - Action:
              - codebuild:CreateReportGroup
              - codebuild:CreateReport
              - codebuild:UpdateReport
              - codebuild:BatchPutTestCases
            Effect: Allow
            Resource:
              Fn::Join:
                - ""
                - - "arn:"
```

```
                - Ref: AWS::Partition
                - ":codebuild:"
                - Ref: AWS::Region
                - ":"
                - Ref: AWS::AccountId
                - :report-group/
                - Ref: BuildProject
                - -*
          - Action:
              - ecr:GetAuthorizationToken
            Effect: Allow
            Resource: "*"
          - Action:
              - ecr:BatchCheckLayerAvailability
              - ecr:CompleteLayerUpload
              - ecr:GetAuthorizationToken
              - ecr:InitiateLayerUpload
              - ecr:PutImage
              - ecr:UploadLayerPart
            Effect: Allow
            Resource:
              Fn::GetAtt:
                - ECRRepo
                - Arn
          - Action:
              - proton:GetService
            Effect: Allow
            Resource: "*"
          - Action:
              - s3:GetObject*
              - s3:GetBucket*
              - s3:List*
              - s3:DeleteObject*
              - s3:PutObject*
              - s3:Abort*
            Effect: Allow
            Resource:
              - Fn::GetAtt:
                  - PipelineArtifactsBucket
                  - Arn
              - Fn::Join:
                  - ""
                  - - Fn::GetAtt:
                        - PipelineArtifactsBucket
```

```
                      - Arn
                  - /*
        - Action:
            - kms:Decrypt
            - kms:DescribeKey
            - kms:Encrypt
            - kms:ReEncrypt*
            - kms:GenerateDataKey*
          Effect: Allow
          Resource:
            Fn::GetAtt:
              - PipelineArtifactsBucketEncryptionKey
              - Arn
        - Action:
            - kms:Decrypt
            - kms:Encrypt
            - kms:ReEncrypt*
            - kms:GenerateDataKey*
          Effect: Allow
          Resource:
            Fn::GetAtt:
              - PipelineArtifactsBucketEncryptionKey
              - Arn
      Version: "2012-10-17"
    PolicyName: PublishRoleDefaultPolicy
    Roles:
      - Ref: PublishRole

DeploymentRole:
  Type: AWS::IAM::Role
  Properties:
    AssumeRolePolicyDocument:
      Statement:
        - Action: sts:AssumeRole
          Effect: Allow
          Principal:
            Service: codebuild.amazonaws.com
      Version: "2012-10-17"
DeploymentRoleDefaultPolicy:
  Type: AWS::IAM::Policy
  Properties:
    PolicyDocument:
      Statement:
        - Action:
```

```
            - logs:CreateLogGroup
            - logs:CreateLogStream
            - logs:PutLogEvents
          Effect: Allow
          Resource:
            - Fn::Join:
                - ""
                - - "arn:"
                  - Ref: AWS::Partition
                  - ":logs:"
                  - Ref: AWS::Region
                  - ":"
                  - Ref: AWS::AccountId
                  - :log-group:/aws/codebuild/Deploy*Project*
            - Fn::Join:
                - ""
                - - "arn:"
                  - Ref: AWS::Partition
                  - ":logs:"
                  - Ref: AWS::Region
                  - ":"
                  - Ref: AWS::AccountId
                  - :log-group:/aws/codebuild/Deploy*Project:*
        - Action:
            - codebuild:CreateReportGroup
            - codebuild:CreateReport
            - codebuild:UpdateReport
            - codebuild:BatchPutTestCases
          Effect: Allow
          Resource:
            Fn::Join:
              - ""
              - - "arn:"
                - Ref: AWS::Partition
                - ":codebuild:"
                - Ref: AWS::Region
                - ":"
                - Ref: AWS::AccountId
                - :report-group/Deploy*Project
                - -*
        - Action:
            - proton:UpdateServiceInstance
            - proton:GetServiceInstance
          Effect: Allow
```

```
            Resource: "*"
          - Action:
              - s3:GetObject*
              - s3:GetBucket*
              - s3:List*
            Effect: Allow
            Resource:
              - Fn::GetAtt:
                  - PipelineArtifactsBucket
                  - Arn
              - Fn::Join:
                  - ""
                  - - Fn::GetAtt:
                        - PipelineArtifactsBucket
                        - Arn
                    - /*
          - Action:
              - kms:Decrypt
              - kms:DescribeKey
            Effect: Allow
            Resource:
              Fn::GetAtt:
                - PipelineArtifactsBucketEncryptionKey
                - Arn
          - Action:
              - kms:Decrypt
              - kms:Encrypt
              - kms:ReEncrypt*
              - kms:GenerateDataKey*
            Effect: Allow
            Resource:
              Fn::GetAtt:
                - PipelineArtifactsBucketEncryptionKey
                - Arn
        Version: "2012-10-17"
      PolicyName: DeploymentRoleDefaultPolicy
      Roles:
        - Ref: DeploymentRole
  PipelineArtifactsBucketEncryptionKey:
    Type: AWS::KMS::Key
    Properties:
      KeyPolicy:
        Statement:
          - Action:
```

```
            - kms:Create*
            - kms:Describe*
            - kms:Enable*
            - kms:List*
            - kms:Put*
            - kms:Update*
            - kms:Revoke*
            - kms:Disable*
            - kms:Get*
            - kms:Delete*
            - kms:ScheduleKeyDeletion
            - kms:CancelKeyDeletion
            - kms:GenerateDataKey
            - kms:TagResource
            - kms:UntagResource
          Effect: Allow
          Principal:
            AWS:
              Fn::Join:
                - ""
                - - "arn:"
                  - Ref: AWS::Partition
                  - ":iam::"
                  - Ref: AWS::AccountId
                  - :root
          Resource: "*"
        - Action:
            - kms:Decrypt
            - kms:DescribeKey
            - kms:Encrypt
            - kms:ReEncrypt*
            - kms:GenerateDataKey*
          Effect: Allow
          Principal:
            AWS:
              Fn::GetAtt:
                - PipelineRole
                - Arn
          Resource: "*"
        - Action:
            - kms:Decrypt
            - kms:DescribeKey
            - kms:Encrypt
            - kms:ReEncrypt*
```

```
            - kms:GenerateDataKey*
          Effect: Allow
          Principal:
            AWS:
              Fn::GetAtt:
                - PublishRole
                - Arn
          Resource: "*"
        - Action:
            - kms:Decrypt
            - kms:Encrypt
            - kms:ReEncrypt*
            - kms:GenerateDataKey*
          Effect: Allow
          Principal:
            AWS:
              Fn::GetAtt:
                - PublishRole
                - Arn
          Resource: "*"
        - Action:
            - kms:Decrypt
            - kms:DescribeKey
          Effect: Allow
          Principal:
            AWS:
              Fn::GetAtt:
                - DeploymentRole
                - Arn
          Resource: "*"
        - Action:
            - kms:Decrypt
            - kms:Encrypt
            - kms:ReEncrypt*
            - kms:GenerateDataKey*
          Effect: Allow
          Principal:
            AWS:
              Fn::GetAtt:
                - DeploymentRole
                - Arn
          Resource: "*"
      Version: "2012-10-17"
  UpdateReplacePolicy: Delete
```

```
    DeletionPolicy: Delete
  PipelineArtifactsBucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketEncryption:
        ServerSideEncryptionConfiguration:
          - ServerSideEncryptionByDefault:
              KMSMasterKeyID:
                Fn::GetAtt:
                  - PipelineArtifactsBucketEncryptionKey
                  - Arn
              SSEAlgorithm: aws:kms
      PublicAccessBlockConfiguration:
        BlockPublicAcls: true
        BlockPublicPolicy: true
        IgnorePublicAcls: true
        RestrictPublicBuckets: true
    UpdateReplacePolicy: Retain
    DeletionPolicy: Retain
  PipelineArtifactsBucketEncryptionKeyAlias:
    Type: AWS::KMS::Alias
    Properties:
      AliasName: 'alias/codepipeline-encryption-key-{{ service.name }}'     # resource
parameter
      TargetKeyId:
        Fn::GetAtt:
          - PipelineArtifactsBucketEncryptionKey
          - Arn
    UpdateReplacePolicy: Delete
    DeletionPolicy: Delete
  PipelineRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Statement:
          - Action: sts:AssumeRole
            Effect: Allow
            Principal:
              Service: codepipeline.amazonaws.com
        Version: "2012-10-17"
  PipelineRoleDefaultPolicy:
    Type: AWS::IAM::Policy
    Properties:
      PolicyDocument:
```

```
        Statement:
          - Action:
              - s3:GetObject*
              - s3:GetBucket*
              - s3:List*
              - s3:DeleteObject*
              - s3:PutObject*
              - s3:Abort*
            Effect: Allow
            Resource:
              - Fn::GetAtt:
                  - PipelineArtifactsBucket
                  - Arn
              - Fn::Join:
                  - ""
                  - - Fn::GetAtt:
                        - PipelineArtifactsBucket
                        - Arn
                    - /*
          - Action:
              - kms:Decrypt
              - kms:DescribeKey
              - kms:Encrypt
              - kms:ReEncrypt*
              - kms:GenerateDataKey*
            Effect: Allow
            Resource:
              Fn::GetAtt:
                - PipelineArtifactsBucketEncryptionKey
                - Arn
          - Action: codestar-connections:*
            Effect: Allow
            Resource: "*"
          - Action: sts:AssumeRole
            Effect: Allow
            Resource:
              Fn::GetAtt:
                - PipelineBuildCodePipelineActionRole
                - Arn
          - Action: sts:AssumeRole
            Effect: Allow
            Resource:
              Fn::GetAtt:
                - PipelineDeployCodePipelineActionRole
```

```
                - Arn
        Version: "2012-10-17"
      PolicyName: PipelineRoleDefaultPolicy
      Roles:
        - Ref: PipelineRole
  Pipeline:
    Type: AWS::CodePipeline::Pipeline
    Properties:
      RoleArn:
        Fn::GetAtt:
          - PipelineRole
          - Arn
      Stages:
        - Actions:
            - ActionTypeId:
                Category: Source
                Owner: AWS
                Provider: CodeStarSourceConnection
                Version: "1"
              Configuration:
                ConnectionArn: '{{ service.repository_connection_arn }}'   # resource
parameter
                FullRepositoryId: '{{ service.repository_id }}'            # resource
parameter
                BranchName: '{{ service.branch_name }}'                    # resource
parameter
              Name: Checkout
              OutputArtifacts:
                - Name: Artifact_Source_Checkout
              RunOrder: 1
          Name: Source
        - Actions:
            - ActionTypeId:
                Category: Build
                Owner: AWS
                Provider: CodeBuild
                Version: "1"
              Configuration:
                ProjectName:
                  Ref: BuildProject
              InputArtifacts:
                - Name: Artifact_Source_Checkout
              Name: Build
              OutputArtifacts:
```

```
                - Name: BuildOutput
              RoleArn:
                Fn::GetAtt:
                  - PipelineBuildCodePipelineActionRole
                  - Arn
              RunOrder: 1
          Name: Build {%- for service_instance in service_instances %}
        - Actions:
            - ActionTypeId:
                Category: Build
                Owner: AWS
                Provider: CodeBuild
                Version: "1"
              Configuration:
                ProjectName:
                  Ref: Deploy{{loop.index}}Project
              InputArtifacts:
                - Name: BuildOutput
              Name: Deploy
              RoleArn:
                Fn::GetAtt:
                  - PipelineDeployCodePipelineActionRole
                  - Arn
              RunOrder: 1
          Name: 'Deploy{{service_instance.name}}'         # resource parameter
{%- endfor %}
      ArtifactStore:
        EncryptionKey:
          Id:
            Fn::GetAtt:
              - PipelineArtifactsBucketEncryptionKey
              - Arn
          Type: KMS
        Location:
          Ref: PipelineArtifactsBucket
        Type: S3
    DependsOn:
      - PipelineRoleDefaultPolicy
      - PipelineRole
  PipelineBuildCodePipelineActionRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Statement:
```

```
          - Action: sts:AssumeRole
            Effect: Allow
            Principal:
              AWS:
                Fn::Join:
                  - ""
                  - - "arn:"
                    - Ref: AWS::Partition
                    - ":iam::"
                    - Ref: AWS::AccountId
                    - :root
        Version: "2012-10-17"
  PipelineBuildCodePipelineActionRoleDefaultPolicy:
    Type: AWS::IAM::Policy
    Properties:
      PolicyDocument:
        Statement:
          - Action:
              - codebuild:BatchGetBuilds
              - codebuild:StartBuild
              - codebuild:StopBuild
            Effect: Allow
            Resource:
              Fn::GetAtt:
                - BuildProject
                - Arn
        Version: "2012-10-17"
      PolicyName: PipelineBuildCodePipelineActionRoleDefaultPolicy
      Roles:
        - Ref: PipelineBuildCodePipelineActionRole
  PipelineDeployCodePipelineActionRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Statement:
          - Action: sts:AssumeRole
            Effect: Allow
            Principal:
              AWS:
                Fn::Join:
                  - ""
                  - - "arn:"
                    - Ref: AWS::Partition
                    - ":iam::"
```

```
                    - Ref: AWS::AccountId
                    - :root
        Version: "2012-10-17"
  PipelineDeployCodePipelineActionRoleDefaultPolicy:
    Type: AWS::IAM::Policy
    Properties:
      PolicyDocument:
        Statement:
          - Action:
              - codebuild:BatchGetBuilds
              - codebuild:StartBuild
              - codebuild:StopBuild
            Effect: Allow
            Resource:
              Fn::Join:
                - ""
                - - "arn:"
                  - Ref: AWS::Partition
                  - ":codebuild:"
                  - Ref: AWS::Region
                  - ":"
                  - Ref: AWS::AccountId
                  - ":project/Deploy*"
        Version: "2012-10-17"
      PolicyName: PipelineDeployCodePipelineActionRoleDefaultPolicy
      Roles:
        - Ref: PipelineDeployCodePipelineActionRole
Outputs:
  PipelineEndpoint:
    Description: The URL to access the pipeline
    Value: !Sub "https://${AWS::Region}.console.aws.amazon.com/codesuite/codepipeline/
pipelines/${Pipeline}/view?region=${AWS::Region}"
```

CodeBuild Bereitstellungsvorlagen-Bundle

CodeBuild Anstatt IaC-Vorlagen zum Rendern von IaC-Dateien zu verwenden und diese mit einer IaC-Bereitstellungs-Engine auszuführen, führt AWS Proton einfach Ihre Shell-Befehle aus. Dazu AWS Proton erstellt ein - AWS CodeBuild Projekt für die Umgebung im Umgebungskonto und startet einen Auftrag zum Ausführen Ihrer Befehle für jede AWS Proton Ressourcenerstellung oder -aktualisierung. Wenn Sie ein Vorlagen-Bundle erstellen, stellen Sie ein Manifest bereit, das Befehle zur Infrastrukturbereitstellung und -aufhebung sowie alle Programme, Skripts und anderen Dateien angibt, die diese Befehle möglicherweise benötigen. Ihre Befehle können Eingaben lesen, die AWS

Proton bereitstellt, und sind für die Bereitstellung oder Aufhebung der Bereitstellung von Infrastruktur und die Generierung von Ausgabewerten verantwortlich.

Das Manifest gibt auch an, wie die Eingabedatei rendern AWS Proton soll, die Ihr Code eingeben und Eingabewerte abrufen kann. Er kann in JSON oder HCL gerendert werden. Weitere Informationen zu Eingabeparametern finden Sie unter the section called “CodeBuild Bereitstellungsparameter”. Weitere Informationen zu Manifestdateien finden Sie unter the section called “Manifest und Wrapup”.

> **Note**
>
> Sie können die CodeBuild Bereitstellung mit Umgebungen und Services verwenden. Derzeit können Sie Komponenten nicht auf diese Weise bereitstellen.

Beispiel: Verwenden der AWS CDK mit CodeBuild Bereitstellung

Als Beispiel für die Verwendung der CodeBuild Bereitstellung können Sie Code einschließen, der die verwendet, AWS Cloud Development Kit (AWS CDK) um AWS Ressourcen bereitzustellen (bereitzustellen) und die Bereitstellung aufzuheben (zerstören), sowie ein Manifest, das das CDK installiert und Ihren CDK-Code ausführt.

In den folgenden Abschnitten werden Beispieldateien aufgeführt, die Sie in ein CodeBuild Bereitstellungsvorlagenpaket aufnehmen können, das eine Umgebung mithilfe der bereitstellt AWS CDK.

Manifest

Die folgende Manifestdatei legt die CodeBuild Bereitstellung fest und enthält die Befehle, die für die Installation und Verwendung von AWS CDK, die Verarbeitung von Ausgabedateien und die Rückgabe von Ausgaben an erforderlich sind AWS Proton.

Example Infrastruktur/Manifest.yaml

```
infrastructure:
  templates:
    - rendering_engine: codebuild
      settings:
        image: aws/codebuild/amazonlinux2-x86_64-standard:4.0
        runtimes:
          nodejs: 16
```

```
        provision:
          - npm install
          - npm run build
          - npm run cdk bootstrap
          - npm run cdk deploy -- --require-approval never --outputs-file proton-
outputs.json
          - jq 'to_entries | map_values(.value) | add | to_entries | map({key:.key,
 valueString:.value})' < proton-outputs.json > outputs.json
          - aws proton notify-resource-deployment-status-change --resource-arn
 $RESOURCE_ARN --status IN_PROGRESS --outputs file://./outputs.json
        deprovision:
          - npm install
          - npm run build
          - npm run cdk destroy
        project_properties:
          VpcConfig:
            VpcId: "{{ environment.inputs.codebuild_vpc_id }}"
            Subnets: "{{ environment.inputs.codebuild_subnets }}"
            SecurityGroupIds: "{{ environment.inputs.codebuild_security_groups }}"
```

Schema

Die folgende Schemadatei definiert Parameter für die Umgebung. Ihr AWS CDK Code kann während der Bereitstellung auf Werte dieser Parameter verweisen.

Example schema/schema.yaml

```
schema:
  format:
    openapi: "3.0.0"
  environment_input_type: "MyEnvironmentInputType"
  types:
    MyEnvironmentInputType:
      type: object
      description: "Input properties for my environment"
      properties:
        my_sample_input:
          type: string
          description: "This is a sample input"
          default: "hello world"
        my_other_sample_input:
          type: string
          description: "Another sample input"
```

```
      required:
        - my_other_sample_input
```

AWS CDK -Dateien

Die folgenden Dateien sind ein Beispiel für ein Node.js-CDK-Projekt.

Example Infrastructure/package.json

```
{
  "name": "ProtonEnvironment",
  "version": "0.1.0",
  "bin": {
    "ProtonEnvironmente": "bin/ProtonEnvironment.js"
  },
  "scripts": {
    "build": "tsc",
    "watch": "tsc -w",
    "test": "jest",
    "cdk": "cdk"
  },
  "devDependencies": {
    "@types/jest": "^28.1.7",
    "@types/node": "18.7.6",
    "jest": "^28.1.3",
    "ts-jest": "^28.0.8",
    "aws-cdk": "2.37.1",
    "ts-node": "^10.9.1",
    "typescript": "~4.7.4"
  },
  "dependencies": {
    "aws-cdk-lib": "2.37.1",
    "constructs": "^10.1.77",
    "source-map-support": "^0.5.21"
  }
}
```

Example Infrastructure/tsconfig.json

```
{
  "compilerOptions": {
    "target": "ES2018",
    "module": "commonjs",
```

```
    "lib": [
      "es2018"
    ],
    "declaration": true,
    "strict": true,
    "noImplicitAny": true,
    "strictNullChecks": true,
    "noImplicitThis": true,
    "alwaysStrict": true,
    "noUnusedLocals": false,
    "noUnusedParameters": false,
    "noImplicitReturns": true,
    "noFallthroughCasesInSwitch": false,
    "inlineSourceMap": true,
    "inlineSources": true,
    "experimentalDecorators": true,
    "strictPropertyInitialization": false,
    "resolveJsonModule": true,
    "esModuleInterop": true,
    "typeRoots": [
      "./node_modules/@types"
    ]
  },
  "exclude": [
    "node_modules",
    "cdk.out"
  ]
}
```

Example Infrastruktur/cdk.json

```
{
  "app": "npx ts-node --prefer-ts-exts bin/ProtonEnvironment.ts",
  "outputsFile": "proton-outputs.json",
  "watch": {
    "include": [
      "**"
    ],
    "exclude": [
      "README.md",
      "cdk*.json",
      "**/*.d.ts",
      "**/*.js",
```

```
      "tsconfig.json",
      "package*.json",
      "yarn.lock",
      "node_modules",
      "test"
    ]
  },
  "context": {
    "@aws-cdk/aws-apigateway:usagePlanKeyOrderInsensitiveId": true,
    "@aws-cdk/core:stackRelativeExports": true,
    "@aws-cdk/aws-rds:lowercaseDbIdentifier": true,
    "@aws-cdk/aws-lambda:recognizeVersionProps": true,
    "@aws-cdk/aws-cloudfront:defaultSecurityPolicyTLSv1.2_2021": true,
    "@aws-cdk-containers/ecs-service-extensions:enableDefaultLogDriver": true,
    "@aws-cdk/aws-ec2:uniqueImdsv2TemplateName": true,
    "@aws-cdk/core:target-partitions": [
      "aws",
      "aws-cn"
    ]
  }
}
```

Example Infrastruktur/bin/ProtonEnvironment.ts

```
#!/usr/bin/env node
import 'source-map-support/register';
import * as cdk from 'aws-cdk-lib';
import { ProtonEnvironmentStack } from '../lib/ProtonEnvironmentStack';

const app = new cdk.App();
new ProtonEnvironmentStack(app, 'ProtonEnvironmentStack', {});
```

Example infrastructure/lib/ProtonEnvironmentStack.ts

```
import { Stack, StackProps } from 'aws-cdk-lib';
import { Construct } from 'constructs';
import * as cdk from 'aws-cdk-lib';
import * as ssm from 'aws-cdk-lib/aws-ssm';
import input from '../proton-inputs.json';

export class ProtonEnvironmentStack extends Stack {
  constructor(scope: Construct, id: string, props?: StackProps) {
    super(scope, id, { ...props, stackName: process.env.STACK_NAME });
```

```
    const ssmParam = new ssm.StringParameter(this, "ssmParam", {
      stringValue: input.environment.inputs.my_sample_input,
      parameterName: `${process.env.STACK_NAME}-Param`,
      tier: ssm.ParameterTier.STANDARD
    })

    new cdk.CfnOutput(this, 'ssmParamOutput', {
      value: ssmParam.parameterName,
      description: 'The name of the ssm parameter',
      exportName: `${process.env.STACK_NAME}-Param`
    });
  }
}
```

Rendern der Eingabedatei

Wenn Sie eine Umgebung mit einer CodeBuild-basierten Bereitstellungsvorlage erstellen, AWS Proton rendert eine Eingabedatei mit Eingabeparameterwerten, die Sie angegeben haben. Ihr Code kann sich auf diese Werte beziehen. Die folgende Datei ist ein Beispiel für eine gerenderte Eingabedatei.

Example Infrastruktur/proton-inputs.json

```
{
  "environment": {
    "name": "myenv",
    "inputs": {
      "my_sample_input": "10.0.0.0/16",
      "my_other_sample_input": "11.0.0.0/16"
    }
  }
}
```

Terraform-IaC-Dateien

Erfahren Sie, wie Sie Terraform Infrastructure as Code (IaC)-Dateien mit verwenden AWS Proton. Terraform ist eine weit verbreitete Open-Source-IaC-Engine, die von entwickelt wurdeHashiCorp. Terraform-Module werden in der HCL- HashiCorpSprache von entwickelt und unterstützen mehrere Backend-Infrastrukturanbieter, einschließlich Amazon Web Services.

AWS Proton unterstützt die selbstverwaltete Bereitstellung für Terraform IaC .

Ein vollständiges Beispiel für ein Bereitstellungs-Repository, das auf Pull-Anfragen reagiert und die Infrastrukturbereitstellung implementiert, finden Sie unter Terraform- OpenSource GitHub Aktionen-Automatisierungsvorlage für AWS Proton auf GitHub.

So funktioniert die selbstverwaltete Bereitstellung mit Terraform-IaC-Vorlagenpaketdateien:

1. Wenn Sie eine Umgebung aus Terraform-Vorlagenpaketen erstellen, AWS Proton kompiliert Ihre `.tf` Dateien mit Konsolen- oder `spec file` Eingabeparametern.
2. Er stellt eine Pull-Anforderung, um die kompilierten IaC-Dateien mit dem Repository zusammenzuführen, das Sie bei registriert haben AWS Proton.
3. Wenn die Anforderung genehmigt wurde, AWS Proton wartet auf den Bereitstellungsstatus, den Sie angeben.
4. Wenn die Anforderung abgelehnt wird, wird die Umgebungserstellung abgebrochen.
5. Wenn bei der Pull-Anforderung eine Zeitüberschreitung auftritt, ist die Umgebungserstellung nicht abgeschlossen.

AWS Proton mit Überlegungen zu Terraform IaC:

- AWS Proton verwaltet Ihre Terraform-Bereitstellung nicht.
- Sie müssen ein Bereitstellungs-Repository mit .makes-Pull-Anforderungen in diesem Repository registrieren. AWS Proton AWS Proton
- Sie müssen eine CodeStar Verbindung erstellen, um eine Verbindung AWS Proton zu Ihrem Bereitstellungs-Repository herzustellen.
- Um aus AWS Proton kompilierten IaC-Dateien bereitzustellen, müssen Sie auf AWS Proton Pull-Anforderungen antworten. AWS Proton makes-Pull-Anforderungen nach Erstellungs- und Aktualisierungsaktionen für Umgebung und Service. Weitere Informationen finden Sie unter AWS Proton-Umgebungen und AWS Proton-Services.
- Um eine Pipeline aus AWS Proton kompilierten IaC-Dateien bereitzustellen, müssen Sie ein CI/CD-Pipeline-Repository erstellen.
- Ihre auf Pull-Anfragen basierende Bereitstellungsautomatisierung muss Schritte enthalten, um AWS Proton über Statusänderungen bereitgestellter AWS Proton Ressourcen zu benachrichtigen. Sie können die AWS Proton NotifyResourceDeploymentStatusChange API verwenden.
- Sie können keine Services, Pipelines und Komponenten bereitstellen, die aus CloudFormation IaC-Dateien erstellt wurden, in Umgebungen, die aus Terraform-IaC-Dateien erstellt wurden.

- Sie können keine Services, Pipelines und Komponenten bereitstellen, die aus Terraform-IaC-Dateien erstellt wurden, in Umgebungen, die aus CloudFormation IaC-Dateien erstellt wurden.

Wenn Sie Ihre Terraform-IaC-Dateien für vorbereiten AWS Proton, fügen Sie Ihren Eingabevariablen Namespaces hinzu, wie in den folgenden Beispielen gezeigt. Weitere Informationen finden Sie unter Parameter.

Beispiel 1: AWS Proton Umgebung Terraform IaC-Datei

```
terraform {
  required_providers {
    aws = {
      source  = "hashicorp/aws"
      version = "~> 3.0"
    }
  }
  // This tells terraform to store the state file in s3 at the location
  // s3://terraform-state-bucket/tf-os-sample/terraform.tfstate
  backend "s3" {
    bucket = "terraform-state-bucket"
    key    = "tf-os-sample/terraform.tfstate"
    region = "us-east-1"
  }
}

// Configure the AWS Provider
provider "aws" {
  region = "us-east-1"
  default_tags {
    tags = var.proton_tags
  }
}

resource "aws_ssm_parameter" "my_ssm_parameter" {
  name  = "my_ssm_parameter"
  type  = "String"
  // Use the Proton environment.inputs. namespace
  value = var.environment.inputs.ssm_parameter_value
}
```

Kompilierte Infrastruktur als Code

Wenn Sie eine Umgebung oder einen Service erstellen, AWS Proton kompiliert Ihre Infrastruktur als Codedateien mit Konsole oder `spec file` Eingaben. Es erstellt - `proton.`*`resource-type`*`.variables.tf` und -`proton.auto.tfvars.json`Dateien für Ihre Eingaben, die von Terraform verwendet werden können, wie in den folgenden Beispielen gezeigt. Diese Dateien befinden sich in einem angegebenen Repository in einem Ordner, der dem Namen der Umgebung oder der Service-Instance entspricht.

Das Beispiel zeigt, wie Tags in die Variablendefinition und Variablenwerte AWS Proton einschließt und wie Sie diese AWS Proton Tags an bereitgestellte Ressourcen weitergeben können. Weitere Informationen finden Sie unter the section called “Weitergabe von Tags an bereitgestellte Ressourcen”.

Beispiel 2: kompilierte IaC-Dateien für eine Umgebung mit dem Namen „dev“.

dev/environment.tf:

```
terraform {
  required_providers {
    aws = {
      source  = "hashicorp/aws"
      version = "~> 3.0"
    }
  }
  // This tells terraform to store the state file in s3 at the location
  // s3://terraform-state-bucket/tf-os-sample/terraform.tfstate
  backend "s3" {
    bucket = "terraform-state-bucket"
    key    = "tf-os-sample/terraform.tfstate"
    region = "us-east-1"
  }
}

// Configure the AWS Provider
provider "aws" {
  region = "us-east-1"
  default_tags {
    tags = var.proton_tags
  }
}
```

```
resource "aws_ssm_parameter" "my_ssm_parameter" {
  name  = "my_ssm_parameter"
  type  = "String"
  // Use the Proton environment.inputs. namespace
  value = var.environment.inputs.ssm_parameter_value
}
```

dev/proton.environment.variables.tf:

```
variable "environment" {
  type = object({
    inputs = map(string)
    name = string
  })
}

variable "proton_tags" {
  type = map(string)
  default = null
}
```

dev/proton.auto.tfvars.json:

```
{
  "environment": {
    "name": "dev",
    "inputs": {
      "ssm_parameter_value": "MyNewParamValue"
    }
  }

  "proton_tags" : {
    "proton:account" : "123456789012",
    "proton:template" : "arn:aws:proton:us-east-1:123456789012:environment-template/
fargate-env",
    "proton:environment" : "arn:aws:proton:us-east-1:123456789012:environment/dev"
  }
}
```

Repository-Pfade

AWS Proton verwendet Konsolen- oder Spezifikationseingaben aus Umgebungs- oder Serviceerstellungsaktionen, um das Repository und den Pfad zu finden, in dem die kompilierten IaC-Dateien gespeichert werden sollen. Die Eingabewerte werden an die Namespace-Eingabeparameter übergeben.

AWS Proton unterstützt zwei Repository-Pfadlayouts. In den folgenden Beispielen werden die Pfade nach den Ressourcenparametern im Namespace aus zwei Umgebungen benannt. Jede Umgebung verfügt über Service-Instances von zwei Services, und die Service-Instances eines der Services verfügen über direkt definierte Komponenten.

Ressourcentyp	Name-Parameter	=	Ressourcennname
Umgebung	`environment.name`		`"env-prod"`
Umgebung	`environment.name`		`"env-staged"`
Service	`service.name`		`"service-one"`
Service-Instance	`service_instance.name`	=	`"instance-one-prod"`
Service-Instance	`service_instance.name`		`"instance-one-staged"`
Service	`service.name`		`"service-two"`
Service-Instance	`service_instance.name`		`"instance-two-prod"`

Ressourcentyp	Name-Parameter	=	Ressourcennname
Komponente	`service_instance.components.default.name`		`"component-prod"`
Service-Instance	`service_instance.name`		`"instance-two-staged"`
Komponente	`service_instance.components.default.name`		`"component-staged"`

Layout 1

Wenn das angegebene Repository mit einem -`environments`Ordner AWS Proton findet, wird ein Ordner erstellt, der die kompilierten IaC-Dateien enthält und mit dem benannt ist`environment.name`.

Wenn das angegebene Repository mit einem -`environments`Ordner AWS Proton findet, der einen Ordnernamen enthält, der mit einem mit der Service-Instance kompatiblen Umgebungsnamen übereinstimmt, erstellt es einen Ordner, der die kompilierten IaC-Dateien enthält und mit dem benannt ist`service_instance.name`.

```
/repo
    /environments
        /env-prod                               # environment folder
            main.tf
            proton.environment.variables.tf
            proton.auto.tfvars.json

            /service-one-instance-one-prod    # instance folder
                main.tf
                proton.service_instance.variables.tf
                proton.auto.tfvars.json

            /service-two-instance-two-prod    # instance folder
                main.tf
                proton.service_instance.variables.tf
```

```
            proton.auto.tfvars.json

        /component-prod                  # component folder
            main.tf
            proton.component.variables.tf
            proton.auto.tfvars.json

    /env-staged                          # environment folder
        main.tf
        proton.variables.tf
        proton.auto.tfvars.json

        /service-one-instance-one-staged  # instance folder
            main.tf
            proton.service_instance.variables.tf
            proton.auto.tfvars.json

        /service-two-instance-two-staged  # instance folder
            main.tf
            proton.service_instance.variables.tf
            proton.auto.tfvars.json

        /component-staged                # component folder
            main.tf
            proton.component.variables.tf
            proton.auto.tfvars.json
```

Layout 2

Wenn das angegebene Repository ohne -`environments`Ordner AWS Proton findet, wird ein -`environment.name`Ordner erstellt, in dem es die kompilierten IaC-Dateien der Umgebung findet.

Wenn das angegebene Repository mit einem Ordnernamen AWS Proton findet, der mit einem mit der Service-Instance kompatiblen Umgebungsnamen übereinstimmt, erstellt es einen `service_instance.name` Ordner, in dem es die kompilierten IaC-Dateien sucht.

```
/repo
    /env-prod                            # environment folder
        main.tf
        proton.environment.variables.tf
        proton.auto.tfvars.json
```

```
        /service-one-instance-one-prod    # instance folder
            main.tf
            proton.service_instance.variables.tf
            proton.auto.tfvars.json

        /service-two-instance-two-prod    # instance folder
            main.tf
            proton.service_instance.variables.tf
            proton.auto.tfvars.json

        /component-prod                   # component folder
            main.tf
            proton.component.variables.tf
            proton.auto.tfvars.json

    /env-staged                           # environment folder
        main.tf
        proton.variables.tf
        proton.auto.tfvars.json

        /service-one-instance-one-staged  # instance folder
            main.tf
            proton.service_instance.variables.tf
            proton.auto.tfvars.json

        /service-two-instance-two-staged  # instance folder
            main.tf
            proton.service_instance.variables.tf
            proton.auto.tfvars.json

        /component-staged                 # component folder
            main.tf
            proton.component.variables.tf
            proton.auto.tfvars.json
```

Schemadatei

Wenn Sie als Administrator den Abschnitt API-Datenmodelle (Schemas) öffnen verwenden, um eine YAML-Datei für das Parameterschema für Ihr Vorlagenpaket zu definieren, AWS Proton kann Parameterwerteingaben anhand der Anforderungen validieren, die Sie in Ihrem Schema definiert haben.

Weitere Informationen zu Formaten und verfügbaren Schlüsselwörtern finden Sie im Abschnitt Schemaobjekt der OpenAPI .

Schemaanforderungen für Umgebungsvorlagenpakete

Ihr Schema muss dem Abschnitt Datenmodelle (Schemas) der OpenAPI im YAML-Format folgen. Sie muss auch Teil Ihres Umgebungsvorlagenpakets sein.

Für Ihr Umgebungsschema müssen Sie die formatierten Header einschließen, um festzustellen, ob Sie den Abschnitt Datenmodelle (Schemas) der Open API verwenden. In den folgenden Beispielen für Umgebungsschemata werden diese Header in den ersten drei Zeilen angezeigt.

Ein `environment_input_type` muss enthalten und mit einem von Ihnen angegebenen Namen definiert sein. In den folgenden Beispielen ist dies in Zeile 5 definiert. Durch die Definition dieses Parameters verknüpfen Sie ihn mit einer AWS Proton Umgebungsressource.

Um dem Open API-Schemamodell zu folgen, müssen Sie einschließen`types`. Im folgenden Beispiel ist dies Zeile 6.

Im Anschluss an müssen `types`Sie einen -`environment_input_type`Typ definieren.
Sie definieren die Eingabeparameter für Ihre Umgebung als Eigenschaften des `environment_input_type`. Sie müssen mindestens eine Eigenschaft mit einem Namen einschließen, der mindestens einem Parameter entspricht, der in der IaC-Datei (Environment Infrastructure as Code) aufgeführt ist, die dem Schema zugeordnet ist.

Wenn Sie eine Umgebung erstellen und benutzerdefinierte Parameterwerte angeben, AWS Proton verwendet die Schemadatei, um sie abzugleichen, zu validieren und in die geschweiften Parameter in der zugehörigen CloudFormation IaC-Datei einzufügen. Geben Sie für jede Eigenschaft (Parameter) ein `name` und an`type`. Geben Sie optional auch `description``default`, und an`pattern`.

Zu den definierten Parametern für das folgende Beispiel für ein Standard-Umgebungsvorlagenschema gehören `vpc_cidr``subnet_one_cidr`, und `subnet_two_cidr` mit dem `default` Schlüsselwort und den Standardwerten. Wenn Sie eine Umgebung mit diesem Paketschema für Umgebungsvorlagen erstellen, können Sie die Standardwerte akzeptieren oder Ihre eigenen angeben. Wenn ein Parameter keinen Standardwert hat und als `required` Eigenschaft (Parameter) aufgeführt ist, müssen Sie Werte dafür angeben, wenn Sie eine Umgebung erstellen.

Das zweite Beispiel für ein Standard-Umgebungsvorlagenschema listet den `required` Parameter auf`my_other_sample_input`.

Sie können ein Schema für zwei Arten von Umgebungsvorlagen erstellen. Weitere Informationen finden Sie unter Vorlagen registrieren und veröffentlichen.

- Standard-Umgebungsvorlagen

  Im folgenden Beispiel wird ein Umgebungseingabetyp mit einer Beschreibung und Eingabeeigenschaften definiert. Dieses Schemabeispiel kann mit der in Beispiel 3 gezeigten AWS Proton CloudFormation IaC-Datei verwendet werden. ???

  Beispielschema für eine Standardumgebungsvorlage:

```
schema:                           # required
  format:                         # required
    openapi: "3.0.0"              # required
  # required              defined by administrator
  environment_input_type: "PublicEnvironmentInput"
  types:                          # required
    # defined by administrator
    PublicEnvironmentInput:
      type: object
      description: "Input properties for my environment"
      properties:
        vpc_cidr:                  # parameter
          type: string
          description: "This CIDR range for your VPC"
          default: 10.0.0.0/16
          pattern: ([0-9]{1,3}\.){3}[0-9]{1,3}($|/(16|24))
        subnet_one_cidr:           # parameter
          type: string
          description: "The CIDR range for subnet one"
          default: 10.0.0.0/24
          pattern: ([0-9]{1,3}\.){3}[0-9]{1,3}($|/(16|24))
        subnet_two_cidr:           # parameter
          type: string
          description: "The CIDR range for subnet one"
          default: 10.0.1.0/24
          pattern: ([0-9]{1,3}\.){3}[0-9]{1,3}($|/(16|24))
```

  Beispielschema für eine Standardumgebungsvorlage, die einen `required` Parameter enthält:

```
schema:                           # required
  format:                         # required
```

```
  openapi: "3.0.0"                # required
# required               defined by administrator
environment_input_type: "MyEnvironmentInputType"
types:                            # required
  # defined by administrator
  MyEnvironmentInputType:
    type: object
    description: "Input properties for my environment"
    properties:
      my_sample_input:            # parameter
        type: string
        description: "This is a sample input"
        default: "hello world"
      my_other_sample_input:      # parameter
        type: string
        description: "Another sample input"
      another_optional_input:     # parameter
        type: string
        description: "Another optional input"
        default: "!"
    required:
      - my_other_sample_input
```

- Vom Kunden verwaltete Umgebungsvorlagen

  Im folgenden Beispiel enthält das Schema nur eine Liste von Ausgaben, die die Ausgaben von dem IaC replizieren, den Sie zur Bereitstellung Ihrer vom Kunden verwalteten Infrastruktur verwendet haben. Sie müssen Ausgabewerttypen nur als Zeichenfolgen definieren (keine Listen, Arrays oder andere Typen). Der nächste Codeausschnitt zeigt beispielsweise den Abschnitt „Ausgaben“ einer externen AWS CloudFormation Vorlage. Dies stammt aus der Vorlage in Beispiel 1. Es kann verwendet werden, um eine externe vom Kunden verwaltete Infrastruktur für einen AWS Proton Fargate-Service zu erstellen, der aus Beispiel 4 erstellt wurde.

  > **Important**
  >
  > Als Administrator müssen Sie sicherstellen, dass Ihre bereitgestellte und verwaltete Infrastruktur und alle Ausgabeparameter mit den zugehörigen vom Kunden verwalteten Umgebungsvorlagen kompatibel sind. AWS Proton kann Änderungen in Ihrem Namen nicht berücksichtigen, da diese Änderungen für nicht sichtbar sind AWS Proton. Inkonsistenzen führen zu Fehlern.

Beispiel für CloudFormation IaC-Dateiausgaben für eine vom Kunden verwaltete Umgebungsvorlage:

```
// Cloudformation Template Outputs
[...]
Outputs:
  ClusterName:
    Description: The name of the ECS cluster
    Value: !Ref 'ECSCluster'
  ECSTaskExecutionRole:
    Description: The ARN of the ECS role
    Value: !GetAtt 'ECSTaskExecutionRole.Arn'
  VpcId:
    Description: The ID of the VPC that this stack is deployed in
    Value: !Ref 'VPC'
[...]
```

Das Schema für das entsprechende AWS Proton kundenverwaltete Umgebungsvorlagenpaket wird im folgenden Beispiel gezeigt. Jeder Ausgabewert ist als Zeichenfolge definiert.

Beispielschema für eine vom Kunden verwaltete Umgebungsvorlage:

```
schema:                           # required
  format:                         # required
    openapi: "3.0.0"              # required
  # required              defined by administrator
  environment_input_type: "EnvironmentOutput"
  types:                          # required
    # defined by administrator
    EnvironmentOutput:
      type: object
      description: "Outputs of the environment"
      properties:
        ClusterName:              # parameter
          type: string
          description: "The name of the ECS cluster"
        ECSTaskExecutionRole:     # parameter
          type: string
          description: "The ARN of the ECS role"
        VpcId:                    # parameter
          type: string
```

```
          description: "The ID of the VPC that this stack is deployed in"
[...]
```

Schemaanforderungen für Servicevorlagenpakete

Ihr Schema muss dem Abschnitt Datenmodelle (Schemas) der OpenAPI im YAML-Format folgen, wie in den folgenden Beispielen gezeigt. Sie müssen eine Schemadatei in Ihrem Servicevorlagenpaket bereitstellen.

In den folgenden Serviceschemabeispielen müssen Sie die formatierten Header einschließen. Im folgenden Beispiel befindet sich dies in den ersten drei Zeilen. Dadurch wird festgestellt, dass Sie den Abschnitt Datenmodelle (Schemas) der Open API verwenden.

Ein `service_input_type` muss enthalten und mit einem von Ihnen angegebenen Namen definiert sein. Im folgenden Beispiel befindet sich dies in Zeile 5. Dadurch werden die Parameter einer - AWS Proton Service-Ressource zugeordnet.

Eine - AWS Proton Service-Pipeline ist standardmäßig enthalten, wenn Sie die Konsole oder die CLI verwenden, um einen Service zu erstellen. Wenn Sie eine Service-Pipeline für Ihren Service einschließen, müssen Sie `pipeline_input_type` mit einem von Ihnen angegebenen Namen angeben. Im folgenden Beispiel befindet sich dies in Zeile 7. Fügen Sie diesen Parameter nicht ein, wenn Sie keine - AWS Proton Service-Pipeline einbeziehen. Weitere Informationen finden Sie unter Vorlagen registrieren und veröffentlichen.

Um dem Open API-Schemamodell zu folgen, müssen Sie `types` im folgenden Beispiel in Zeile 9 angeben.

Im Anschluss an müssen `types`Sie einen `service_input_type` Typ definieren. Sie definieren die Eingabeparameter für Ihren Service als Eigenschaften des `service_input_type`. Sie müssen mindestens eine Eigenschaft mit einem Namen einschließen, der mindestens einem Parameter entspricht, der in der IaC-Datei (Service Infrastructure as Code) aufgeführt ist, die dem Schema zugeordnet ist.

Um eine Service-Pipeline zu definieren, müssen Sie unter Ihrer `service_input_type` Definition eine definieren`pipeline_input_type`. Wie oben, müssen Sie mindestens eine Eigenschaft mit einem Namen einschließen, der mindestens einem Parameter entspricht, der in einer Pipeline-IaC-Datei aufgeführt ist, die dem Schema zugeordnet ist. Fügen Sie diese Definition nicht ein, wenn Sie keine - AWS Proton Service-Pipeline einbeziehen.

Wenn Sie als Administrator oder Entwickler einen Service erstellen und benutzerdefinierte Parameterwerte angeben, AWS Proton verwendet die Schemadatei, um sie abzugleichen, zu validieren und in die geschweiften Parameter der zugehörigen CloudFormation IaC-Datei einzufügen. Geben Sie für jede Eigenschaft (Parameter) ein `name` und ein `antype`. Geben Sie optional auch `descriptiondefault`, und an`pattern`.

Zu den definierten Parametern für das Beispielschema gehören `portdesired_count`, `task_size` und `image` mit dem `default` Schlüsselwort und den Standardwerten. Wenn Sie einen Service mit diesem Bundle-Schema für die Servicevorlage erstellen, können Sie die Standardwerte akzeptieren oder Ihre eigenen angeben. Der Parameter `unique_name` ist auch im Beispiel enthalten und hat keinen Standardwert. Sie wird als `required` Eigenschaft (Parameter) aufgeführt. Sie als Administrator oder Entwickler müssen Werte für `required` Parameter angeben, wenn Sie Services erstellen.

Wenn Sie eine Servicevorlage mit einer Service-Pipeline erstellen möchten, fügen Sie die `pipeline_input_type` in Ihr Schema ein.

Beispiel für eine Serviceschemadatei für einen Service, der eine - AWS Proton Service-Pipeline enthält.

Dieses Schemabeispiel kann mit den in Beispiel 4 und Beispiel 5 gezeigten AWS Proton IaC-Dateien verwendet werden. Eine Service-Pipeline ist enthalten.

```
schema:                           # required
  format:                         # required
    openapi: "3.0.0"              # required
  # required           defined by administrator
  service_input_type: "LoadBalancedServiceInput"
  # only include if including AWS Proton service pipeline, defined by administrator
  pipeline_input_type: "PipelineInputs"

  types:                          # required
    # defined by administrator
    LoadBalancedServiceInput:
      type: object
      description: "Input properties for a loadbalanced Fargate service"
      properties:
        port:                     # parameter
          type: number
          description: "The port to route traffic to"
          default: 80
          minimum: 0
```

```
        maximum: 65535
      desired_count:             # parameter
        type: number
        description: "The default number of Fargate tasks you want running"
        default: 1
        minimum: 1
      task_size:                 # parameter
        type: string
        description: "The size of the task you want to run"
        enum: ["x-small", "small", "medium", "large", "x-large"]
        default: "x-small"
      image:                     # parameter
        type: string
        description: "The name/url of the container image"
        default: "public.ecr.aws/z9d2n7e1/nginx:1.19.5"
        minLength: 1
        maxLength: 200
      unique_name:               # parameter
        type: string
        description: "The unique name of your service identifier. This will be used
to name your log group, task definition and ECS service"
        minLength: 1
        maxLength: 100
    required:
      - unique_name
  # defined by administrator
  PipelineInputs:
    type: object
    description: "Pipeline input properties"
    properties:
      dockerfile:                # parameter
        type: string
        description: "The location of the Dockerfile to build"
        default: "Dockerfile"
        minLength: 1
        maxLength: 100
      unit_test_command:         # parameter
        type: string
        description: "The command to run to unit test the application code"
        default: "echo 'add your unit test command here'"
        minLength: 1
        maxLength: 200
```

Wenn Sie eine Servicevorlage ohne Service-Pipeline erstellen möchten, schließen Sie die nicht `pipeline_input_type` in Ihr Schema ein, wie im folgenden Beispiel gezeigt.

Beispiel für eine Serviceschemadatei für einen Service, der keine - AWS Proton Service-Pipeline enthält

```
schema:                           # required
  format:                         # required
    openapi: "3.0.0"              # required
  # required            defined by administrator
  service_input_type: "MyServiceInstanceInputType"

  types:                          # required
    # defined by administrator
    MyServiceInstanceInputType:
      type: object
      description: "Service instance input properties"
      required:
        - my_sample_service_instance_required_input
      properties:
        my_sample_service_instance_optional_input:   # parameter
          type: string
          description: "This is a sample input"
          default: "hello world"
        my_sample_service_instance_required_input:   # parameter
          type: string
          description: "Another sample input"
```

Vorlagendateien für einpacken AWS Proton

Nachdem Sie Ihre Umgebungs- und Serviceinfrastruktur als Code (IaC)-Dateien und ihre jeweiligen Schemadateien vorbereitet haben, müssen Sie sie in Verzeichnissen organisieren. Sie müssen auch eine Manifest-YAML-Datei erstellen. Die Manifestdatei listet die IaC-Dateien in einem Verzeichnis, die Rendering-Engine und die Vorlagensprache auf, die zur Entwicklung des IaC in dieser Vorlage verwendet wurde.

> **Note**
>
> Eine Manifestdatei kann auch unabhängig von Vorlagenpaketen als direkte Eingabe für direkt definierte Komponenten verwendet werden. In diesem Fall wird immer eine einzelne

IaC-Vorlagendatei angegeben, sowohl für als auch für CloudFormation Terraform. Weitere Informationen zu Komponenten finden Sie unter Komponenten.

Die Manifestdatei muss dem im folgenden Beispiel gezeigten Format und Inhalt entsprechen.

CloudFormation Manifestdateiformat:

Mit listen CloudFormationSie eine einzelne Datei auf.

```
infrastructure:
  templates:
    - file: "cloudformation.yaml"
      rendering_engine: jinja
      template_language: cloudformation
```

Terraform-Manifestdateiformat:

Mit Terraform können Sie explizit eine einzelne Datei auflisten oder den Platzhalter verwenden*, um jede der Dateien in einem Verzeichnis aufzulisten.

> **Note**
>
> Der Platzhalter enthält nur Dateien, deren Namen mit enden.tf. Andere Dateien werden ignoriert.

```
infrastructure:
  templates:
    - file: "*"
      rendering_engine: hcl
      template_language: terraform
```

CodeBuild-basiertes Bereitstellungsmanifestdateiformat:

Bei der CodeBuild-basierten Bereitstellung geben Sie die Bereitstellung und Aufhebung der Bereitstellung von Shell-Befehlen an.

> **Note**
>
> Zusätzlich zum Manifest sollte Ihr Paket alle Dateien enthalten, von denen Ihre Befehle abhängen.

Das folgende Beispielmanifest verwendet die CodeBuild-basierte Bereitstellung, um Ressourcen mithilfe der () bereitzustellen AWS Cloud Development Kit (AWS CDK) (bereitzustellen) und bereitzustellen (zerstörenAWS CDK). Das Vorlagenpaket sollte auch den CDK-Code enthalten.

Während der Bereitstellung erstellt AWS Proton eine Eingabedatei mit Werten für Eingabeparameter, die Sie im Schema der Vorlage mit dem Namen definiert habenproton-input.json.

```
infrastructure:
  templates:
    - rendering_engine: codebuild
      settings:
        image: aws/codebuild/amazonlinux2-x86_64-standard:4.0
        runtimes:
          nodejs: 16
        provision:
          - npm install
          - npm run build
          - npm run cdk bootstrap
          - npm run cdk deploy -- --require-approval never --outputs-file proton-
outputs.json
          - jq 'to_entries | map_values(.value) | add | to_entries | map({key:.key,
 valueString:.value})' < proton-outputs.json > outputs.json
          - aws proton notify-resource-deployment-status-change --resource-arn
 $RESOURCE_ARN --status IN_PROGRESS --outputs file://./outputs.json
        deprovision:
          - npm install
          - npm run build
          - npm run cdk destroy
        project_properties:
          VpcConfig:
            VpcId: "{{ environment.inputs.codebuild_vpc_id }}"
            Subnets: "{{ environment.inputs.codebuild_subnets }}"
            SecurityGroupIds: "{{ environment.inputs.codebuild_security_groups }}"
```

Nachdem Sie die Verzeichnisse und Manifestdateien für Ihre Umgebung oder Ihr Servicevorlagenpaket eingerichtet haben, gzippen Sie die Verzeichnisse in einen Tarbium und laden sie in einen Amazon Simple Storage Service (Amazon S3)-Bucket hoch, in dem sie abrufen AWS Proton kann, oder in ein Git-Repository für die Vorlagensynchronisierung .

Wenn Sie eine Nebenversion einer Umgebung oder eine Servicevorlage erstellen, die Sie bei registriert haben AWS Proton, geben Sie den Pfad zu Ihrer Umgebung oder Ihrem Servicevorlagenpaket an, die sich in Ihrem S3-Bucket befindet. AWS Proton speichert sie mit der neuen Unterversion der Vorlage. Sie können die neue Unterversion der Vorlage auswählen, um Umgebungen oder Services mit zu erstellen oder zu aktualisieren AWS Proton.

Paketumbruch für Umgebungsvorlagen

Es gibt zwei Arten von Umgebungsvorlagen-Bundles, die Sie für erstellen AWS Proton.

- Um ein Umgebungsvorlagenpaket für eine Standardumgebungsvorlage zu erstellen, organisieren Sie die Schema-, Infrastructure as Code (IaC)-Dateien und die Manifestdatei in Verzeichnissen, wie in der folgenden Verzeichnisstruktur des Umgebungsvorlagenpakets gezeigt.
- Um ein Umgebungsvorlagenpaket für eine vom Kunden verwaltete Umgebungsvorlage zu erstellen, geben Sie nur die Schemadatei und das Verzeichnis an. Schließen Sie das Infrastrukturverzeichnis und files. AWS Proton throws keinen Fehler ein, wenn das Infrastrukturverzeichnis und die Dateien enthalten sind.

Weitere Informationen finden Sie unter Vorlagen registrieren und veröffentlichen.

CloudFormation Verzeichnisstruktur des Umgebungsvorlagen-Bundles:

```
/schema
  schema.yaml
/infrastructure
  manifest.yaml
  cloudformation.yaml
```

Verzeichnisstruktur des Terraform-Umgebungsvorlagen-Bundles:

```
/schema
  schema.yaml
/infrastructure
  manifest.yaml
```

```
  environment.tf
```

Paketumbruch der Servicevorlage

Um ein Servicevorlagenpaket zu erstellen, müssen Sie das Schema, die Infrastructure as Code (IaC)-Dateien und die Manifestdateien in Verzeichnissen organisieren, wie im Beispiel für die Verzeichnisstruktur des Servicevorlagenpakets gezeigt.

Wenn Sie keine Service-Pipeline in Ihr Vorlagenpaket aufnehmen, schließen Sie das Pipeline-Verzeichnis und die Dateien nicht ein und legen `"pipelineProvisioning": "CUSTOMER_MANAGED"` Sie beim Erstellen der Servicevorlage fest, die diesem Vorlagenpaket zugeordnet werden soll.

> **Note**
>
> Sie können nicht mehr ändern, `pipelineProvisioning` nachdem die Servicevorlage erstellt wurde.

Weitere Informationen finden Sie unter Vorlagen registrieren und veröffentlichen.

CloudFormation Verzeichnisstruktur des -Servicevorlagenpakets:

```
/schema
  schema.yaml
/instance_infrastructure
  manifest.yaml
  cloudformation.yaml
/pipeline_infrastructure
  manifest.yaml
  cloudformation.yaml
```

Verzeichnisstruktur des Terraform-Servicevorlagenpakets:

```
/schema
  schema.yaml
/instance_infrastructure
  manifest.yaml
  instance.tf
/pipeline_infrastructure
```

```
    manifest.yaml
    pipeline.tf
```

Überlegungen zum Vorlagenpaket

- Infrastructure as Code (IaC)-Dateien

  AWS Proton überprüft Vorlagen auf das richtige Dateiformat. AWS Proton Prüft jedoch nicht auf Vorlagenentwicklungs-, Abhängigkeits- und logische Fehler. Angenommen, Sie haben die Erstellung eines Amazon S3-Buckets in Ihrer AWS CloudFormation IaC-Datei als Teil Ihrer Service- oder Umgebungsvorlage angegeben. Basierend auf diesen Vorlagen wird ein Service erstellt. Angenommen, Sie möchten den Service irgendwann löschen. Wenn der angegebene S3-Bucket nicht leer ist und die CloudFormation IaC-Datei ihn nicht als `Retain` in der markiert`DeletionPolicy`, AWS Proton schlägt bei der Löschoperation des Services fehl.
- Beschränkungen und Format der Bundle-Dateigröße
  - Die Begrenzungen für Dateigröße, Anzahl und Namen finden Sie unter AWS Proton-Kontingente.
  - Die Verzeichnisse der Vorlagenpakete von Dateien werden in einen Teramon eingebunden und befinden sich in einem Amazon Simple Storage Service (Amazon S3)-Bucket.
  - Jede Datei im Paket muss eine gültige formatierte YAML-Datei sein.
- Verschlüsselung des S3-Bucket-Vorlagenpakets

  Wenn Sie sensible Daten in Ihren Vorlagenpaketen im Ruhezustand in Ihrem S3-Bucket verschlüsseln möchten, verwenden Sie SSE-S3- oder SSE-KMS-Schlüssel, um zu erlauben AWS Proton , sie abzurufen.

AWS Proton-Vorlagen

Um Ihr Vorlagenpaket zu IhrerAWS Proton Vorlagenbibliothek hinzuzufügen, erstellen Sie eine Vorlagen-Nebenversion und registrieren Sie sie beiAWS Proton. Geben Sie bei der Erstellung der Vorlage den Namen des Amazon S3 S3-Buckets und den Pfad für Ihr Vorlagenpaket ein. Nachdem die Vorlagen veröffentlicht wurden, können sie von Mitgliedern des Plattformteams und Entwicklern ausgewählt werden. AWS ProtonVerwendet die Vorlage, nachdem sie ausgewählt wurden, um Infrastruktur und Anwendungen zu erstellen und bereitzustellen.

Als Administrator können Sie eine Umgebungsvorlage erstellen und bei registrierenAWS Proton. Diese Umgebungsvorlage kann dann verwendet werden, um mehrere Umgebungen bereitzustellen. Es kann beispielsweise verwendet werden, um „dev“, „Staging“ und „Prod“ -Umgebungen bereitzustellen. Die „dev“ -Umgebung könnte eine VPC mit privaten Subnetzen und einer restriktiven Zugriffsrichtlinie für alle Ressourcen umfassen. Umgebungsausgänge können als Eingaben für Dienste verwendet werden.

Sie können Umgebungsvorlagen erstellen und registrieren, um zwei verschiedene Arten von Umgebungen zu erstellen. Sowohl Sie als auch Entwickler könnenAWS Proton Dienste für beide Typen bereitstellen.

- Registrieren und veröffentlichen Sie eine Standardumgebungsvorlage,AWS Proton mit der eine Standardumgebung erstellt wird, die die Umgebungsinfrastruktur bereitstellt und verwaltet.
- Registrieren und veröffentlichen Sie eine Vorlage für eine vom Kunden verwaltete Umgebung, dieAWS Proton verwendet wird, um eine vom Kunden verwaltete Umgebung zu erstellen, die eine Verbindung zu Ihrer vorhandenen bereitgestellten Infrastruktur herstellt. AWS Protonverwaltet Ihre bestehende bereitgestellte Infrastruktur nicht.

Sie können Dienstvorlagen erstellen und registrierenAWS Proton, um Dienste in Umgebungen bereitzustellen. EineAWS Proton Umgebung muss erstellt werden, bevor ein Dienst in ihr bereitgestellt werden kann.

In der folgenden Liste wird beschrieben, wie Sie Vorlagen mit erstellen und verwaltenAWS Proton.

- (Optional) Bereiten Sie eine IAM-Rolle vor, um den Zugriff der Entwickler aufAWS Proton API-Aufrufe undAWS Proton IAM-Servicerollen zu kontrollieren. Weitere Informationen finden Sie unter the section called “IAM-Rollen”.
- Stellen Sie ein Vorlagenpaket zusammen. Weitere Informationen finden Sie unter Vorlagenpakete.

- Erstellen und registrieren Sie eine Vorlage mit,AWS Proton nachdem das Vorlagenpaket zusammengestellt, komprimiert und in einem Amazon S3 S3-Bucket gespeichert wurde. Dies können Sie entweder in der Konsole oder über dieAWS CLI.
- Testen und verwenden Sie die Vorlage, umAWS Proton bereitgestellte Ressourcen zu erstellen und zu verwalten, nachdem sie registriert wurdeAWS Proton.
- Erstellen und verwalten Sie Haupt- und Nebenversionen der Vorlage während der gesamten Lebensdauer der Vorlage.

Sie können die Vorlagenversionen manuell oder mit Vorlagensynchronisierungskonfigurationen verwalten:

- Verwenden Sie dieAWS Proton Konsole undAWS CLI um eine neue Neben- oder Hauptversion zu erstellen.
- Erstellen Sie eine Konfiguration für die Vorlagensynchronisierung, mit derAWS Proton automatisch eine neue Neben- oder Hauptversion erstellt werden kann, wenn eine Änderung an Ihrem Vorlagenpaket in einem von Ihnen definierten Repository erkannt wird.

Weitere Informationen finden Sie in der TheAWS Proton Service API-Referenz.

Themen

Versionierte Vorlagen

Als Administrator oder Mitglied eines Plattformteams definieren, erstellen und verwalten Sie eine Bibliothek mit versionierten Vorlagen, die zur Bereitstellung von Infrastrukturressourcen verwendet werden. Es gibt zwei Arten von Vorlagenversionen: Nebenversionen und Hauptversionen.

- Nebenversionen — Änderungen an der Vorlage, die ein abwärtskompatibles Schema haben. Aufgrund dieser Änderungen muss der Entwickler beim Update auf die neue Vorlagenversion keine neuen Informationen angeben.

  Wenn Sie versuchen, eine geringfügige Versionsänderung vorzunehmenAWS Proton, versuchen Sie nach besten Kräften festzustellen, ob das Schema der neuen Version mit den vorherigen Nebenversionen der Vorlage abwärtskompatibel ist. Wenn das neue Schema nicht abwärtskompatibel ist,AWS Proton schlägt die Registrierung der neuen Nebenversion fehl.

  > **Note**
  >
  > Die Kompatibilität wird ausschließlich anhand des Schemas bestimmt. AWS Protonüberprüft nicht, ob die IaC-Datei (Template Bundle Infrastructure as Code) mit den vorherigen Nebenversionen abwärtskompatibel ist. Prüft beispielsweiseAWS Proton nicht, ob die neue IaC-Datei grundlegende Änderungen für die Anwendungen verursacht, die auf der Infrastruktur ausgeführt werden, die in einer früheren Nebenversion der Vorlage bereitgestellt wurde.

- Hauptversionen — Änderungen an der Vorlage, die möglicherweise nicht abwärtskompatibel sind. Diese Änderungen erfordern in der Regel neue Eingaben des Entwicklers und beinhalten häufig Änderungen des Vorlagenschemas.

  Manchmal entscheiden Sie sich manchmal dafür, eine abwärtskompatible Änderung auf der Grundlage des Betriebsmodells Ihres Teams als Hauptversion zu bezeichnen.

WieAWS Proton bestimmt wird, ob es sich bei einer Anforderung einer Vorlagenversion um eine Nebenversion oder eine Hauptversion handelt, hängt davon ab, wie Vorlagenänderungen nachverfolgt werden:

- Wenn Sie explizit die Erstellung einer neuen Vorlagenversion anfordern, fordern Sie eine Hauptversion an, indem Sie eine Hauptversionsnummer angeben, und Sie fordern eine Nebenversion an, indem Sie keine Hauptversionsnummer angeben.
- Wenn Sie die Vorlagensynchronisierung verwenden (und daher keine expliziten Anforderungen an die Vorlagenversion stellen), wirdAWS Proton versucht, neue Nebenversionen für Vorlagenänderungen zu erstellen, die in der vorhandenen YAML-Datei vorgenommen werden. AWS Protonerstellt eine Hauptversion, wenn Sie ein neues Verzeichnis für die neue Vorlagenänderung erstellen (z. B. von v1 zu v2 wechseln).

> **Note**
>
> Eine Registrierung einer neuen Nebenversion auf der Grundlage der Vorlagensynchronisierung schlägt immer noch fehl, wennAWS Proton festgestellt wird, dass die Änderung nicht abwärtskompatibel ist.

Wenn Sie eine neue Version einer Vorlage veröffentlichen, wird sie zur empfohlenen Version, wenn es sich um die höchste Haupt- und Nebenversion handelt. NeueAWS Proton Ressourcen werden mit der neuen empfohlenen Version erstellt und Administratoren werdenAWS Proton aufgefordert, die neue Version zu verwenden und vorhandeneAWS Proton Ressourcen zu aktualisieren, die eine veraltete Version verwenden.

Vorlagen registrieren und veröffentlichen

Sie können Umgebungs- und Dienstvorlagen mit registrieren und veröffentlichenAWS Proton, wie in den folgenden Abschnitten beschrieben.

Sie können eine neue Version einer Vorlage mit der Konsole oderAWS CLI.

Alternativ können Sie die Konsole verwenden oderAWS CLI um eine Vorlage zu erstellen und eine Vorlagensynchronisierung dafür zu konfigurieren. Diese Konfiguration ermöglicht dieAWS Proton Synchronisierung von Template-Bundles aus, die sich in registrierten Git-Repositorys befinden, die Sie definiert haben. Immer wenn ein Commit in dein Repository übertragen wird, das eines deiner Template-Bundles ändert, wird eine neue Neben- oder Hauptversion deiner Vorlage erstellt, sofern die Version noch nicht existiert. Weitere Informationen zu den Konfigurationsvoraussetzungen und Anforderungen für die Vorlagensynchronisierung finden Sie unterKonfigurationen für die Vorlagensynchronisierung.

Umgebungsvorlagen registrieren und veröffentlichen

Sie können die folgenden Arten von Umgebungsvorlagen registrieren und veröffentlichen.

- Registrieren und veröffentlichen Sie eine Standardumgebungsvorlage, die für die Bereitstellung und Verwaltung der UmgebungsinfrastrukturAWS Proton verwendet wird.
- Registrieren und veröffentlichen Sie eine Vorlage für eine vom Kunden verwaltete UmgebungAWS Proton, mit der Sie eine Verbindung zu Ihrer vorhandenen bereitgestellten Infrastruktur herstellen, die Sie verwalten. AWS Protonverwaltet Ihre bestehende bereitgestellte Infrastruktur nicht.

> **Important**
>
> Stellen Sie als Administrator sicher, dass Ihre bereitgestellte und verwaltete Infrastruktur und alle Ausgabeparameter mit den zugehörigen, vom Kunden verwalteten Umgebungsvorlagen kompatibel sind. AWS Protonkann Änderungen in Ihrem Namen nicht berücksichtigen, da diese Änderungen für nicht sichtbar sindAWS Proton. Inkonsistenzen führen zu Fehlern.

Sie können die Konsole oder die verwendenAWS CLI, um eine Umgebungsvorlage zu registrieren und zu veröffentlichen.

AWS Management Console

Verwenden Sie die Konsole, um eine neue Umgebungsvorlage zu registrieren und zu veröffentlichen.

1. Wählen Sie in der AWS ProtonKonsole Umgebungsvorlagen aus.
2. Wählen Sie Umgebungsvorlage erstellen.
3. Wählen Sie auf der Seite Umgebungsvorlage erstellen im Abschnitt Vorlagenoptionen eine der beiden verfügbaren Vorlagenoptionen aus.
   - Erstellen Sie eine Vorlage für die Bereitstellung neuer Umgebungen.
   - Erstellen Sie eine Vorlage, um die bereitgestellte Infrastruktur zu verwenden, die Sie verwalten.
4. Wenn Sie Vorlage für die Bereitstellung neuer Umgebungen erstellen ausgewählt haben, wählen Sie im Abschnitt Quelle des Vorlagenpakets eine der drei verfügbaren Quellenoptionen für das Vorlagenpaket aus. Weitere Informationen zu den Anforderungen und Voraussetzungen für die Synchronisierung von Vorlagen finden Sie unterKonfigurationen für die Vorlagensynchronisierung.
   - Verwenden Sie eines unserer Beispielvorlagenpakete.
   - Verwenden Sie Ihr eigenes Vorlagenpaket.
   - Synchronisiere Vorlagen aus Git.
5. Geben Sie einen Pfad zu einem Vorlagenpaket an.
   a. Wenn Sie sich für „Verwenden Sie eines unserer Beispielvorlagenpakete“ entschieden haben:

Wählen Sie im Abschnitt Beispielvorlagenpaket ein Beispielvorlagenpaket aus.

b. Wenn du „Vorlagen von Git synchronisieren“ ausgewählt hast, gehe im Abschnitt Quellcode wie folgt vor:

   i. Wählen Sie das Repository für Ihre Vorlagensynchronisierungskonfiguration aus.

   ii. Geben Sie den Namen des Repository-Zweigs ein, von dem aus synchronisiert werden soll.

   iii. (Optional) Geben Sie den Namen eines Verzeichnisses ein, um die Suche nach Ihrem Vorlagenpaket einzuschränken.

c. Andernfalls geben Sie im Abschnitt Speicherort des S3-Bundles einen Pfad zu Ihrem Vorlagenpaket an.

6. Im Abschnitt Vorlagendetails.

   a. Geben Sie einen Vorlagennamen ein.

   b. (Optional) Geben Sie einen Display name (Anzeigenamen) für die Vorlage ein.

   c. (Optional) Geben Sie eine Beschreibung der Vorlage für die Umgebungsvorlage ein.

7. (Optional) Aktivieren Sie das Kontrollkästchen für Verschlüsselungseinstellungen anpassen (erweitert) im Abschnitt Verschlüsselungseinstellungen, um Ihren eigenen Verschlüsselungsschlüssel anzugeben.

8. (Optional) Wählen Sie im Abschnitt „Tags“ die Option „Neues Tag hinzufügen“ und geben Sie einen Schlüssel und einen Wert ein, um ein vom Kunden verwaltetes Tag zu erstellen.

9. Wählen Sie Create Environment Template.

   Sie befinden sich jetzt auf einer neuen Seite, auf der der Status und die Details für Ihre neue Umgebungsvorlage angezeigt werden. Zu diesen Details gehören eine Liste vonAWS und vom Kunden verwalteten Tags. AWS Protongeneriert automatischAWS verwaltete Tags für Sie, wenn SieAWS Proton Ressourcen erstellen. Weitere Informationen finden Sie unter AWS ProtonRessourcen und Tagging.

10. Der Status einer neuen Umgebungsvorlage beginnt im Status Entwurf. Sie und andere berechtigte`proton:CreateEnvironment` Personen können es einsehen und darauf zugreifen. Folgen Sie dem nächsten Schritt, um die Vorlage anderen zur Verfügung zu stellen.

11. Wählen Sie im Abschnitt Vorlagenversionen das Optionsfeld links neben der Nebenversion der Vorlage, die Sie gerade erstellt haben (1.0). Alternativ können Sie im Info-Alert die Option Veröffentlichen wählen und den nächsten Schritt überspringen.
12. Wählen Sie im Abschnitt Vorlagenversionen die Option Veröffentlichen aus.
13. Der Status der Vorlage ändert sich in Veröffentlicht. Da es sich um die neueste Version der Vorlage handelt, handelt es sich um die empfohlene Version.
14. Wählen Sie im Navigationsbereich Umgebungsvorlagen aus, um eine Liste Ihrer Umgebungsvorlagen und Details anzuzeigen.

Verwenden Sie die Konsole, um neue Haupt- und Nebenversionen einer Umgebungsvorlage zu registrieren.

Weitere Informationen finden Sie unter Versionierte Vorlagen.

1. Wählen Sie in der AWS ProtonKonsole Environment Templates aus.
2. Wählen Sie in der Liste der Umgebungsvorlagen den Namen der Umgebungsvorlage aus, für die Sie eine Haupt- oder Nebenversion erstellen möchten.
3. Wählen Sie in der Detailansicht der Umgebungsvorlage im Abschnitt Vorlagenversionen die Option Neue Version erstellen aus.
4. Wählen Sie auf der Seite Neue Umgebungsvorlagenversion erstellen im Abschnitt Quelle des Vorlagenpakets eine der beiden verfügbaren Quellenoptionen für das Vorlagenpaket aus.
   - Verwenden Sie eines unserer Beispielvorlagenpakete.
   - Verwenden Sie Ihr eigenes Vorlagenpaket.
5. Geben Sie einen Pfad zum ausgewählten Vorlagenpaket an.
   - Wenn Sie „Eines unserer Beispielvorlagenpakete verwenden“ ausgewählt haben, wählen Sie im Abschnitt Beispielvorlagenpaket ein Beispielvorlagenpaket aus.
   - Wenn Sie „Eigenes Vorlagenpaket verwenden“ ausgewählt haben, wählen Sie im Abschnitt Speicherort des S3-Bundles den Pfad zu Ihrem Vorlagenpaket aus.
6. Im Abschnitt Vorlagendetails.
   a. (Optional) Geben Sie einen Display name (Anzeigenamen) für die Vorlage ein.
   b. (Optional) Geben Sie eine Beschreibung der Vorlage für die Service-Vorlage ein.
7. Wählen Sie im Abschnitt Vorlagendetails eine der folgenden Optionen.

- Um eine Nebenversion zu erstellen, lassen Sie das Kontrollkästchen Häkchen, um eine neue Hauptversion zu erstellen, leer.
- Um eine Hauptversion zu erstellen, aktivieren Sie das Kontrollkästchen Aktivieren, um eine neue Hauptversion zu erstellen.

8. Fahren Sie mit den Konsolenschritten fort, um die neue Neben- oder Hauptversion zu erstellen, und wählen Sie Neue Version erstellen.

AWS CLI

Verwenden Sie die CLI, um eine neue Umgebungsvorlage zu registrieren und zu veröffentlichen, wie in den folgenden Schritten gezeigt.

1. Erstellen Sie eine standardmäßige Vorlage für eine vom Kunden verwaltete OR-Umgebung, indem Sie die Region, den Namen, den Anzeigenamen (optional) und die Beschreibung (optional) angeben.

   a. Erstellen Sie eine Standardumgebungsvorlage.

      Führen Sie den Befehl aus:

```
$ aws proton create-environment-template \
    --name "simple-env" \
    --display-name "Fargate" \
    --description "VPC with public access"
```

      Antwort:

```
{
    "environmentTemplate": {
        "arn": "arn:aws:proton:region-id:123456789012:environment-template/
simple-env",
        "createdAt": "2020-11-11T23:02:45.336000+00:00",
        "description": "VPC with public access",
        "displayName": "VPC",
        "lastModifiedAt": "2020-11-11T23:02:45.336000+00:00",
        "name": "simple-env"
    }
}
```

b. Erstellen Sie eine Vorlage für eine vom Kunden verwaltete Umgebung, indem Sie den`provisioning` Parameter mit dem Wert hinzufügen`CUSTOMER_MANAGED`.

Führen Sie den Befehl aus:

```
$ aws proton create-environment-template \
    --name "simple-env" \
    --display-name "Fargate" \
    --description "VPC with public access" \
    --provisioning "CUSTOMER_MANAGED"
```

Antwort:

```
{
    "environmentTemplate": {
        "arn": "arn:aws:proton:region-id:123456789012:environment-template/
simple-env",
        "createdAt": "2020-11-11T23:02:45.336000+00:00",
        "description": "VPC with public access",
        "displayName": "VPC",
        "lastModifiedAt": "2020-11-11T23:02:45.336000+00:00",
        "name": "simple-env",
        "provisioning": "CUSTOMER_MANAGED"
    }
}
```

2. Erstellen Sie eine Nebenversion 0 der Hauptversion 1 der Umgebungsvorlage

Dieser und die übrigen Schritte sind für die Standardvorlagen und die Vorlagen für die vom Kunden verwaltete Umgebung identisch.

Geben Sie den Vorlagennamen, die Hauptversion sowie den Namen und Schlüssel des S3-Buckets für den Bucket an, der Ihr Umgebungsvorlagenpaket enthält.

Führen Sie den Befehl aus:

```
$ aws proton create-environment-template-version \
    --template-name "simple-env" \
    --description "Version 1" \
    --source s3="{bucket=your_s3_bucket, key=your_s3_key}"
```

Antwort:

```
{
    "environmentTemplateVersion": {
        "arn": "arn:aws:proton:region-id:123456789012:environment-template/
simple-env:1.0",
        "createdAt": "2020-11-11T23:02:47.763000+00:00",
        "description": "Version 1",
        "lastModifiedAt": "2020-11-11T23:02:47.763000+00:00",
        "majorVersion": "1",
        "minorVersion": "0",
        "status": "REGISTRATION_IN_PROGRESS",
        "templateName": "simple-env"
    }
}
```

3. Verwenden Sie den Befehl get, um den Status der Registrierung zu überprüfen.

   Führen Sie den Befehl aus:

```
$ aws proton get-environment-template-version \
    --template-name "simple-env" \
    --major-version "1" \
    --minor-version "0"
```

   Antwort:

```
{
    "environment": {
        "arn": "arn:aws:proton:region-id:123456789012:environment-template/
simple-env:1.0",
        "createdAt": "2020-11-11T23:02:47.763000+00:00",
        "description": "Version 1",
        "lastModifiedAt": "2020-11-11T23:02:47.763000+00:00",
        "majorVersion": "1",
        "minorVersion": "0",
        "recommendedMinorVersion": "0",
        "schema": "schema:\n  format:\n    openapi: \"3.0.0\"\n
 environment_input_type: \"MyEnvironmentInputType\"\n  types:\n
 MyEnvironmentInputType:\n      type: object\n      description: \"Input
 properties for my environment\"\n      properties:\n        my_sample_input:\n
          type: string\n          description: \"This is a sample input\"\n
```

```
      default: \"hello world\"\n        my_other_sample_input:\n          type:
 string\n          description: \"Another sample input\"\n      required:\n
   - my_other_sample_input\n",
        "status": "DRAFT",
        "statusMessage": "",
        "templateName": "simple-env"
    }
}
```

4. Veröffentlichen Sie die Nebenversion 0 der Hauptversion 1 der Umgebungsvorlage, indem Sie den Vorlagennamen sowie die Haupt- und Nebenversion angeben. Diese Version ist die`Recommended` Version.

   Führen Sie den Befehl aus:

```
$ aws proton update-environment-template-version \
    --template-name "simple-env" \
    --major-version "1" \
    --minor-version "0" \
    --status "PUBLISHED"
```

   Antwort:

```
{
    "environmentTemplateVersion": {
        "arn": "arn:aws:proton:region-id:123456789012:environment-template/
simple-env:1.0",
        "createdAt": "2020-11-11T23:02:47.763000+00:00",
        "description": "Version 1",
        "lastModifiedAt": "2020-11-11T23:02:54.610000+00:00",
        "majorVersion": "1",
        "minorVersion": "0",
        "recommendedMinorVersion": "0",
        "schema": "schema:\n  format:\n    openapi: \"3.0.0\"\n
 environment_input_type: \"MyEnvironmentInputType\"\n  types:\n
 MyEnvironmentInputType:\n      type: object\n      description: \"Input
 properties for my environment\"\n      properties:\n        my_sample_input:\n
          type: string\n          description: \"This is a sample input\"\n
      default: \"hello world\"\n        my_other_sample_input:\n          type:
 string\n          description: \"Another sample input\"\n      required:\n
   - my_other_sample_input\n",
        "status": "PUBLISHED",
```

```
        "statusMessage": "",
        "templateName": "simple-env"
    }
}
```

Nachdem Sie mit dem eine neue Vorlage erstellt habenAWS CLI, können Sie sich eine Liste derAWS vom Kunden verwalteten Tags anzeigen lassen. AWS Protongeneriert automatischAWS verwaltete Tags für Sie. Sie können auch vom Kunden verwaltete Tags ändern und erstellen, indem Sie die verwendenAWS CLI. Weitere Informationen finden Sie unter AWS ProtonRessourcen und Tagging.

Führen Sie den Befehl aus:

```
$ aws proton list-tags-for-resource \
    --resource-arn "arn:aws:proton:region-id:123456789012:environment-
template/simple-env"
```

Service-Vorlagen registrieren und veröffentlichen

Wenn Sie eine Dienstvorlagenversion erstellen, geben Sie eine Liste kompatibler Umgebungsvorlagen an. Auf diese Weise haben Entwickler bei der Auswahl einer Service-Vorlage Optionen für die Umgebung, in der sie ihren Service bereitstellen möchten.

Bevor Sie einen Service anhand einer Service-Vorlage erstellen oder eine Service-Vorlage veröffentlichen, vergewissern Sie sich, dass Umgebungen anhand der aufgelisteten kompatiblen Umgebungsvorlagen bereitgestellt wurden.

Sie können einen Dienst nicht auf die neue Hauptversion aktualisieren, wenn er in einer Umgebung bereitgestellt wird, die auf der Grundlage einer entfernten kompatiblen Umgebungsvorlage erstellt wurde.

Um kompatible Umgebungsvorlagen für eine Dienstvorlagenversion hinzuzufügen oder zu entfernen, erstellen Sie eine neue Hauptversion davon.

Sie können die Konsole oder die verwendenAWS CLI, um eine Service-Vorlage zu registrieren und zu veröffentlichen.

AWS Management Console

Verwenden Sie die Konsole, um eine neue Service-Vorlage zu registrieren und zu veröffentlichen.

1. Wählen Sie in der AWS ProtonKonsole Service Templates aus.
2. Wählen Sie Create Service Template.
3. Wählen Sie auf der Seite Servicevorlage erstellen im Abschnitt Quelle des Vorlagenpakets eine der verfügbaren Vorlagenoptionen aus.
   - Verwenden Sie Ihr eigenes Vorlagenpaket.
   - Synchronisiere Vorlagen aus Git.
4. Geben Sie einen Pfad zu einem Vorlagenpaket an.
   a. Wenn du im Abschnitt Quellcode-Repository die Option Vorlagen von Git synchronisieren ausgewählt hast:
      i. Wählen Sie das Repository für Ihre Vorlagensynchronisierungskonfiguration aus.
      ii. Geben Sie den Namen des Repository-Zweigs ein, von dem aus synchronisiert werden soll.
      iii. (Optional) Geben Sie den Namen eines Verzeichnisses ein, um die Suche nach Ihrem Vorlagenpaket einzuschränken.
   b. Andernfalls geben Sie im Abschnitt Speicherort des S3-Bundles einen Pfad zu Ihrem Vorlagenpaket an.
5. Im Abschnitt Vorlagendetails.
   a. Geben Sie einen Vorlagennamen ein.
   b. (Optional) Geben Sie einen Display name (Anzeigenamen) für die Vorlage ein.
   c. (Optional) Geben Sie eine Beschreibung der Vorlage für die Service-Vorlage ein.
6. Wählen Sie im Abschnitt Kompatible Umgebungsvorlagen aus einer Liste kompatibler Umgebungsvorlagen aus.
7. (Optional) Wählen Sie im Abschnitt Verschlüsselungseinstellungen die Option Verschlüsselungseinstellungen anpassen (erweitert), um Ihren eigenen Verschlüsselungsschlüssel bereitzustellen.
8. (Optional) Im Abschnitt Pipeline:

Wenn Sie keine Service-Pipeline-Definition in Ihre Service-Vorlage aufnehmen, deaktivieren Sie das Kontrollkästchen Pipeline — optional unten auf der Seite. Sie können dies nicht ändern, nachdem die Service-Vorlage erstellt wurde. Weitere Informationen finden Sie unter Vorlagenpakete.

9. (Optional) Wählen Sie im Abschnitt Unterstützte Komponentenquellen für Komponentenquellen die Option Direkt definiert aus, um das Anhängen direkt definierter Komponenten an Ihre Service-Instanzen zu ermöglichen.
10. (Optional) Wählen Sie im Abschnitt „Tags“ die Option „Neues Tag hinzufügen“ und geben Sie einen Schlüssel und einen Wert ein, um ein vom Kunden verwaltetes Tag zu erstellen.
11. Wählen Sie Create a service template.

    Sie befinden sich jetzt auf einer neuen Seite, auf der der Status und die Details für Ihre neue Service-Vorlage angezeigt werden. Zu diesen Details gehören eine Liste vonAWS und vom Kunden verwalteten Tags. AWS Protongeneriert automatischAWS verwaltete Tags für Sie, wenn SieAWS Proton Ressourcen erstellen. Weitere Informationen finden Sie unter AWS ProtonRessourcen und Tagging.
12. Der Status einer neuen Servicevorlage beginnt im Status Entwurf. Sie und andere berechtigte`proton:CreateService` Personen können es einsehen und darauf zugreifen. Folgen Sie dem nächsten Schritt, um die Vorlage anderen zur Verfügung zu stellen.
13. Wählen Sie im Abschnitt Vorlagenversionen das Optionsfeld links neben der Nebenversion der Vorlage, die Sie gerade erstellt haben (1.0). Alternativ können Sie im Info-Alert die Option Veröffentlichen wählen und den nächsten Schritt überspringen.
14. Wählen Sie im Abschnitt Vorlagenversionen die Option Veröffentlichen aus.
15. Der Status der Vorlage ändert sich in Veröffentlicht. Da es sich um die neueste Version der Vorlage handelt, handelt es sich um die empfohlene Version.
16. Wählen Sie im Navigationsbereich Dienstvorlagen aus, um eine Liste Ihrer Servicevorlagen und Details anzuzeigen.

Verwenden Sie die Konsole, um neue Haupt- und Nebenversionen einer Service-Vorlage zu registrieren.

Weitere Informationen finden Sie unter Versionierte Vorlagen.

1. Wählen Sie in der AWS ProtonKonsole Service Templates aus.

2. Wählen Sie in der Liste der Service-Vorlagen den Namen der Service-Vorlage aus, für die Sie eine Haupt- oder Nebenversion erstellen möchten.
3. Wählen Sie in der Detailansicht der Service-Vorlage im Abschnitt Vorlagenversionen die Option Neue Version erstellen aus.
4. Wählen Sie auf der Seite Neue Service-Vorlagenversion erstellen im Abschnitt Bundle-Quelle die Option Eigenes Vorlagenpaket verwenden aus.
5. Wählen Sie im Abschnitt Standort des S3-Bundles den Pfad zu Ihrem Vorlagenpaket aus.
6. Im Abschnitt Vorlagendetails.
   a. (Optional) Geben Sie einen Display name (Anzeigenamen) für die Vorlage ein.
   b. (Optional) Geben Sie eine Beschreibung der Vorlage für die Service-Vorlage ein.
7. Wählen Sie im Abschnitt Vorlagendetails eine der folgenden Optionen.
   - Um eine Nebenversion zu erstellen, lassen Sie das Kontrollkästchen Häkchen, um eine neue Hauptversion zu erstellen, leer.
   - Um eine Hauptversion zu erstellen, aktivieren Sie das Kontrollkästchen Aktivieren, um eine neue Hauptversion zu erstellen.
8. Fahren Sie mit den Konsolenschritten fort, um die neue Neben- oder Hauptversion zu erstellen, und wählen Sie Neue Version erstellen.

AWS CLI

Um eine Dienstvorlage zu erstellen, die einen Dienst ohne Dienstpipeline bereitstellt, fügen Sie dem`create-service-template` Befehl den Parameter und`--pipeline-provisioning "CUSTOMER_MANAGED"` den Wert hinzu. Konfigurieren Sie Ihre Vorlagenpakete wie unterVorlagenpakete Erstellung und beschriebenSchemaanforderungen für Servicevorlagenpakete.

> **Note**
>
> Sie können die Servicevorlage nicht mehr ändern,`pipelineProvisioning` nachdem sie erstellt wurde.

1. Verwenden Sie die CLI, um eine neue Service-Vorlage mit oder ohne Service-Pipeline zu registrieren und zu veröffentlichen, wie in den folgenden Schritten gezeigt.

   a. Erstellen Sie mithilfe der CLI eine Service-Vorlage mit einer Service-Pipeline.

      Geben Sie den Namen, den Anzeigenamen (optional) und die Beschreibung (optional) an.

      Führen Sie den Befehl aus:

```
$ aws proton create-service-template \
    --name "fargate-service" \
    --display-name "Fargate" \
    --description "Fargate-based Service"
```

      Antwort:

```
{
    "serviceTemplate": {
        "arn": "arn:aws:proton:region-id:123456789012:service-template/
fargate-service",
        "createdAt": "2020-11-11T23:02:55.551000+00:00",
        "description": "Fargate-based Service",
        "displayName": "Fargate",
        "lastModifiedAt": "2020-11-11T23:02:55.551000+00:00",
        "name": "fargate-service"
    }
}
```

   b. Erstellen Sie eine Service-Vorlage ohne Service-Pipeline.

      Fügen Sie `--pipeline-provisioning` hinzu.

      Führen Sie den Befehl aus:

```
$ aws proton create-service-template \
    --name "fargate-service" \
    --display-name "Fargate" \
    --description "Fargate-based Service" \
    --pipeline-provisioning "CUSTOMER_MANAGED"
```

      Antwort:

```
{
    "serviceTemplate": {
        "arn": "arn:aws:proton:region-id:123456789012:service-template/
fargate-service",
        "createdAt": "2020-11-11T23:02:55.551000+00:00",
        "description": "Fargate-based Service",
        "displayName": "Fargate",
        "lastModifiedAt": "2020-11-11T23:02:55.551000+00:00",
        "name": "fargate-service",
        "pipelineProvisioning": "CUSTOMER_MANAGED"
    }
}
```

2. Erstellen Sie eine Nebenversion 0 der Hauptversion 1 der Servicevorlage.

   Geben Sie den Vorlagennamen, die kompatiblen Umgebungsvorlagen, die Hauptversion sowie den Namen und Schlüssel des S3-Buckets für den Bucket an, der Ihr Service-Vorlagenpaket enthält.

   Führen Sie den Befehl aus:

```
$ aws proton create-service-template-version \
    --template-name "fargate-service" \
    --description "Version 1" \
    --source s3="{bucket=your_s3_bucket, key=your_s3_key}" \
    --compatible-environment-templates '[{"templateName":"simple-
env","majorVersion":"1"}]'
```

   Antwort:

```
{
    "serviceTemplateMinorVersion": {
        "arn": "arn:aws:proton:region-id:123456789012:service-template/fargate-
service:1.0",
        "compatibleEnvironmentTemplates": [
            {
                "majorVersion": "1",
                "templateName": "simple-env"
            }
        ],
        "createdAt": "2020-11-11T23:02:57.912000+00:00",
```

```
        "description": "Version 1",
        "lastModifiedAt": "2020-11-11T23:02:57.912000+00:00",
        "majorVersion": "1",
        "minorVersion": "0",
        "status": "REGISTRATION_IN_PROGRESS",
        "templateName": "fargate-service"
    }
}
```

3. Verwenden Sie den Befehl get, um den Status der Registrierung zu überprüfen.

   Führen Sie den Befehl aus:

```
$ aws proton get-service-template-version \
    --template-name "fargate-service" \
    --major-version "1" \
    --minor-version "0"
```

   Antwort:

```
{
    "serviceTemplateMinorVersion": {
        "arn": "arn:aws:proton:us-east-1:123456789012:service-template/fargate-
service:1.0",
        "compatibleEnvironmentTemplates": [
            {
                "majorVersion": "1",
                "templateName": "simple-env"
            }
        ],
        "createdAt": "2020-11-11T23:02:57.912000+00:00",
        "description": "Version 1",
        "lastModifiedAt": "2020-11-11T23:02:57.912000+00:00",
        "majorVersion": "1",
        "minorVersion": "0",
        "schema": "schema:\n  format:\n    openapi: \"3.0.0\"\n
 pipeline_input_type: \"MyPipelineInputType\"\n  service_input_type:
 \"MyServiceInstanceInputType\"\n\n  types:\n    MyPipelineInputType:\n
    type: object\n      description: \"Pipeline input properties\"\n
 required:\n        - my_sample_pipeline_required_input\n      properties:\n
        my_sample_pipeline_optional_input:\n          type: string\n
   description: \"This is a sample input\"\n          default: \"hello world
```

```
\"\n        my_sample_pipeline_required_input:\n          type: string\n
     description: \"Another sample input\"\n\n    MyServiceInstanceInputType:
\n      type: object\n      description: \"Service instance input properties
\"\n      required:\n        - my_sample_service_instance_required_input\n
    properties:\n        my_sample_service_instance_optional_input:\n
   type: string\n          description: \"This is a sample input\"\n
 default: \"hello world\"\n        my_sample_service_instance_required_input:\n
         type: string\n          description: \"Another sample input\"",
        "status": "DRAFT",
        "statusMessage": "",
        "templateName": "fargate-service"
    }
}
```

4. Veröffentlichen Sie die Dienstvorlage, indem Sie den Befehl update verwenden, um den Status zu ändern"PUBLISHED".

   Führen Sie den Befehl aus:

```
$ aws proton update-service-template-version \
    --template-name "fargate-service" \
    --description "Version 1" \
    --major-version "1" \
    --minor-version "0" \
    --status "PUBLISHED"
```

   Antwort:

```
{
    "serviceTemplateVersion": {
        "arn": "arn:aws:proton:region-id:123456789012:service-template/fargate-
service:1.0",
        "compatibleEnvironmentTemplates": [
            {
                "majorVersion": "1",
                "templateName": "simple-env"
            }
        ],
        "createdAt": "2020-11-11T23:02:57.912000+00:00",
        "description": "Version 1",
        "lastModifiedAt": "2020-11-11T23:02:57.912000+00:00",
        "majorVersion": "1",
        "minorVersion": "0",
```

```
        "recommendedMinorVersion": "0",
        "schema": "schema:\n  format:\n    openapi: \"3.0.0\"\n
 pipeline_input_type: \"MyPipelineInputType\"\n  service_input_type:
 \"MyServiceInstanceInputType\"\n\n  types:\n    MyPipelineInputType:\n
    type: object\n      description: \"Pipeline input properties\"\n
 required:\n        - my_sample_pipeline_required_input\n      properties:\n
        my_sample_pipeline_optional_input:\n          type: string\n
 description: \"This is a sample input\"\n          default: \"hello pipeline
\"\n        my_sample_pipeline_required_input:\n          type: string\n
     description: \"Another sample input\"\n\n    MyServiceInstanceInputType:
\n      type: object\n      description: \"Service instance input properties
\"\n      required:\n        - my_sample_service_instance_required_input\n
    properties:\n        my_sample_service_instance_optional_input:\n
   type: string\n          description: \"This is a sample input\"\n
 default: \"hello world\"\n        my_sample_service_instance_required_input:\n
         type: string\n          description: \"Another sample input\"\n",
        "status": "PUBLISHED",
        "statusMessage": "",
        "templateName": "fargate-service"
    }
}
```

5. Überprüfen Sie, ob Version 1.0 veröffentlichtAWS Proton wurde, indem Sie den Befehl get verwenden, um die Detaildaten der Servicevorlage abzurufen.

   Führen Sie den Befehl aus:

```
$ aws proton get-service-template-version \
    --template-name "fargate-service" \
    --major-version "1" \
    --minor-version "0"
```

   Antwort:

```
{
    "serviceTemplateMinorVersion": {
        "arn": "arn:aws:proton:us-east-1:123456789012:service-template/fargate-
service:1.0",
        "compatibleEnvironmentTemplates": [
            {
                "majorVersion": "1",
                "templateName": "simple-env"
            }
```

```
        ],
        "createdAt": "2020-11-11T23:02:57.912000+00:00",
        "description": "Version 1",
        "lastModifiedAt": "2020-11-11T23:03:04.767000+00:00",
        "majorVersion": "1",
        "minorVersion": "0",
        "schema": "schema:\n  format:\n    openapi: \"3.0.0\"\n
 pipeline_input_type: \"MyPipelineInputType\"\n  service_input_type:
 \"MyServiceInstanceInputType\"\n\n  types:\n    MyPipelineInputType:\n
    type: object\n      description: \"Pipeline input properties\"\n
 required:\n        - my_sample_pipeline_required_input\n      properties:\n
        my_sample_pipeline_optional_input:\n          type: string\n
   description: \"This is a sample input\"\n          default: \"hello world
\"\n        my_sample_pipeline_required_input:\n          type: string\n
     description: \"Another sample input\"\n\n    MyServiceInstanceInputType:
\n      type: object\n      description: \"Service instance input properties
\"\n      required:\n        - my_sample_service_instance_required_input\n
    properties:\n        my_sample_service_instance_optional_input:\n
   type: string\n          description: \"This is a sample input\"\n
 default: \"hello world\"\n        my_sample_service_instance_required_input:\n
         type: string\n          description: \"Another sample input\"",
        "status": "PUBLISHED",
        "statusMessage": "",
        "templateName": "fargate-service"
    }
}
```


Vorlagendaten anzeigen

Mithilfe der AWS ProtonKonsole und können Sie sich Vorlagenlisten mit Details und einzelne Vorlagen mit Detaildaten anzeigen lassenAWS CLI.

Die Vorlagendaten für die vom Kunden verwaltete Umgebung enthalten den`provisioned` Parameter mit dem Wert`CUSTOMER_MANAGED`.

Wenn eine Service-Vorlage keine Service-Pipeline enthält, enthalten die Service-Vorlagendaten den`pipelineProvisioning` Parameter mit dem Wert`CUSTOMER_MANAGED`.

Weitere Informationen finden Sie unter Vorlagen registrieren und veröffentlichen.

Sie können die Konsole oder die verwendenAWS CLI, um Vorlagendaten aufzulisten und anzuzeigen.

AWS Management Console

Verwenden Sie die Konsole, um Vorlagen aufzulisten und anzuzeigen.

1. Um eine Liste der Vorlagen anzuzeigen, wählen Sie Vorlagen (Umgebung oder Service).
2. Um Detaildaten anzuzeigen, wählen Sie den Namen einer Vorlage.

   Sehen Sie sich die Detaildaten der Vorlage, eine Liste der Haupt- und Nebenversionen der Vorlage sowie eine Liste derAWS Proton Ressourcen an, die mithilfe von Vorlagenversionen und Vorlagen-Tags bereitgestellt wurden.

   Die empfohlene Hauptversion und Nebenversion sind als Empfohlen gekennzeichnet.

AWS CLI

Verwenden Sie dieAWS CLI, um Vorlagen aufzulisten und anzusehen.

Führen Sie den Befehl aus:

```
$ aws proton get-environment-template-version \
    --template-name "simple-env" \
    --major-version "1" \
    --minor-version "0"
```

Antwort:

```
{
    "environmentTemplateVersion": {
        "arn": "arn:aws:proton:region-id:123456789012:environment-template/simple-
env:1.0",
        "createdAt": "2020-11-10T18:35:08.293000+00:00",
        "description": "Version 1",
        "lastModifiedAt": "2020-11-10T18:35:11.162000+00:00",
        "majorVersion": "1",
        "minorVersion": "0",
        "recommendedMinorVersion": "0",
        "schema": "schema:\n  format:\n    openapi: \"3.0.0\"\n
 environment_input_type: \"MyEnvironmentInputType\"\n  types:\n
 MyEnvironmentInputType:\n      type: object\n      description: \"Input properties
 for my environment\"\n      properties:\n        my_sample_input:\n
  type: string\n          description: \"This is a sample input\"\n
 default: \"hello world\"\n        my_other_sample_input:\n          type: string
```

```
\n          description: \"Another sample input\"\n      required:\n        -
 my_other_sample_input\n",
        "status": "DRAFT",
        "statusMessage": "",
        "templateName": "simple-env"
    }
}
```

Führen Sie den Befehl aus:

```
$ aws proton list-environment-templates
```

Antwort:

```
{
    "templates": [
        {
            "arn": "arn:aws:proton:region-id:123456789012:environment-template/
simple-env-3",
            "createdAt": "2020-11-10T18:35:05.763000+00:00",
            "description": "VPC with Public Access",
            "displayName": "VPC",
            "lastModifiedAt": "2020-11-10T18:35:05.763000+00:00",
            "name": "simple-env-3",
            "recommendedVersion": "1.0"
        },
        {
            "arn": "arn:aws:proton:region-id:123456789012:environment-template/
simple-env-1",
            "createdAt": "2020-11-10T00:14:06.881000+00:00",
            "description": "Some SSM Parameters",
            "displayName": "simple-env-1",
            "lastModifiedAt": "2020-11-10T00:14:06.881000+00:00",
            "name": "simple-env-1",
            "recommendedVersion": "1.0"
        }
    ]
}
```

Sehen Sie sich eine Nebenversion einer Service-Vorlage an.

Führen Sie den Befehl aus:

```
$ aws proton get-service-template-version \
    --template-name "fargate-service" \
    --major-version "1" \
    --minor-version "0"
```

Antwort:


```
{
    "serviceTemplateMinorVersion": {
        "arn": "arn:aws:proton:us-east-1:123456789012:service-template/fargate-
service:1.0",
        "compatibleEnvironmentTemplates": [
            {
                "majorVersion": "1",
                "templateName": "simple-env"
            }
        ],
        "createdAt": "2020-11-11T23:02:57.912000+00:00",
        "description": "Version 1",
        "lastModifiedAt": "2020-11-11T23:02:57.912000+00:00",
        "majorVersion": "1",
        "minorVersion": "0",
        "schema": "schema:\n  format:\n    openapi: \"3.0.0\"\n
 pipeline_input_type: \"MyPipelineInputType\"\n  service_input_type:
 \"MyServiceInstanceInputType\"\n\n  types:\n    MyPipelineInputType:\n
    type: object\n      description: \"Pipeline input properties\"\n
 required:\n        - my_sample_pipeline_required_input\n      properties:\n
       my_sample_pipeline_optional_input:\n          type: string\n
 description: \"This is a sample input\"\n          default: \"hello world\"\n
  my_sample_pipeline_required_input:\n          type: string\n          description:
 \"Another sample input\"\n\n    MyServiceInstanceInputType:\n      type: object
\n      description: \"Service instance input properties\"\n      required:\n
       - my_sample_service_instance_required_input\n      properties:\n
 my_sample_service_instance_optional_input:\n          type: string\n
 description: \"This is a sample input\"\n          default: \"hello world\"\n
     my_sample_service_instance_required_input:\n          type: string\n
 description: \"Another sample input\"",
        "status": "DRAFT",
        "statusMessage": "",
        "templateName": "fargate-service"
    }
}
```

Zeigen Sie eine Dienstvorlage ohne Service-Pipeline an, wie im nächsten Beispiel für Befehl und Antwort gezeigt.

Führen Sie den Befehl aus:

```
$ aws proton get-service-template \
    --name "simple-svc-template-cli"
```

Antwort:

```
{
    "serviceTemplate": {
        "arn": "arn:aws:proton:region-id:123456789012:service-template/simple-svc-
template-cli",
        "createdAt": "2021-02-18T15:38:57.949000+00:00",
        "displayName": "simple-svc-template-cli",
        "lastModifiedAt": "2021-02-18T15:38:57.949000+00:00",
        "status": "DRAFT",
        "name": "simple-svc-template-cli",
        "pipelineProvisioning": "CUSTOMER_MANAGED"
    }
}
```

Einer Vorlage aktualisieren

Sie können eine Vorlage wie in der folgenden Liste beschrieben über die aktualisieren.

- Bearbeiten Sie das`description` oder`display name` einer Vorlage, wenn Sie entweder die Konsole oder verwendenAWS CLI. Sie können das*name* einer Vorlage nicht bearbeiten.
- Aktualisieren Sie den Status einer Template-Nebenversion, wenn Sie entweder die Konsole oderAWS CLI. Sie können den Status nur von`DRAFT` bis ändern`PUBLISHED`.
- Bearbeiten Sie den Anzeigenamen und die Beschreibung einer Neben- oder Hauptversion einer Vorlage, wenn Sie die verwendenAWS CLI.

AWS Management Console

Bearbeiten Sie eine Beschreibung und den Display name (Anzeigenamen) der Vorlage in der Konsole wie in den folgenden Schritten beschrieben.

In der Liste der Vorlagen.

1. Wählen Sie in der AWS ProtonKonsole Vorlagen (Umgebung oder Service) aus.
2. Wählen Sie in der Liste der Vorlagen das Optionsfeld links neben der Vorlage aus, für die Sie die Beschreibung oder den Anzeigenamen aktualisieren möchten.
3. Wählen Sie Aktionen und dann Bearbeiten.
4. Geben Sie auf der Seite Vorlage bearbeiten (Umgebung oder Dienst) im Abschnitt Vorlagendetails Ihre Änderungen in das Formular ein und wählen Sie Änderungen speichern.

Ändern Sie den Status einer Nebenversion einer Vorlage mithilfe der Konsole, um eine Vorlage wie im Folgenden beschrieben zu veröffentlichen. Sie können den Status nur von`DRAFT` bis ändern`PUBLISHED`.

Auf der Detailseite der Vorlage (Umgebung oder Service).

1. Wählen Sie in der AWS ProtonKonsole Vorlagen (Umgebung oder Service) aus.
2. Wählen Sie in der Liste der Vorlagen den Namen der Vorlage aus, für die Sie den Status einer Nebenversion von Entwurf auf Veröffentlicht aktualisieren möchten.
3. Wählen Sie auf der Detailseite der Vorlage (Umgebung oder Service) im Abschnitt Vorlagenversionen das Optionsfeld links neben der Nebenversion aus, die Sie veröffentlichen möchten.
4. Wählen Sie im Abschnitt Vorlagenversionen die Option Veröffentlichen. Der Status ändert sich von Entwurf zu Veröffentlicht.

AWS CLI

Der folgende Beispielbefehl und die folgende Antwort zeigen, wie Sie die Beschreibung einer Umgebungsvorlage bearbeiten können.

Führen Sie den folgenden Befehl aus.

```
$ aws proton update-environment-template \
    --name "simple-env" \
    --description "A single VPC with public access"
```

Antwort:

```
{
    "environmentTemplate": {
        "arn": "arn:aws:proton:region-id:123456789012:environment-template/simple-
env",
        "createdAt": "2020-11-28T22:02:10.651000+00:00",
        "description": "A single VPC with public access",
        "displayName": "simple-env",
        "lastModifiedAt": "2020-11-29T16:11:18.956000+00:00",
        "majorVersion": "1",
        "minorVersion": "0",
        "recommendedMinorVersion": "0",
        "schema": "schema:\n  format:\n    openapi: \"3.0.0\"\n
 environment_input_type: \"MyEnvironmentInputType\"\n  types:\n
 MyEnvironmentInputType:\n      type: object\n      description: \"Input properties
 for my environment\"\n      properties:\n        my_sample_input:\n
  type: string\n          description: \"This is a sample input\"\n
 default: \"hello world\"\n        my_other_sample_input:\n          type: string
\n          description: \"Another sample input\"\n      required:\n        -
 my_other_sample_input\n",
        "status": "PUBLISHED",
        "statusMessage": "",
        "templateName": "simple-env"
    }
}
```


Sie können die auch verwendenAWS CLI, um Servicevorlagen zu aktualisieren. In Schritt 5 finden SieService-Vorlagen registrieren und veröffentlichen ein Beispiel für die Aktualisierung des Status einer Nebenversion einer Service-Vorlage.

Löschen Sie Vorlagen

Vorlagen können mit der Konsole und gelöscht werdenAWS CLI.

Sie können eine Nebenversion einer Umgebungsvorlage löschen, wenn für diese Version keine Umgebungen bereitgestellt wurden.

Sie können eine Nebenversion einer Dienstvorlage löschen, wenn für diese Version keine Dienstinstanzen oder Pipelines bereitgestellt wurden. Ihre Pipeline kann in einer anderen Vorlagenversion als in Ihrer Service-Instance bereitgestellt werden. Wenn Ihre Dienstinstanz beispielsweise von 1.0 auf Version 1.1 aktualisiert wurde und Ihre Pipeline immer noch auf Version 1.0 bereitgestellt wird, können Sie die Service-Vorlage 1.0 nicht löschen.

AWS Management Console

Sie können die Konsole verwenden, um die gesamte Vorlage oder einzelne Neben- und Hauptversionen einer Vorlage zu löschen.

Verwenden Sie die Konsole, um Vorlagen wie folgt.

> **Note**
>
> Wenn Sie die Konsole zum Löschen von Vorlagen.
>
> - Wenn Sie die gesamte Vorlage löschen, löschen Sie auch die Haupt- und Nebenversionen der Vorlage.

In der Liste der Vorlagen (Umgebung oder Dienst).

1. Wählen Sie in der AWS ProtonKonsole Vorlagen (Umgebung oder Service) aus.
2. Wählen Sie in der Liste der Vorlagen das Optionsfeld links neben der Vorlage aus, die Sie löschen möchten.

   Sie können eine gesamte Vorlage nur löschen, wenn für ihre Versionen keineAWS Proton Ressourcen bereitgestellt wurden.
3. Wählen Sie Aktionen und dann Löschen, um die gesamte Vorlage zu löschen.
4. Ein Modal fordert Sie auf, den Löschvorgang zu bestätigen.
5. Folgen Sie den Anweisungen und wählen Sie Ja, löschen.

Auf der Detailseite der Vorlage (Umgebung oder Service).

1. Wählen Sie in der AWS ProtonKonsole Vorlagen (Umgebung oder Service) aus.
2. Wählen Sie in der Liste der Vorlagen den Namen der Vorlage aus, die Sie vollständig löschen möchten, oder löschen Sie einzelne Haupt- oder Nebenversionen davon.
3. Um die gesamte Vorlage zu löschen.

   Sie können eine gesamte Vorlage nur löschen, wenn für ihre Versionen keineAWS Proton Ressourcen bereitgestellt wurden.

   a. Wählen Sie Löschen in der oberen rechten Ecke der Seite.

b. Ein Modal fordert Sie auf, den Löschvorgang zu bestätigen.

c. Folgen Sie den Anweisungen und wählen Sie Ja, löschen.

4. Um Haupt- oder Nebenversionen einer Vorlage zu löschen.

   Sie können eine Nebenversion einer Vorlage nur löschen, wenn für diese Version keineAWS Proton Ressourcen bereitgestellt wurden.

   a. Wählen Sie im Abschnitt Vorlagenversionen das Optionsfeld links neben der Version aus, die Sie löschen möchten.

   b. Wählen Sie im Abschnitt Vorlagenversionen die Option Löschen.

   c. Ein Modal fordert Sie auf, den Löschvorgang zu bestätigen.

   d. Folgen Sie den Anweisungen und wählen Sie Ja, löschen.

AWS CLI

AWS CLIVorlagenlöschvorgänge beinhalten nicht das Löschen anderer Versionen einer Vorlage. Wenn Sie die verwendenAWS CLI, löschen Sie Vorlagen mit den folgenden Bedingungen.

- Löschen Sie eine gesamte Vorlage, wenn keine Neben- oder Hauptversionen der Vorlage vorhanden sind.
- Löschen Sie eine Hauptversion, wenn Sie die letzte verbleibende Nebenversion löschen.
- Löschen Sie eine Nebenversion einer Vorlage, wenn für diese Version keineAWS Proton Ressourcen bereitgestellt wurden.
- Löschen Sie die empfohlene Nebenversion einer Vorlage, wenn keine anderen Nebenversionen der Vorlage existieren und für diese Version keineAWS Proton Ressourcen bereitgestellt wurden.

Die folgenden Beispielbefehle und Antworten zeigen, wie Sie dieAWS CLI zum Löschen von Vorlagen verwenden.

Führen Sie den Befehl aus:

```
$ aws proton delete-environment-template-version \
    --template-name "simple-env" \
    --major-version "1" \
    --minor-version "0"
```

Antwort:

```
{
    "environmentTemplateVersion": {
        "arn": "arn:aws:proton:region-id:123456789012:environment-template/simple-
env:1.0",
        "createdAt": "2020-11-11T23:02:47.763000+00:00",
        "description": "Version 1",
        "lastModifiedAt": "2020-11-11T23:02:54.610000+00:00",
        "majorVersion": "1",
        "minorVersion": "0",
        "status": "PUBLISHED",
        "statusMessage": "",
        "templateName": "simple-env"
    }
}
```

Führen Sie den Befehl aus:

```
$ aws proton delete-environment-template \
    --name "simple-env"
```

Antwort:

```
{
    "environmentTemplate": {
        "arn": "arn:aws:proton:region-id:123456789012:environment-template/simple-
env",
        "createdAt": "2020-11-11T23:02:45.336000+00:00",
        "description": "VPC with Public Access",
        "displayName": "VPC",
        "lastModifiedAt": "2020-11-12T00:23:22.339000+00:00",
        "name": "simple-env",
        "recommendedVersion": "1.0"
    }
}
```

Führen Sie den Befehl aus:

```
$ aws proton delete-service-template-version \
    --template-name "fargate-service" \
```

```
    --major-version "1" \
    --minor-version "0"
```

Antwort:

```
{
    "serviceTemplateVersion": {
        "arn": "arn:aws:proton:region-id:123456789012:service-template/fargate-
service:1.0",
        "compatibleEnvironmentTemplates": [{"majorVersion": "1", "templateName":
 "simple-env"}],
        "createdAt": "2020-11-28T22:07:05.798000+00:00",
        "lastModifiedAt": "2020-11-28T22:19:05.368000+00:00",
        "majorVersion": "1",
        "minorVersion": "0",
        "status": "PUBLISHED",
        "statusMessage": "",
        "templateName": "fargate-service"
    }
}
```

Konfigurationen für die Vorlagensynchronisierung

Erfahren Sie, wie Sie eine Vorlage für die Vermietung konfigurierenAWS ProtonSynchronisieren Sie anhand von Vorlagenpaketen, die sich in registrierten Git-Repositorys befinden, die Sie definieren. Wenn ein Commit in dein Repository gepusht wird,AWS Protonsucht nach Änderungen an Ihren Repository-Vorlagenpaketen. Wenn es eine Änderung des Template-Bundles feststellt, wird eine neue Neben- oder Hauptversion seiner Vorlage erstellt, sofern die Version noch nicht existiert.AWS Protonunterstützt derzeitGitHub,GitHubEnterprise undBitBucket.

Einen Commit in ein synchronisiertes Template-Bundle übertragen

Wenn du einen Commit an einen Branch weiterleitest, der von einem deiner Templates verfolgt wird,AWS Protonklont dein Repository und bestimmt, welche Vorlagen es synchronisieren muss. Es durchsucht die Dateien in Ihrem Verzeichnis nach Verzeichnissen, die der Konvention von entsprechen`{template-name}/{major-version}/`.

DanachAWS Protonermittelt, welche Vorlagen und Hauptversionen mit Ihrem Repository und Branch verknüpft sind, und versucht, all diese Vorlagen parallel zu synchronisieren.

Bei jeder Synchronisation mit einer bestimmten VorlageAWS Protonprüft zunächst, ob sich der Inhalt des Vorlagenverzeichnisses seit der letzten erfolgreichen Synchronisierung geändert hat. Wenn sich der Inhalt nicht geändert hat,AWS Protonüberspringt die Registrierung eines doppelten Bundles. Dadurch wird sichergestellt, dass eine neue Vorlagennebenversion erstellt wird, wenn sich der Inhalt des Vorlagenpakets ändert. Wenn sich der Inhalt des Vorlagenpakets geändert hat, wird das Bundle bei registriertAWS Proton.

Nachdem das Vorlagenpaket registriert wurde,AWS Protonüberwacht den Registrierungsstatus, bis die Registrierung abgeschlossen ist.

Es kann jeweils nur eine Synchronisierung mit einer bestimmten Neben- und Hauptversion einer Vorlage erfolgen. Alle Commits, die während einer laufenden Synchronisierung möglicherweise per Push übertragen wurden, werden gebündelt. Die gebündelten Commits werden synchronisiert, nachdem der vorherige Synchronisierungsversuch abgeschlossen ist.

Dienstvorlagen werden synchronisiert

AWS Protonkann sowohl Umgebungs- als auch Dienstvorlagen aus Ihrem Git-Repository synchronisieren. Um Ihre Service-Vorlagen zu synchronisieren, fügen Sie eine zusätzliche Datei mit dem Namen hinzu`.template-registration.yaml`zu jedem Hauptversionsverzeichnis in Ihrem Vorlagenpaket. Diese Datei enthält zusätzliche Details, dieAWS Protonbenötigt, wenn es nach einem Commit eine Service-Template-Version für Sie erstellt:kompatible Umgebungenundunterstützte Komponentenquellen.

Der vollständige Pfad der Datei lautet*`service-template-name`*`/`*`major-version`*`/.template-registration.yaml`. Weitere Informationen finden Sie unter the section called “Synchronisieren von Dienstvorlagen”.

Überlegungen zur Konfiguration der Vorlagensynchronisierung

Lesen Sie die folgenden Überlegungen zur Verwendung von Vorlagensynchronisierungskonfigurationen.

- Repositorys dürfen nicht größer als 250 MB sein.
- Um die Vorlagensynchronisierung zu konfigurieren, verknüpfen Sie das Repository zunächst mitAWS Proton. Weitere Informationen finden Sie unter the section called “Erstellen eines Redie”.
- Wenn eine neue Vorlagenversion aus einer synchronisierten Vorlage erstellt wird, befindet sie sich im`DRAFT`Bundesstaat.

- Eine neue Nebenversion einer Vorlage wird erstellt, wenn eine der folgenden Bedingungen zutrifft:
  - Der Inhalt des Vorlagenpakets unterscheidet sich von dem Inhalt der letzten synchronisierten Vorlagennebenversion.
  - Die letzte zuvor synchronisierte Nebenversion der Vorlage wurde gelöscht.
- Die Synchronisierung kann nicht angehalten werden.
- Sowohl neue Neben- als auch Hauptversionen werden automatisch synchronisiert.
- Neue Vorlagen der obersten Ebene können nicht durch Konfigurationen zur Vorlagensynchronisierung erstellt werden.
- Mit einer Konfiguration zur Vorlagensynchronisierung können Sie nicht mit einer Vorlage aus mehreren Repositorys synchronisieren.
- Sie können keine Tags anstelle von Branches verwenden.
- Wenn dueine Dienstvorlage erstellen, geben Sie kompatible Umgebungsvorlagen an.
- Sie können eine Umgebungsvorlage erstellen und sie als kompatible Umgebung für Ihre Dienstvorlage im selben Commit hinzufügen.
- Synchronisierungen mit einer einzigen Hauptversion der Vorlage werden nacheinander ausgeführt. Wenn während einer Synchronisierung neue Commits erkannt werden, werden sie gebündelt und am Ende der aktiven Synchronisierung angewendet. Synchronisierungen mit verschiedenen Hauptversionen von Vorlagen erfolgen parallel.
- Wenn Sie den Branch ändern, von dem aus Ihre Vorlagen synchronisiert werden, werden alle laufenden Synchronisierungen aus dem alten Branch zuerst abgeschlossen. Dann beginnt die Synchronisierung mit dem neuen Zweig.
- Wenn Sie das Repository ändern, von dem aus Ihre Vorlagen synchronisiert werden, schlagen alle laufenden Synchronisierungen aus dem alten Repository möglicherweise fehl oder werden vollständig ausgeführt. Das hängt davon ab, in welcher Phase der Synchronisierung sie sich befinden.

Weitere Informationen finden Sie auf derDasAWS ProtonService-API-Referenz.

Themen

Erstellen Sie eine Konfiguration für die Vorlagensynchronisierung

Erfahren Sie, wie Sie eine Vorlagen-Synchronisierungskonfiguration mit erstellenAWS Proton.

Voraussetzungen für die Konfiguration der Vorlagensynchronisierung erstellen:

- Du hastein Repository verlinktmitAWS Proton.
- EINVorlagenpaketbefindet sich in Ihrem Repository.

Der Repository-Link besteht aus folgenden Elementen:

- EinCodeConnectionsVerbindung, die gibtAWS ProtonErlaubnis, auf Ihr Repository zuzugreifen und dessen Benachrichtigungen zu abonnieren.
- EINMit dem Dienst verknüpfte Rolle. Wenn Sie Ihr Repository verknüpfen, wird die mit dem Service verknüpfte Rolle für Sie erstellt.

Bevor Sie Ihre erste Konfiguration für die Vorlagensynchronisierung erstellen, übertragen Sie ein Vorlagenpaket in Ihr Repository, wie im folgenden Verzeichnislayout dargestellt.

```
/templates/                                                 # subdirectory (optional)
/templates/my-env-template/                                 # template name
/templates/my-env-template/v1/                              # template version
/templates/my-env-template/v1/infrastructure/               # template bundle
/templates/my-env-template/v1/schema/
```

Nachdem Sie Ihre erste Konfiguration für die Vorlagensynchronisierung erstellt haben, werden neue Vorlagenversionen automatisch erstellt, wenn Sie einen Commit pushen, der ein aktualisiertes Vorlagenpaket unter einer neuen Version hinzufügt (z. B. unter`/my-env-template/v2/`).

```
/templates/                                                 # subdirectory (optional)
/templates/my-env-template/                                 # template name
/templates/my-env-template/v1/                              # template version
/templates/my-env-template/v1/infrastructure/               # template bundle
/templates/my-env-template/v1/schema/
/templates/my-env-template/v2/
/templates/my-env-template/v2/infrastructure/
/templates/my-env-template/v2/schema/
```

Sie können neue Template-Bundle-Versionen für eine oder mehrere synchronisierte Vorlagen in einem einzigen Commit aufnehmen.AWS Protonerstellt eine neue Vorlagenversion für jede neue Version des Vorlagenpakets, die im Commit enthalten war.

Nachdem Sie die Konfiguration für die Vorlagensynchronisierung erstellt haben, können Sie immer noch manuell neue Versionen der Vorlage in der Konsole oder mit demAWS CLIindem Sie Vorlagenpakete aus einem S3-Bucket hochladen. Die Vorlagensynchronisierung funktioniert nur in eine Richtung: von Ihrem Repository zuAWS Proton. Manuell erstellte Vorlagenversionensind nichtsynchronisiert.

Nachdem Sie eine Konfiguration für die Vorlagensynchronisierung eingerichtet haben,AWS Protonwartet auf Änderungen an Ihrem Repository. Immer wenn eine Änderung übertragen wird, sucht es nach einem Verzeichnis, das den gleichen Namen wie Ihre Vorlage hat. Es sucht dann in diesem Verzeichnis nach Verzeichnissen, die wie Hauptversionen aussehen.AWS Protonregistriert das Vorlagenpaket für die entsprechende Hauptversion der Vorlage. Die neuen Versionen sind immer in derDRAFTBundesstaat. Du kannstdie neuen Versionen veröffentlichenmit der Konsole oderAWS CLI.

Nehmen wir zum Beispiel an, Sie haben eine Vorlage namens`my-env-template`konfiguriert für die Synchronisierung von`my-repo/templates`kein Zweig`main`mit dem folgenden Layout.

```
/code
/code/service.go
README.md
/templates/
/templates/my-env-template/
/templates/my-env-template/v1/
/templates/my-env-template/v1/infrastructure/
/templates/my-env-template/v1/schema/
/templates/my-env-template/v2/
/templates/my-env-template/v2/infrastructure/
/templates/my-env-template/v2/schema/
```

AWS Protonsynchronisiert den Inhalt von`/templates/my-env-template/v1/`zu`my-env-template:1`und der Inhalt von`/templates/my-env-template/v2/`zu`my-env-template:2`. Falls sie noch nicht existieren, werden diese Hauptversionen erstellt.

AWS Protonhat das erste Verzeichnis gefunden, das dem Vorlagennamen entsprach. Sie können die Verzeichnisse einschränkenAWS Protonsucht durch Angabe eines`subdirectoryPath`wenn

Sie eine Konfiguration für die Vorlagensynchronisierung erstellen oder bearbeiten. Sie können beispielsweise Folgendes angeben`/production-templates/zumsubdirectoryPath`.

Sie können eine Konfiguration für die Vorlagensynchronisierung mithilfe der Konsole oder der CLI erstellen.

AWS Management Console

Erstellen Sie mithilfe der Konsole eine Vorlage und eine Konfiguration für die Vorlagensynchronisierung.

1. In derAWS ProtonKonsole, wähleVorlagen für Umgebungen.
2. WähleUmgebungsvorlage erstellen.
3. In derUmgebungsvorlage erstellenSeite, in derOptionen für VorlagenAbschnitt, wählenErstellen Sie eine Vorlage für die Bereitstellung neuer Umgebungen.
4. In derQuelle des VorlagenpaketsAbschnitt, wählenSynchronisiere Vorlagen von Git.
5. In derQuellcode-RepositoryAbschnitt:
   a. FürEndlager, wählen Sie das verknüpfte Repository aus, das Ihr Vorlagenpaket enthält.
   b. FürFiliale, wählen Sie einen Repository-Zweig aus, von dem aus synchronisiert werden soll.
   c. (Fakultativ) FürVerzeichnis für Vorlagen-Pakete, geben Sie den Namen eines Verzeichnisses ein, um die Suche nach Ihrem Vorlagenpaket einzugrenzen.
6. ImDetails zur VorlageAbschnitt.
   a. Geben Sie einName der Vorlage.
   b. (Optional) Geben Sie einAnzeigename der Vorlage.
   c. (Optional) Geben Sie einBeschreibung der Vorlagefür die Umgebungsvorlage.
7. (Optional) Aktivieren Sie das Kontrollkästchen fürPassen Sie die Verschlüsselungseinstellungen an (erweitert)in derVerschlüsselungseinstellungenAbschnitt zur Bereitstellung Ihres eigenen Verschlüsselungsschlüssels.
8. (Optional) In derSchlagworteAbschnitt, wählenNeues Tag hinzufügenund geben Sie einen Schlüssel und einen Wert ein, um ein vom Kunden verwaltetes Tag zu erstellen.
9. WählenUmgebungsvorlage erstellen.

   Sie befinden sich jetzt auf einer neuen Seite, auf der der Status und die Details für Ihre neue Umgebungsvorlage angezeigt werden. Zu diesen Details gehört eine Liste vonAWSverwaltete

und vom Kunden verwaltete Tags.AWS Protongeneriert automatischAWSverwaltete Tags für Sie beim ErstellenAWS ProtonRessourcen. Weitere Informationen finden Sie unter AWS ProtonRessourcen und Tagging.

10. Wählen Sie auf der Detailseite der VorlageSynchronisierenRegisterkarte zum Anzeigen der Konfigurationsdetails für die Vorlagensynchronisierung.
11. Wählen SieVorlagenversionenRegisterkarte, um Vorlagenversionen mit Statusdetails anzuzeigen.
12. Der Status einer neuen Umgebungsvorlage beginnt imEntwurfBundesstaat. Du und andere mit`proton:CreateEnvironment`Berechtigungen können es einsehen und darauf zugreifen. Folgen Sie dem nächsten Schritt, um die Vorlage anderen zur Verfügung zu stellen.
13. In derVorlagenversionenWählen Sie im Abschnitt das Optionsfeld links neben der Nebenversion der Vorlage, die Sie gerade erstellt haben (1.0). Als Alternative können Sie wählenVeröffentlichenin der Informationswarnung und überspringen Sie den nächsten Schritt.
14. In derVorlagenversionenAbschnitt, wählen SieVeröffentlichen.
15. Der Status der Vorlage ändert sich zuVeröffentlicht. Es ist das neueste undEmpfohlenVersion der Vorlage.
16. Wählen Sie im NavigationsbereichVorlagen für Umgebungenum eine Liste Ihrer Umgebungsvorlagen und Details anzuzeigen.

Das Verfahren zum Erstellen einer Dienstvorlage und einer Konfiguration für die Vorlagensynchronisierung ist ähnlich.

AWS CLI

Erstellen Sie eine Vorlage und eine Konfiguration für die Vorlagensynchronisierung mithilfe derAWS CLI.

1. Erstellen Sie eine Vorlage. In diesem Beispiel wird eine Umgebungsvorlage erstellt.

   Führen Sie den folgenden Befehl aus.

   ```
   $ aws proton create-environment-template \
       --name "env-template"
   ```

   Die Antwort lautet wie folgt.

```
{
    "environmentTemplate": {
        "arn": "arn:aws:proton:us-east-1:123456789012:environment-template/env-
template",
        "createdAt": "2021-11-07T23:32:43.045000+00:00",
        "displayName": "env-template",
        "lastModifiedAt": "2021-11-07T23:32:43.045000+00:00",
        "name": "env-template",
        "status": "DRAFT",
        "templateName": "env-template"
    }
}
```

2. Erstellen Sie Ihre Template-Synchronisierungskonfiguration mitAWS CLIindem Sie Folgendes angeben:

   - Die Vorlage, mit der Sie synchronisieren möchten. Nachdem Sie die Konfiguration für die Vorlagensynchronisierung erstellt haben, können Sie daraus immer noch manuell in der Konsole oder mit demAWS CLI.
   - Der Name der Vorlage.
   - Der Vorlagentyp.
   - Das verknüpfte Repository, aus dem Sie synchronisieren möchten.
   - Der Anbieter des verknüpften Repositorys.
   - Der Zweig, in dem sich das Vorlagenpaket befindet.
   - (Optional) Der Pfad zu dem Verzeichnis, das Ihr Vorlagenpaket enthält. StandardmäßigAWS Protonsucht nach dem ersten Verzeichnis, das Ihrem Vorlagennamen entspricht.

   Führen Sie den folgenden Befehl aus.

```
$ aws proton create-template-sync-config \
    --template-name "env-template" \
    --template-type "ENVIRONMENT" \
    --repository-name "myrepos/templates" \
    --repository-provider "GITHUB" \
    --branch "main" \
    --subdirectory "env-template/"
```

Die Antwort lautet wie folgt.

```
{
    "templateSyncConfigDetails": {
        "branch": "main",
        "repositoryName": "myrepos/templates",
        "repositoryProvider": "GITHUB",
        "subdirectory": "templates",
        "templateName": "env-template",
        "templateType": "ENVIRONMENT"
    }
}
```

3. Informationen zum Veröffentlichen Ihrer Vorlagenversion finden Sie unterVorlagen registrieren und veröffentlichen.

Synchronisieren von Dienstvorlagen

Die vorherigen Beispiele zeigen, wie Sie Umgebungsvorlagen synchronisieren können. Dienstvorlagen sind ähnlich. Um Dienstvorlagen zu synchronisieren, fügen Sie eine zusätzliche Datei mit dem Namen hinzu`.template-registration.yaml`zu jedem Hauptversionsverzeichnis in Ihrem Vorlagenpaket. Diese Datei enthält zusätzliche Details, dieAWS Protonwird benötigt, wenn es nach einem Commit eine Service-Vorlagenversion für Sie erstellt. Wenn Sie explizit eine Service-Vorlagenversion mit demAWS ProtonKonsole oder API, Sie geben diese Details als Eingaben an, und diese Datei ersetzt diese Eingaben für die Vorlagensynchronisierung.

```
./templates/                                              # subdirectory (optional)
 /templates/my-svc-template/                              # service template name
 /templates/my-svc-template/v1/                           # service template version
 /templates/my-svc-template/v1/.template-registration.yaml   # service template version
 properties
 /templates/my-svc-template/v1/instance_infrastructure/      # template bundle
 /templates/my-svc-template/v1/schema/
```

Die`.template-registration.yaml`Die Datei enthält die folgenden Details:

- Kompatible Umgebungen[erforderlich] — Umgebungen, die auf diesen Umgebungsvorlagen und Hauptversionen basieren, sind mit Diensten kompatibel, die auf dieser Dienstvorlagenversion basieren.

- Unterstützte Komponentenquellen[optional] — Komponenten, die diese Quellen verwenden, sind mit Diensten kompatibel, die auf dieser Dienstvorlagenversion basieren. Wenn nicht angegeben, können Komponenten nicht an diese Dienste angehängt werden. Weitere Informationen zu Komponenten finden Sie unterKomponenten.

Die YAML-Syntax der Datei lautet wie folgt:

```
compatible_environments:
  - env-templ-name:major-version
  - ...
supported_component_sources:
  - DIRECTLY_DEFINED
```

Geben Sie eine oder mehrere Kombinationen aus Umgebungsvorlage und Hauptversion an. Spezifizierensupported_component_sourcesist optional, und der einzige unterstützte Wert istDIRECTLY_DEFINED.

Example .template-registration.yaml

In diesem Beispiel ist die Version der Dienstvorlage kompatibel mit den Hauptversionen 1 und 2 vonmy-env-templateUmgebungsvorlage. Es ist auch kompatibel mit den Hauptversionen 1 und 3 vonanother-env-templateVorlage für die Umgebung. Die Datei spezifiziert nichtsupported_component_sources, sodass Komponenten nicht an Dienste angehängt werden können, die auf dieser Dienstvorlagenversion basieren.

```
compatible_environments:
  - my-env-template:1
  - my-env-template:2
  - another-env-template:1
  - another-env-template:3
```

> **Note**
>
> BisherAWS Protonhat eine andere Datei definiert,.compatible-envs, um kompatible Umgebungen anzugeben.AWS Protonunterstützt diese Datei und ihr Format aus Gründen der Abwärtskompatibilität weiterhin. Wir empfehlen, es nicht mehr zu verwenden, da es nicht erweiterbar ist und neuere Funktionen wie Komponenten nicht unterstützt.

Konfigurationsdetails für die Vorlagensynchronisierung anzeigen

Zeigen Sie die Konfigurationsdetails zur Vorlagensynchronisierung mithilfe der Konsole oder der CLI an.

AWS Management Console

Verwenden Sie die Konsole, um die Konfigurationsdetails für die Vorlagensynchronisierung anzuzeigen.

1. Wählen Sie im NavigationsbereichVorlagen (Umgebung oder Dienst).
2. Um Detaildaten anzuzeigen, wählen Sie den Namen einer Vorlage, für die Sie eine Konfiguration zur Vorlagensynchronisierung erstellt haben.
3. Wählen Sie auf der Detailseite der Vorlage dieSynchronisierenRegisterkarte, um die detaillierten Konfigurationsdaten der Vorlagensynchronisierung anzuzeigen.

AWS CLI

Verwenden SieAWS CLIum eine synchronisierte Vorlage anzuzeigen.

Führen Sie den folgenden Befehl aus.

```
$ aws proton get-template-sync-config \
    --template-name "svc-template" \
    --template-type "SERVICE"
```

Die Antwort lautet wie folgt.

```
{
    "templateSyncConfigDetails": {
        "branch": "main",
        "repositoryProvider": "GITHUB",
        "repositoryName": "myrepos/myrepo",
        "subdirectory": "svc-template",
        "templateName": "svc-template",
        "templateType": "SERVICE"
    }
}
```

Benutze dieAWS CLIum den Status der Vorlagensynchronisierung abzurufen.

Für`template-version`, geben Sie die Hauptversion der Vorlage ein.

Führen Sie den folgenden Befehl aus.

```
$ aws proton get-template-sync-status \
    --template-name "env-template" \
    --template-type "ENVIRONMENT" \
    --template-version "1"
```

Bearbeiten Sie eine Konfiguration für die Vorlagensynchronisierung

Sie können alle Konfigurationsparameter für die Vorlagensynchronisierung bearbeiten, außer`template-name`und`template-type`.

Erfahren Sie, wie Sie eine Konfiguration für die Vorlagensynchronisierung mithilfe der Konsole oder der CLI bearbeiten.

AWS Management Console

Bearbeiten Sie einen Konfigurationszweig für die Vorlagensynchronisierung mithilfe der Konsole.

In der Liste der Vorlagen.

1. In derAWS ProtonKonsole, wähleVorlagen (Umgebung oder Service).
2. Wählen Sie in der Liste der Vorlagen den Namen der Vorlage mit der Vorlagensynchronisierungskonfiguration aus, die Sie bearbeiten möchten.
3. Wählen Sie auf der Detailseite der Vorlage dieVorlagensynchronisierungRegisterkarte.
4. In derDetails zur VorlagensynchronisierungAbschnitt, wählenBearbeiten.
5. In derBearbeitenSeite, in derQuellcode-RepositoryAbschnitt, fürFiliale, wählen Sie einen Zweig aus, und wählen Sie dannKonfiguration speichern.

AWS CLI

Der folgende Beispielbefehl und die folgende Antwort zeigen, wie Sie eine Vorlagensynchronisierungskonfiguration bearbeiten können**`branch`**mit der CLI.

Führen Sie den folgenden Befehl aus.

```
$ aws proton update-template-sync-config \
    --template-name "env-template" \
    --template-type "ENVIRONMENT" \
    --repository-provider "GITHUB" \
    --repository-name "myrepos/templates" \
    --branch "fargate" \
    --subdirectory "env-template"
```

Die Antwort lautet wie folgt.

```
{
    "templateSyncConfigDetails": {
        "branch": "fargate",
        "repositoryProvider": "GITHUB",
        "repositoryName": "myrepos/myrepo",
        "subdirectory": "templates",
        "templateName": "env-template",
        "templateType": "ENVIRONMENT"
    }
}
```

Sie können auf ähnliche Weise die verwendenAWS CLIum synchronisierte Dienstvorlagen zu aktualisieren.

Löschen Sie eine Konfiguration für die Vorlagensynchronisierung

Löschen Sie eine Konfiguration für die Vorlagensynchronisierung mithilfe der Konsole oder der CLI.

AWS Management Console

Löschen Sie eine Vorlagensynchronisierungskonfiguration mithilfe der Konsole.

1. Wählen Sie auf der Seite mit den Vorlagendetails dieSynchronisierenRegisterkarte.
2. In derDetails synchronisierenAbschnitt, wählenVerbindung trennen.

AWS CLI

Die folgenden Beispielbefehle und -antworten zeigen, wie SieAWS CLIum synchronisierte Vorlagenkonfigurationen zu löschen.

Führen Sie den folgenden Befehl aus.

```
$ aws proton delete-template-sync-config \
    --template-name "env-template" \
    --template-type "ENVIRONMENT"
```

Die Antwort lautet wie folgt.

```
{
    "templateSyncConfig": {
        "templateName": "env-template",
        "templateType": "ENVIRONMENT"
    }
}
```

Service-Synchronisationskonfigurationen

Mit Service Sync können Sie Ihre AWS Proton Dienste mithilfe von Git konfigurieren und bereitstellen. Sie können Service Sync verwenden, um erste Bereitstellungen und Updates für Ihren AWS Proton Service mit einer in einem Git-Repository definierten Konfiguration zu verwalten. Über Git kannst du Funktionen wie Versionsverfolgung und Pull-Requests verwenden, um deine Dienste zu konfigurieren, zu verwalten und bereitzustellen. Service Sync kombiniert AWS Proton Git, um Ihnen bei der Bereitstellung einer standardisierten Infrastruktur zu helfen, die anhand von AWS Proton Vorlagen definiert und verwaltet wird. Es verwaltet Servicedefinitionen in Ihrem Git-Repository und reduziert den Toolwechsel. Im Vergleich zur alleinigen Verwendung von Git können Sie durch die Standardisierung der Vorlagen und die Bereitstellung AWS Proton in weniger Zeit für die Verwaltung Ihrer Infrastruktur aufwenden. AWS Protonbietet außerdem eine höhere Transparenz und Überprüfbarkeit sowohl für Entwickler als auch für Plattformteams.

AWS ProtonOPS datei

Die `proton-ops` Datei definiert, wo AWS Proton sich die Spezifikationsdatei befindet, die zum Aktualisieren Ihrer Serviceinstanz verwendet wird. Es definiert auch, in welcher Reihenfolge Dienstinstanzen aktualisiert werden und wann Änderungen von einer Instanz auf eine andere übertragen werden sollen.

Die `proton-ops` Datei unterstützt das Synchronisieren einer Serviceinstanz mithilfe der Spezifikationsdatei oder mehrerer Spezifikationsdateien, die sich in Ihrem verknüpften Repository

befinden. Sie können dies tun, indem Sie einen Sync-Block in der `proton-ops` Datei definieren, wie im folgenden Beispiel.

Beispiel. /configuration/proton-ops.yaml:

```
sync:
  services:
      frontend-svc:
          alpha:
              branch: dev
              spec: ./frontend-svc/test/frontend-spec.yaml
          beta:
              branch: dev
              spec: ./frontend-svc/test/frontend-spec.yaml
          gamma:
              branch: pre-prod
              spec: ./frontend-svc/pre-prod/frontend-spec.yaml
          prod-one:
              branch: prod
              spec: ./frontend-svc/prod/frontend-spec-second.yaml
          prod-two:
              branch: prod
              spec: ./frontend-svc/prod/frontend-spec-second.yaml
          prod-three:
              branch: prod
              spec: ./frontend-svc/prod/frontend-spec-second.yaml
```

Im vorherigen Beispiel `frontend-svc` ist dies der Dienstname und`alpha`,`beta`,`gamma`, `prod-one`prod-two, und `prod-three` sind die Instanzen.

Bei der `spec` Datei kann es sich um alle Instanzen oder um eine Teilmenge der Instanzen handeln, die in der `proton-ops` Datei definiert sind. Es muss jedoch mindestens die Instanz innerhalb des Branches und die Spezifikation haben, von der aus sie synchronisiert wird. Wenn in der `proton-ops` Datei keine Instanzen mit dem spezifischen Zweig und dem Speicherort der `spec` Datei definiert sind, erstellt oder aktualisiert Service Sync diese Instanzen nicht.

Die folgenden Beispiele zeigen, wie die `spec` Dateien aussehen. Denken Sie daran, dass die `proton-ops` Datei aus diesen `spec` Dateien synchronisiert wird.

Beispiel**`./frontend-svc/test/frontend-spec.yaml`**:

```
proton: "ServiceSpec"
```

```
instances:
- name: "alpha"
  environment: "frontend-env"
  spec:
    port: 80
    desired_count: 1
    task_size: "x-small"
    image: "public.ecr.aws/z9d2n7e1/nginx:1.21.0"
- name: "beta"
  environment: "frontend-env"
  spec:
    port: 80
    desired_count: 1
    task_size: "x-small"
    image: "public.ecr.aws/z9d2n7e1/nginx:1.21.0"
```

Beispiel **`./frontend-svc/pre-prod/frontend-spec.yaml`**:

```
proton: "ServiceSpec"
instances:
- name: "gamma"
  environment: "frontend-env"
  spec:
    port: 80
    desired_count: 1
    task_size: "x-small"
    image: "public.ecr.aws/z9d2n7e1/nginx:1.21.0"
```

Beispiel **`./frontend-svc/prod/frontend-spec-second.yaml`**:

```
proton: "ServiceSpec"
instances:
- name: "prod-one"
  environment: "frontend-env"
  spec:
    port: 80
    desired_count: 1
    task_size: "x-small"
    image: "public.ecr.aws/z9d2n7e1/nginx:1.21.0"
- name: "prod-two"
  environment: "frontend-env"
  spec:
    port: 80
```

```
    desired_count: 1
    task_size: "x-small"
    image: "public.ecr.aws/z9d2n7e1/nginx:1.21.0"
- name: "prod-three"
  environment: "frontend-env"
  spec:
    port: 80
    desired_count: 1
    task_size: "x-small"
    image: "public.ecr.aws/z9d2n7e1/nginx:1.21.0"
```

Wenn eine Instanz nicht synchronisiert wird und bei dem Versuch, sie zu synchronisieren, weiterhin ein Problem auftritt, kann der Aufruf der `GetServiceInstanceSyncStatus`API zur Lösung des Problems beitragen.

> **Note**
>
> Kunden, die Service Sync verwenden, sind immer noch durch AWS Proton Beschränkungen eingeschränkt.

Blocker

Indem du deinen Service mithilfe AWS Proton von Service Sync synchronisierst, kannst du deine Servicespezifikation aktualisieren und Service-Instances aus deinem Git-Repository erstellen und aktualisieren. Es kann jedoch vorkommen, dass Sie einen Dienst oder eine Instanz manuell über das AWS Management Console oder aktualisieren müssenAWS CLI.

AWS Protonträgt dazu bei, dass manuelle Änderungen, die Sie über das AWS Management Console oder vornehmenAWS CLI, wie das Aktualisieren einer Dienstinstanz oder das Löschen einer Dienstinstanz, nicht überschrieben werden. Um dies zu erreichen, AWS Proton wird automatisch ein Dienstsynchronisierungsblocker erstellt, indem die Dienstsynchronisierung deaktiviert wird, wenn eine manuelle Änderung erkannt wird.

Um alle einem Dienst zugeordneten Blocker abzurufen, müssen Sie für jeden, der dem Dienst `serviceInstance` zugeordnet ist, die folgenden Schritte ausführen:

- Rufen Sie die `getServiceSyncBlockerSummary` API nur mit dem auf`serviceName`.
- Rufen Sie die `getServiceSyncBlockerSummary` API mit dem `serviceName` und auf`serviceInstanceName`.

Dies gibt eine Liste der neuesten Blocker und den ihnen zugeordneten Status zurück. Wenn irgendwelche Blocker als AKTIV markiert sind, musst du sie auflösen, indem du die `UpdateServiceSyncBlocker` API mit dem `blockerId` und `resolvedReason` für jeden einzelnen aufrufst.

Wenn Sie eine Dienstinstanz manuell aktualisieren oder erstellen, AWS Proton wird auf der Dienstinstanz ein Dienstsynchronisierungsblocker erstellt. AWS Protonsynchronisiert weiterhin alle anderen Dienstinstanzen, deaktiviert jedoch die Synchronisierung dieser Dienstinstanz, bis der Blocker aufgelöst ist. Wenn Sie eine Dienstinstanz aus einem Dienst löschen, AWS Proton wird ein Dienstsynchronisierungsblocker für den Dienst erstellt. Dadurch wird AWS Proton verhindert, dass eine der Dienstinstanzen synchronisiert wird, bis der Blocker behoben wurde.

Nachdem Sie alle aktiven Blocker gefunden haben, müssen Sie sie lösen, indem Sie die `UpdateServiceSyncBlocker` API mit dem `blockerId` und `resolvedReason` für jeden der aktiven Blocker aufrufen.

Mithilfe der können Sie feststellenAWS Management Console, ob eine Dienstsynchronisierung deaktiviert ist, indem Sie zur Registerkarte Service Sync navigieren AWS Proton und diese auswählen. Wenn der Dienst oder die Dienstinstanzen blockiert sind, wird eine Schaltfläche zum Aktivieren angezeigt. Um die Servicesynchronisierung zu aktivieren, wählen Sie Aktivieren.

Themen

Erstellen Sie eine Service Sync-Konfiguration

Sie können eine Service-Synchronisationskonfiguration mithilfe der Konsole oder erstellenAWS CLI.

AWS Management Console

1. Wählen Sie auf der Seite „Dienstvorlage auswählen“ eine Vorlage aus und klicken Sie auf Konfigurieren.
2. Geben Sie auf der Seite Service konfigurieren im Abschnitt Dienstdetails einen neuen Dienstnamen ein.

3. (Optional) Geben Sie eine Beschreibung für den Service ein.
4. Wählen Sie im Abschnitt Anwendungsquellcode-Repository die Option Ein verknüpftes Git-Repository auswählen, um ein Repository auszuwählen, mit dem Sie bereits verknüpft sindAWS Proton. Wenn du noch kein verknüpftes Repository hast, wähle Anderes Git-Repository verknüpfen und folge den Anweisungen unter Link zu deinem Repository erstellen.
5. Wählen Sie für Repository den Namen Ihres Quellcode-Repositorys aus der Liste aus.
6. Wählen Sie für Branch den Namen des Repository-Branches für Ihren Quellcode aus der Liste aus.
7. (Optional) Wählen Sie im Bereich Tags die Option Neues Tag hinzufügen aus und geben Sie einen Schlüssel und einen Wert ein, um ein vom Kunden verwaltetes Tag zu erstellen.
8. Wählen Sie Weiter.
9. Wählen Sie auf der Seite Service-Instanzen konfigurieren im Abschnitt Service-Definitionsquelle die Option Service aus Git synchronisieren aus.
10. Wenn Sie Ihre `proton-ops` Datei erstellen AWS Proton möchten, wählen Sie im Abschnitt Service-Definitionsdateien die Option Ich möchte, dass AWS Proton die Dateien erstellt. Mit dieser Option AWS Proton wird die `proton-ops` AND-Datei `spec` an den von Ihnen angegebenen Speicherorten erstellt. Wählen Sie Ich stelle meine eigenen Dateien bereit, um Ihre eigene OPS-Datei zu erstellen.
11. Wählen Sie im Abschnitt Service-Definition-Repository die Option Ein verknüpftes Git-Repository auswählen, um ein Repository auszuwählen, mit dem Sie bereits verknüpft sindAWS Proton.
12. Wählen Sie unter Repository-Name den Namen Ihres Quellcode-Repositorys aus der Liste aus.
13. Wählen Sie für den **`proton-ops`**Datei-Branch den Namen Ihres Branches aus der Liste aus, in der Ihre OPS- und Spezifikationsdatei gespeichert AWS Proton werden sollen.
14. Im Abschnitt Dienstinstanzen wird jedes Feld automatisch anhand der Werte in der `proton-ops` Datei gefüllt.
15. Wählen Sie Weiter und überprüfen Sie Ihre Eingaben.
16. Wählen Sie Create (Erstellen) aus.

AWS CLI

Erstellen Sie eine Service Sync-Konfiguration mit dem AWS CLI

- Führen Sie den folgenden Befehl aus.

```
$ aws proton create-service-sync-config \
    --resource "service-arn" \
    --repository-provider "GITHUB" \
    --repository "example/proton-sync-service" \
    --ops-file-branch "main" \
    --proton-ops-file "./configuration/custom-proton-ops.yaml" (optional)
```

Die Antwort sieht wie folgt.

```
{
    "serviceSyncConfig": {
        "branch": "main",
        "filePath": "./configuration/custom-proton-ops.yaml",
        "repositoryName": "example/proton-sync-service",
        "repositoryProvider": "GITHUB",
        "serviceName": "service name"
    }
}
```

Zeigen Sie Konfigurationsdetails für eine Service-Synchronisation an

Sie können die Konfigurationsdetails für eine Dienstsynchronisierung mithilfe der Konsole oder anzeigenAWS CLI.

AWS Management Console

Verwenden Sie die Konsole, um die Konfigurationsdetails für eine Service-Synchronisation anzuzeigen.

1. Wählen Sie im Navigationsbereich -Services aus.
2. Um Detaildaten anzuzeigen, wählen Sie den Namen eines Dienstes, für den Sie eine Dienstsynchronisierungskonfiguration erstellt haben.

3. Wählen Sie auf der Detailseite für den Service die Registerkarte Service Sync aus, um die Konfigurationsdetaildaten für die Dienstsynchronisierung anzuzeigen.

AWS CLI

Verwenden Sie dieAWS CLI, um einen synchronisierten Dienst zu erhalten.

Führen Sie den folgenden Befehl aus.

```
$ aws proton get-service-sync-config \
    --service-name "service name"
```

Die Antwort sieht wie folgt.

```
{
    "serviceSyncConfig": {
        "branch": "main",
        "filePath": "./configuration/custom-proton-ops.yaml",
        "repositoryName": "example/proton-sync-service",
        "repositoryProvider": "GITHUB",
        "serviceName": "service name"
    }
}
```

Verwenden Sie denAWS CLI, um den Synchronisierungsstatus des Dienstes abzurufen.

Führen Sie den folgenden Befehl aus.

```
$ aws proton get-service-sync-status \
    --service-name "service name"
```

Bearbeiten einer Service-Synchronisationskonfiguration

Sie können eine Service-Synchronisationskonfiguration mithilfe der Konsole oder bearbeitenAWS CLI.

AWS Management Console

Bearbeiten einer Service-Synchronisationskonfiguration unter Verwendung der Konsole.

1. Wählen Sie im Navigationsbereich -Services aus.
2. Um Detaildaten anzuzeigen, wählen Sie den Namen eines Dienstes, für den Sie eine Dienstsynchronisierungskonfiguration erstellt haben.
3. Wählen Sie auf der Seite mit den Servicedetails den Tab Service Sync aus.
4. Wählen Sie im Abschnitt Service Sync die Option Bearbeiten aus.
5. Aktualisieren Sie auf der Seite Bearbeiten die Informationen, die Sie bearbeiten möchten, und wählen Sie dann Speichern.

AWS CLI

Der folgende Beispielbefehl und die folgende Antwort zeigen, wie Sie eine Service Sync-Konfiguration mit dem bearbeiten könnenAWS CLI.

Führen Sie den folgenden Befehl aus.

```
$ aws proton update-service-sync-config \
    --service-name "service name" \
    --repository-provider "GITHUB" \
    --repository "example/proton-sync-service" \
    --ops-file-branch "main" \
    --ops-file "./configuration/custom-proton-ops.yaml"
```

Die Antwort sieht wie folgt.

```
{
    "serviceSyncConfig": {
        "branch": "main",
        "filePath": "./configuration/custom-proton-ops.yaml",
        "repositoryName": "example/proton-sync-service",
        "repositoryProvider": "GITHUB",
        "serviceName": "service name"
    }
}
```

Löschen Sie eine Service Sync-Konfiguration

Sie können eine Service Synchronisationskonfiguration mithilfe der Konsole oder löschenAWS CLI.

AWS Management Console

Löschen einer Service Synchronisationskonfiguration unter Verwendung der Konsole

1. Wählen Sie auf der Seite Service -Detailseite aus.
2. Wählen Sie im Abschnitt Service-Synchronisierungsdetails die Option Trennen aus, um die Verbindung zu Ihrem Repository zu trennen. Nachdem die Verbindung zu Ihrem Repository getrennt wurde, synchronisieren wir den Dienst nicht mehr mit diesem Repository.

AWS CLI

Die folgenden Beispielbefehle und -antworten zeigen, wie Sie die verwendenAWS CLI, um vom Dienst synchronisierte Konfigurationen zu löschen.

Führen Sie den folgenden Befehl aus.

```
$ aws proton delete-service-sync-config \
    --service-name "service name"
```

Die Antwort sieht wie folgt.

```
{
    "serviceSyncConfig": {
        "branch": "main",
        "filePath": "./configuration/custom-proton-ops.yaml",
        "repositoryName": "example/proton-sync-service",
        "repositoryProvider": "GITHUB",
        "serviceName": "service name"
    }
}
```

> **Note**
>
> Service Sync löscht keine Dienstinstanzen. Es löscht nur die Konfiguration.

AWS Proton-Umgebungen

FürAWS Proton, eine Umgebung steht für eine Reihe von gemeinsam genutzten Ressourcen und Richtlinien, dieAWS Proton Dienstleistungenwerden eingesetzt in. Sie können alle Ressourcen enthalten, von denen erwartet wird, dass sie gemeinsam genutzt werden.AWS ProtonDienstinstanzen. Zu diesen Ressourcen können VPCs, Cluster und gemeinsam genutzte Load Balancer oder API-Gateways gehören. EinAWS ProtonEine Umgebung muss erstellt werden, bevor ein Dienst für sie bereitgestellt werden kann.

In diesem Abschnitt wird beschrieben, wie Umgebungen mithilfe von Erstellungs-, Anzeige-, Aktualisierungs- und Löschvorgängen verwaltet werden. >weitere Informationen finden Sie auf derDerAWS ProtonService-API-Referenz.

Themen

IAM-Rollen

MitAWS Proton geben Sie die IAM-Rollen undAWS KMS -Schlüssel für dieAWS Ressourcen an, die Sie besitzen und verwalten. Diese werden später auf Ressourcen angewendet, die Entwicklern gehören und von ihnen verwaltet werden. Sie erstellen eine IAM-Rolle, um den Zugriff Ihres Entwicklerteams auf dieAWS Proton API zu kontrollieren.

AWS Proton-Servicerolle

Wenn Sie eine neue Umgebung erstellen, geben Sie eine zugehörige IAM-Servicerolle an. Die Rolle enthält alle Berechtigungen, die erforderlich sind, um die gesamte bereitgestellte Infrastruktur zu aktualisieren, die sowohl in den Umgebungsvorlagen als auch in den Dienstvorlagen definiert

ist. Rollenbeispiele finden Sie unterAWS ProtonServicerolle für die Bereitstellung mit AWS CloudFormation. Wenn Sie Umgebungskontoverbindungen und Umgebungskonten verwenden, erstellen Sie die Rolle in einem ausgewählten Umgebungskonto. Weitere Informationen erhalten Sie unter Erstellen Sie eine Umgebung in einem Konto und stellen Sie in einem anderen Konto eine Bereitstellung bereit und Verbindungen zu Umgebungskonten.

Wie Sie diese Service-Rolle bereitstellen und wer die Rolle übernimmt, hängt von der Bereitstellungsmethode Ihrer Umgebung ab.

- AWS-managed provisioning — Sie geben dieAWS Proton Rolle entweder direkt bei der Erstellung einer Umgebung oder indirekt über Kontoverbindungen an. AWS Protonübernimmt die Rolle in dem entsprechenden Konto für die Bereitstellungsumgebung und die Service-Infrastruktur.
- Selbstverwaltete Bereitstellung — Es liegt in Ihrer Verantwortung, Ihre Bereitstellungsautomatisierung so zu konfigurieren, dass sie mithilfe der entsprechenden Anmeldeinformationen eine geeignete Rolle übernimmt, wenn ein Pull-Request (PR) eine Bereitstellungsaktion auslöst. Ein Beispiel für eine GitHub Aktion, die eine Rolle übernimmt, finden Sie unter Eine Rolle übernehmen in der Dokumentation „AWSAnmeldeinformationen konfigurieren“ für GitHub Aktionen.

Weitere Informationen zu finden unterthe section called “Methoden der Provisioned”.

Erstellen einer Umgebung

Lerne zu kreierenAWS ProtonUmgebungen.

Sie können eine erstellenAWS ProtonUmgebung auf eine von zwei Arten:

- Erstellen, verwalten und bereitstellen Sie eine Standardumgebung mithilfe einerVorlage für Standardumgebungen.AWS Protonstellt die Infrastruktur für Ihre Umgebung bereit.
- VerbindenAWS Protonzur vom Kunden verwalteten Infrastruktur mithilfe einerVorlage für eine vom Kunden verwaltete Umgebung. Sie stellen Ihre eigenen gemeinsam genutzten Ressourcen außerhalb von bereitAWS Proton, und dann stellen Sie Bereitstellungsausgaben bereit, dieAWS Protonverwenden kann.

Sie können einen von mehreren Bereitstellungsansätzen wählen, wenn Sie eine Umgebung erstellen.

- AWSverwaltete Bereitstellung— Erstellen, verwalten und bereitstellen Sie eine Umgebung in einem einzigen Konto.AWS Protonversorgt Ihre Umgebung.

Diese Methode unterstützt nurCloudFormationVorlagen für Infrastrukturcode (IaC).

- AWSverwaltete Bereitstellung für ein anderes Konto— Erstellen und verwalten Sie in einem einzigen Verwaltungskonto eine Umgebung, die in einem anderen Konto mit Umgebungskontoverbindungen bereitgestellt wird.AWS Protonstellt Ihre Umgebung auf dem anderen Konto bereit. Weitere Informationen erhalten Sie unter Erstellen Sie eine Umgebung in einem Konto und stellen Sie in einem anderen Konto eine Bereitstellung bereit und Verbindungen zu Umgebungskonten.

  Diese Methode unterstützt nurCloudFormationIaC-Vorlagen.

- Selbstverwaltete Bereitstellung—AWS Protonsendet Provisioning-Pull-Requests an ein verknüpftes Repository mit Ihrer eigenen Bereitstellungsinfrastruktur.

  Diese Methode unterstützt nur Terraform IaC-Vorlagen.

- CodeBuildBereitstellung—AWS ProtonVerwendungszweckeAWS CodeBuildum Shell-Befehle auszuführen, die Sie bereitstellen. Ihre Befehle können Eingaben lesen, dieAWS Protonstellt Infrastruktur bereit und ist verantwortlich für die Bereitstellung oder Deprovisionierung der Infrastruktur und die Generierung von Ausgabewerten. Ein Vorlagenpaket für diese Methode enthält Ihre Befehle in einer Manifestdatei und alle Programme, Skripts oder anderen Dateien, die diese Befehle möglicherweise benötigen.

  Als Beispiel für die VerwendungCodeBuildBereitstellung, Sie können Code einbinden, der dieAWS Cloud Development Kit (AWS CDK)zur BereitstellungAWSRessourcen und ein Manifest, das das CDK installiert und Ihren CDK-Code ausführt.

  Weitere Informationen finden Sie unter the section called “CodeBuild -Paket”.

  > **Note**
  >
  > Du kannst benutzenCodeBuildBereitstellung von Umgebungen und Diensten. Derzeit können Sie auf diese Weise keine Komponenten bereitstellen.

MitAWSverwaltete Bereitstellung (sowohl für dasselbe Konto als auch für ein anderes Konto),AWS Protonruft direkt zur Bereitstellung Ihrer Ressourcen auf.

Mit selbstverwalteter BereitstellungAWS Protonerstellt Pull-Requests, um kompilierte IaC-Dateien bereitzustellen, die Ihre IaC-Engine zur Bereitstellung von Ressourcen verwendet.

Weitere Informationen finden Sie unter the section called “Methoden der Provisioned”, the section called “Vorlagenpakete” und the section called “Anforderungen an das Umgebungsschema”.

Themen

- Eine Standardumgebung im selben Konto erstellen und bereitstellen
- Erstellen Sie eine Umgebung in einem Konto und stellen Sie in einem anderen Konto eine Bereitstellung bereit
- Erstellen und Bereitstellen einer Umgebung mithilfe von selbstverwalteter Bereitstellung

Eine Standardumgebung im selben Konto erstellen und bereitstellen

Benutze die Konsole oderAWS CLIum eine Umgebung in einem einzigen Konto zu erstellen und bereitzustellen. Die Bereitstellung wird verwaltet vonAWS.

AWS Management Console

Verwenden Sie die Konsole, um eine Umgebung in einem einzigen Konto zu erstellen und bereitzustellen

1. In derAWS ProtonKonsole, wähleUmgebungen.
2. Wählen Sie Create environment (Umgebung erstellen) aus.
3. In derWählen Sie eine UmgebungsvorlageSeite, wählen Sie eine Vorlage aus und wählen Siekonfigurieren.
4. In derUmgebung konfigurierenSeite, in derBereitstellungAbschnitt, wählenAWSverwaltete Bereitstellung.
5. In derDeployment-KontoAbschnitt, wählenDasAWS-Konto.
6. In derUmgebung konfigurierenSeite, in derUmgebungseinstellungenAbschnitt, geben Sie einen einName der Umgebung.
7. (Optional) Geben Sie eine Beschreibung für die Umgebung ein.
8. In derRollen im UmfeldAbschnitt, wählen Sie denAWS ProtonServicerolle, die Sie als Teil von erstellt habenAWS ProtonServicerollen einrichten.
9. (Optional) In derRolle der KomponenteAbschnitt, wählen Sie eine Servicerolle aus, die es direkt definierten Komponenten ermöglicht, in der Umgebung ausgeführt zu werden, und legt den Umfang der Ressourcen fest, die sie bereitstellen können. Weitere Informationen finden Sie unter Komponenten.

10. (Optional) In derSchlagworteAbschnitt, wählenNeues Schlagwort hinzufügenund geben Sie einen Schlüssel und einen Wert ein, um ein vom Kunden verwaltetes Tag zu erstellen.
11. Wählen Sie Weiter aus.
12. In derBenutzerdefinierte Umgebungseinstellungen konfigurierenSeite, Sie müssen Werte für die eingeben`required`Parameter. Sie können Werte eingeben für`optional`Parameter oder verwenden Sie die Standardeinstellungen, falls angegeben.
13. Wählen SieWeiterund überprüfe deine Eingaben.
14. Wählen Sie Erstellen aus.

    Sehen Sie sich die Umgebungsdetails und den Status sowie dieAWSverwaltete Tags und vom Kunden verwaltete Tags für Ihre Umgebung.
15. Wählen Sie im Navigationsbereich Environments (Umgebungen) aus.

    Auf einer neuen Seite wird eine Liste Ihrer Umgebungen zusammen mit dem Status und anderen Umgebungsdetails angezeigt.

AWS CLI

Benutze dieAWS CLIum eine Umgebung in einem einzigen Konto zu erstellen und bereitzustellen.

Um eine Umgebung zu erstellen, geben Sie dieAWS ProtonServicerolleARN, Pfad zu Ihrer Spezifikationsdatei, Umgebungsname, Umgebungsvorlage ARN, Haupt- und Nebenversionen und Beschreibung (optional).

Das nächste Beispiel zeigt eineYAMLformatierte Spezifikationsdatei, die Werte für zwei Eingaben angibt, die in der Schemadatei der Umgebungsvorlage definiert sind. Sie können das verwenden`get-environment-template-minor-version`Befehl zum Anzeigen des Umgebungsvorlagenschemas.

```
proton: EnvironmentSpec
spec:
  my_sample_input: "the first"
  my_other_sample_input: "the second"
```

Erstellen Sie eine Umgebung, indem Sie den folgenden Befehl ausführen.

```
$ aws proton create-environment \
```

```
    --name "MySimpleEnv" \
    --template-name simple-env \
    --template-major-version 1 \
    --proton-service-role-arn "arn:aws:iam::123456789012:role/AWSProtonServiceRole"
 \
    --spec "file://env-spec.yaml"
```

Antwort:

```
{
    "environment": {
        "arn": "arn:aws:proton:region-id:123456789012:environment/MySimpleEnv",
        "createdAt": "2020-11-11T23:03:05.405000+00:00",
        "deploymentStatus": "IN_PROGRESS",
        "lastDeploymentAttemptedAt": "2020-11-11T23:03:05.405000+00:00",
        "name": "MySimpleEnv",
        "protonServiceRoleArn": "arn:aws:iam::123456789012:role/ProtonServiceRole",
        "templateName": "simple-env"
    }
}
```

Nachdem Sie eine neue Umgebung erstellt haben, können Sie sich eine Liste von ansehenAWSund vom Kunden verwaltete Tags, wie im folgenden Beispielbefehl gezeigt.AWS Protongeneriert automatischAWSverwaltete Tags für Sie. Sie können von Kunden verwaltete Tags auch ändern und erstellen, indem Sie denAWS CLI. Weitere Informationen finden Sie unter AWS ProtonRessourcen und Tagging.

Befehl:

```
$ aws proton list-tags-for-resource \
    --resource-arn "arn:aws:proton:region-id:123456789012:environment/MySimpleEnv"
```

Erstellen Sie eine Umgebung in einem Konto und stellen Sie in einem anderen Konto eine Bereitstellung bereit

Benutze die Konsole oderAWS CLIum eine Standardumgebung in einem Verwaltungskonto zu erstellen, die die Umgebungsinfrastruktur in einem anderen Konto bereitstellt. Die Bereitstellung wird verwaltet vonAWS.

Führen Sie die folgenden Schritte aus, bevor Sie die Konsole oder CLI verwenden.

1. Identifizieren Sie dieAWS-KontoIDs für das Management- und das Umgebungskonto und kopieren Sie sie zur späteren Verwendung.
2. Erstellen Sie im Umgebungskonto einAWS ProtonServicerolle mit Mindestberechtigungen für die zu erstellende Umgebung. Weitere Informationen finden Sie unter AWS ProtonServicerolle für die Bereitstellung mit AWS CloudFormation.

AWS Management Console

Erstellen Sie mithilfe der Konsole eine Umgebung in einem Konto und stellen Sie sie in einem anderen Konto bereit.

1. Erstellen Sie im Umgebungskonto eine Verbindung zum Umgebungskonto und verwenden Sie diese, um eine Anfrage zum Herstellen einer Verbindung mit dem Verwaltungskonto zu senden.

   a. InAWS ProtonKonsole, wähleVerbindungen zu Umgebungskontenim Navigationsbereich.

   b. In derVerbindungen zu UmgebungskontenSeite, wählenAnfrage zur Verbindung.

   > **Note**
   >
   > Stellen Sie sicher, dass die Konto-ID, die imVerbindung zum UmgebungskontoDie Seitenüberschrift entspricht Ihrer vorab identifizierten Umgebungskonto-ID.

   c. In derAnfrage zur VerbindungSeite, in derRolle UmweltAbschnitt, wählenBestehende Servicerolleund der Name der Servicerolle, die Sie für die Umgebung erstellt haben.

   d. In derStellen Sie eine Verbindung zum Verwaltungskonto herAbschnitt, geben Sie den einID des Verwaltungskontosund einName der Umgebungfür deinAWS ProtonUmwelt. Kopieren Sie den Namen zur späteren Verwendung.

   e. Wählen SieAnfrage zur Verbindungin der unteren rechten Ecke der Seite.

   f. Ihre Anfrage wird als ausstehend angezeigt in derUmgebungsverbindungen, die an ein Verwaltungskonto gesendet wurdenEine Tabelle und ein Modal zeigen, wie die Anfrage vom Verwaltungskonto aus akzeptiert wird.

2. Akzeptieren Sie im Verwaltungskonto eine Verbindungsanfrage vom Umgebungskonto aus.

   a. Loggen Sie sich in Ihr Verwaltungskonto ein und wählen SieVerbindungen zu Umgebungskontenin derAWS ProtonKonsole.

   b. In derVerbindungen zu UmgebungskontenSeite, in derVerbindungsanfragen für UmgebungskontenTabelle, wählen Sie die Umgebungskontoverbindung mit der Umgebungskonto-ID aus, die Ihrer vorab identifizierten Umgebungskonto-ID entspricht.

   > **Note**
   >
   > Stellen Sie sicher, dass die Konto-ID, die imVerbindung zum UmgebungskontoDie Seitenüberschrift entspricht Ihrer vorab identifizierten Verwaltungskonto-ID.

   c. Wählen Sie Accept (Akzeptieren) aus. Der Status ändert sich von PENDING zu CONNECTED.

3. Erstellen Sie im Verwaltungskonto eine Umgebung.

   a. Wählen Sie im NavigationsbereichVorlagen für die Umgebung.

   b. In derVorlagen für die UmgebungSeite, wählenUmgebungsvorlage erstellen.

   c. In derWählen Sie eine UmgebungsvorlageSeite, wählen Sie eine Umgebungsvorlage.

   d. In derUmgebung konfigurierenSeite, in derBereitstellungAbschnitt, wählenAWSverwaltete Bereitstellung.

   e. In derDeployment-KontoAbschnitt, wählenEin andererAWSkonto;.

   f. In derAngaben zur UmgebungAbschnitt, wählen Sie IhrenVerbindung zum UmgebungskontoundName der Umgebung.

   g. Wählen Sie Weiter aus.

   h. Füllen Sie die Formulare aus und wählen SieWeiterbis du das erreichstÜberprüfen und erstellenSeite.

   i. Überprüfen und wählenUmgebung schaffen.

AWS CLI

Benutze dieAWS CLIum in einem Konto eine Umgebung und in einem anderen eine Bereitstellung zu erstellen.

Erstellen Sie im Umgebungskonto eine Verbindung zum Umgebungskonto und fordern Sie die Verbindung an, indem Sie den folgenden Befehl ausführen.

```
$ aws proton create-environment-account-connection \
    --environment-name "simple-env-connected" \
    --role-arn "arn:aws:iam::222222222222:role/service-role/env-account-proton-service-role" \
    --management-account-id "111111111111"
```

Antwort:

```
{
    "environmentAccountConnection": {
        "arn": "arn:aws:proton:region-id:222222222222:environment-account-connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "environmentAccountId": "222222222222",
        "environmentName": "simple-env-connected",
        "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "lastModifiedAt": "2021-04-28T23:13:50.847000+00:00",
        "managementAccountId": "111111111111",
        "requestedAt": "2021-04-28T23:13:50.847000+00:00",
        "roleArn": "arn:aws:iam::222222222222:role/service-role/env-account-proton-service-role",
        "status": "PENDING"
    }
}
```

Akzeptieren Sie im Verwaltungskonto die Verbindungsanforderung für das Umgebungskonto, indem Sie den folgenden Befehl ausführen.

```
$ aws proton accept-environment-account-connection \
    --id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Antwort:

```
{
    "environmentAccountConnection": {
        "arn": "arn:aws:proton:region-id:222222222222:environment-account-connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "environmentAccountId": "222222222222",
        "environmentName": "simple-env-connected",
```

```
        "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "lastModifiedAt": "2021-04-28T23:15:33.486000+00:00",
        "managementAccountId": "111111111111",
        "requestedAt": "2021-04-28T23:13:50.847000+00:00",
        "roleArn": "arn:aws:iam::222222222222:role/service-role/env-account-proton-
service-role",
        "status": "CONNECTED"
    }
}
```

Rufen Sie die Verbindung Ihres Umgebungskontos auf, indem Sie den folgenden Befehl ausführen.

```
$ aws proton get-environment-account-connection \
    --id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Antwort:

```
{
    "environmentAccountConnection": {
        "arn": "arn:aws:proton:region-id:222222222222:environment-account-
connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "environmentAccountId": "222222222222",
        "environmentName": "simple-env-connected",
        "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "lastModifiedAt": "2021-04-28T23:15:33.486000+00:00",
        "managementAccountId": "111111111111",
        "requestedAt": "2021-04-28T23:13:50.847000+00:00",
        "roleArn": "arn:aws:iam::222222222222:role/service-role/env-account-proton-
service-role",
        "status": "CONNECTED"
    }
}
```

Erstellen Sie im Verwaltungskonto eine Umgebung, indem Sie den folgenden Befehl ausführen.

```
$ aws proton create-environment \
    --name "simple-env-connected" \
    --template-name simple-env-template \
    --template-major-version "1" \
    --template-minor-version "1" \
```

```
    --spec "file://simple-env-template/specs/original.yaml" \
    --environment-account-connection-id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Antwort:

```
{
    "environment": {
        "arn": "arn:aws:proton:region-id:111111111111:environment/simple-env-
connected",
        "createdAt": "2021-04-28T23:02:57.944000+00:00",
        "deploymentStatus": "IN_PROGRESS",
        "environmentAccountConnectionId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "environmentAccountId": "222222222222",
        "lastDeploymentAttemptedAt": "2021-04-28T23:02:57.944000+00:00",
        "name": "simple-env-connected",
        "templateName": "simple-env-template"
    }
}
```

Erstellen und Bereitstellen einer Umgebung mithilfe von selbstverwalteter Bereitstellung

Wenn Sie selbstverwaltete Bereitstellung verwenden,AWS Protonsendet Provisioning-Pull-Requests an ein verknüpftes Repository mit Ihrer eigenen Bereitstellungsinfrastruktur. Die Pull-Requests starten deinen eigenen Workflow, der aufruftAWSDienstleistungen; zur Bereitstellung von Infrastruktur.

Überlegungen zur selbstverwalteten Bereitstellung:

- Bevor Sie eine Umgebung erstellen, richten Sie ein Repository-Ressourcenverzeichnis für die selbstverwaltete Bereitstellung ein. Weitere Informationen finden Sie unter AWS Proton Infrastructure as Code-Dateien.
- Nachdem Sie die Umgebung erstellt haben,AWS Protonwartet darauf, asynchrone Benachrichtigungen über den Status Ihrer Infrastrukturbereitstellung zu erhalten. Ihr Bereitstellungscode muss den verwendenAWS Proton `NotifyResourceStateChange`API zum Senden dieser asynchronen Benachrichtigungen anAWS Proton.

Sie können die selbstverwaltete Bereitstellung in der Konsole oder mit demAWS CLI. Die folgenden Beispiele zeigen, wie Sie die selbstverwaltete Bereitstellung mit Terraform verwenden können.

AWS Management Console

Verwenden Sie die Konsole, um mithilfe von selbstverwalteter Bereitstellung eine Terraform-Umgebung zu erstellen.

1. In derAWS ProtonKonsole, wähleUmgebungen.
2. Wählen Sie Create environment (Umgebung erstellen) aus.
3. In derWählen Sie eine UmgebungsvorlageSeite, wählen Sie eine Terraform-Vorlage aus und wählen Siekonfigurieren.
4. In derUmgebung konfigurierenSeite, in derBereitstellungAbschnitt, wählenSelbstverwaltete Bereitstellung.
5. In derEinzelheiten zur Bereitstellung des RepositorysAbschnitt:

   a. Wenn du es noch nicht getan hasthat Ihr Provisioning-Repository verknüpft mitAWS Proton, wähleNeues Repositorium, wählen Sie einen der Repository-Anbieter und dann fürCodeStarVerbindung, wählen Sie eine Ihrer Verbindungen.

   > **Note**
   >
   > Wenn Sie noch keine Verbindung zum entsprechenden Repository-Anbieterkonto haben, wählen SieFüge ein neues hinzuCodeStarVerbindung. Erstellen Sie dann eine Verbindung und klicken Sie dann auf die Schaltfläche „Aktualisieren“ neben demCodeStarVerbindungSpeisekarte. Sie sollten jetzt Ihre neue Verbindung im Menü auswählen können.

   Wenn du dein Repository bereits verlinkt hastAWS Proton, wähleBestehendes Repositorium.

   b. FürName des Repositoriums, wählen Sie ein Repository aus. Das Drop-down-Menü zeigt verknüpfte Repositorys fürBestehendes Repositoriumoder die Liste der Repositorien im Anbieterkonto fürNeues Repositorium.

   c. FürName der Filiale, wählen Sie einen der Repository-Zweige aus.
6. In derUmgebungseinstellungenAbschnitt, geben Sie einen einName der Umgebung.
7. (Optional) Geben Sie eine Beschreibung für die Umgebung ein.
8. (Optional) In derSchlagworteAbschnitt, wählenNeues Schlagwort hinzufügenund geben Sie einen Schlüssel und einen Wert ein, um ein vom Kunden verwaltetes Tag zu erstellen.

9. Wählen Sie Weiter aus.
10. In derBenutzerdefinierte Umgebungseinstellungen konfigurierenSeite, Sie müssen Werte für die eingeben`required`Parameter. Sie können Werte eingeben für`optional`Parameter oder verwenden Sie die Standardeinstellungen, falls angegeben.
11. Wählen SieWeiterund überprüfe deine Eingaben.
12. Wählen SieErstellenum eine Pull-Anfrage zu senden.

    - Wenn Sie den Pull-Request genehmigen, ist die Bereitstellung im Gange.
    - Wenn Sie den Pull-Request ablehnen, wird die Erstellung der Umgebung abgebrochen.
    - Wenn der Pull-Request ein Timeout hat, Erstellung der Umgebungist nichtkomplett.
13. Sehen Sie sich die Umgebungsdetails und den Status sowie dieAWSverwaltete Tags und vom Kunden verwaltete Tags für Ihre Umgebung.
14. Wählen Sie im Navigationsbereich Environments (Umgebungen) aus.

    Auf einer neuen Seite wird eine Liste Ihrer Umgebungen zusammen mit dem Status und anderen Umgebungsdetails angezeigt.

AWS CLI

Wenn Sie eine Umgebung mithilfe von selbstverwalteter Bereitstellung erstellen,hinzufügendie`provisioningRepository`Parameter und lassen Sie den`ProtonServiceRoleArn`und`environmentAccountConnectionId`Parameter.

Benutze dieAWS CLIum eine Terraform-Umgebung mit selbstverwalteter Bereitstellung zu erstellen.

1. Erstellen Sie eine Umgebung und senden Sie eine Pull-Anfrage zur Überprüfung und Genehmigung an das Repository.

   Das nächste Beispiel zeigt eine`YAML`formatierte Spezifikationsdatei, die die Werte für zwei Eingaben basierend auf der Schemadatei der Umgebungsvorlage definiert. Sie können das verwenden`get-environment-template-minor-version`Befehl zum Anzeigen des Umgebungsvorlagenschemas.

   Spezifikation:

   ```
   proton: EnvironmentSpec
   ```

```
spec:
  ssm_parameter_value: "test"
```

Erstellen Sie eine Umgebung, indem Sie den folgenden Befehl ausführen.

```
$ aws proton create-environment \
    --name "pr-environment" \
    --template-name "pr-env-template" \
    --template-major-version "1" \
    --provisioning-repository="branch=main,name=myrepos/env-
repo,provider=GITHUB" \
    --spec "file://env-spec.yaml"
```

Antwort: >

```
{
    "environment": {
        "arn": "arn:aws:proton:region-id:123456789012:environment/pr-
environment",
        "createdAt": "2021-11-18T17:06:58.679000+00:00",
        "deploymentStatus": "IN_PROGRESS",
        "lastDeploymentAttemptedAt": "2021-11-18T17:06:58.679000+00:00",
        "name": "pr-environment",
        "provisioningRepository": {
            "arn": "arn:aws:proton:region-id:123456789012:repository/
github:myrepos/env-repo",
            "branch": "main",
            "name": "myrepos/env-repo",
            "provider": "GITHUB"
        },
        "templateName": "pr-env-template"
    }
```

2. Überprüfen Sie die Anfrage.

   - Wenn Sie die Anfrage genehmigen, wird die Bereitstellung durchgeführt.
   - Wenn Sie die Anfrage ablehnen, wird die Erstellung der Umgebung abgebrochen.
   - Wenn der Pull-Request ein Timeout hat, Erstellung der Umgebungist nichtkomplett.

3. Stellen Sie den Bereitstellungsstatus asynchron bereit fürAWS Proton. Das folgende Beispiel benachrichtigtAWS Protoneiner erfolgreichen Bereitstellung.

```
$ aws proton notify-resource-deployment-status-change \
    --resource-arn "arn:aws:proton:region-id:123456789012:environment/pr-environment" \
    --status "SUCCEEDED"
```

Umgebungsdaten anzeigen

Sie können Umgebungsdetaildaten mit einer derAWS ProtonKonsole oder dieAWS CLI.

AWS Management Console

Sie können Listen von Umgebungen mit Details und einzelnen Umgebungen mit Detaildaten anzeigen, indem Sie denAWS ProtonKonsole.

1. Um eine Liste Ihrer Umgebungen anzuzeigen, wählen SieUmgebungenim Navigationsbereich.
2. Um Detaildaten anzuzeigen, wählen Sie den Namen einer Umgebung.

   Sehen Sie sich Ihre Umgebungsdetaildaten an.

AWS CLI

Benutze dieAWS CLI erhaltenoderListeDetails zur Umgebung.

Führen Sie den Befehl aus:

```
$ aws proton get-environment \
    --name "MySimpleEnv"
```

Antwort:

```
{
    "environment": {
        "arn": "arn:aws:proton:region-id:123456789012:environment/MySimpleEnv",
        "createdAt": "2020-11-11T23:03:05.405000+00:00",
        "deploymentStatus": "SUCCEEDED",
        "lastDeploymentAttemptedAt": "2020-11-11T23:03:05.405000+00:00",
        "lastDeploymentSucceededAt": "2020-11-11T23:03:05.405000+00:00",
```

```
        "name": "MySimpleEnv",
        "protonServiceRoleArn": "arn:aws:iam::123456789012:role/ProtonServiceRole",
        "spec": "proton: EnvironmentSpec\nspec:\n  my_sample_input: \"the first\"\n
 my_other_sample_input: \"the second\"\n",
        "templateMajorVersion": "1",
        "templateMinorVersion": "0",
        "templateName": "simple-env"
    }
}
```

Eine Umgebung aktualisieren

Wenn derAWS Protondie Umgebung ist mit einer Umgebungskontoverbindung verknüpft,nichtaktualisiere oder füge die hinzu`protonServiceRoleArn`Parameter zum Aktualisieren oder Herstellen einer Verbindung zu einem Umgebungskonto.

Sie können nur dann auf eine neue Umgebungskontoverbindung aktualisieren, wenn beide der folgenden Bedingungen zutreffen:

- Die Umgebungskontoverbindung wurde in demselben Umgebungskonto erstellt, in dem die aktuelle Umgebungskontoverbindung erstellt wurde.
- >Die Verbindung des Umgebungskontos ist mit der aktuellen Umgebung verknüpft.

Wenn die Umweltist nichtverbunden mit einer Umgebungskontoverbindung,nichtaktualisiere oder füge die hinzu`environmentAccountConnectionId`Parameter.

Sie können entweder die aktualisieren`environmentAccountConnectionId`oder`protonServiceRoleArn`Parameter und Wert. Sie können nicht beide aktualisieren.

Wenn Ihre Umgebung selbstverwaltete Bereitstellung verwendet,nichtaktualisiere die`provisioning-repository`Parameter undauslassendie`environmentAccountConnectionId`und`protonServiceRoleArn`Parameter.

Es gibt vier Modi für die Aktualisierung einer Umgebung, wie in der folgenden Liste beschrieben. Bei Verwendung desAWS CLI, der`deployment-type`Feld definiert den Modus. Wenn Sie die Konsole verwenden, werden diese Modi dem zugeordnetBearbeiten,Aktualisieren,Kleines Update, undHauptfach aktualisierenAktionen, die herunterfallen vonAktionen.

`NONE`

In diesem Modus ein Deploymenttut nichtauftreten. Nur die angeforderten Metadatenparameter werden aktualisiert.

`CURRENT_VERSION`

In diesem Modus wird die Umgebung bereitgestellt und mit der von Ihnen bereitgestellten neuen Spezifikation aktualisiert. Nur angeforderte Parameter werden aktualisiert. Tun Sie es nichtFügen Sie die Parameter der Neben- oder Hauptversion ein, wenn Sie dies verwenden`deployment-type`.

`MINOR_VERSION`

In diesem Modus wird die Umgebung bereitgestellt und standardmäßig mit der veröffentlichten, empfohlenen (neuesten) Nebenversion der aktuellen Hauptversion aktualisiert. Sie können auch eine andere Nebenversion der aktuell verwendeten Hauptversion angeben.

`MAJOR_VERSION`

In diesem Modus wird die Umgebung standardmäßig mit der veröffentlichten, empfohlenen (neuesten) Haupt- und Nebenversion der aktuellen Vorlage bereitgestellt und aktualisiert. Sie können auch eine andere Hauptversion angeben, die höher ist als die verwendete Hauptversion, und eine Nebenversion (optional).

Themen

Aktualisiere eineAWSverwaltete Bereitstellungsumgebung

Die Standardbereitstellung wird nur von Umgebungen unterstützt, die Folgendes bereitstellenAWS CloudFormation.

Benutze die Konsole oderAWS CLIum Ihre Umgebung zu aktualisieren.

AWS Management Console

Aktualisieren Sie eine Umgebung mithilfe der Konsole, wie in den folgenden Schritten gezeigt.

1. Wählen Sie einen der folgenden 2 Schritte aus.

   a. In der Liste der Umgebungen.

      i. In derAWS ProtonKonsole, wähleUmgebungen.

      ii. Wählen Sie in der Liste der Umgebungen das Optionsfeld links neben der Umgebung aus, die Sie aktualisieren möchten.

   b. Auf der Detailseite der Konsolenumgebung.

      i. In derAWS ProtonKonsole, wähleUmgebungen.

      ii. Wählen Sie in der Liste der Umgebungen den Namen der Umgebung aus, die Sie aktualisieren möchten.

2. Wählen Sie einen der nächsten 4 Schritte, um Ihre Umgebung zu aktualisieren.

   a. Um eine Bearbeitung vorzunehmen, für die keine Bereitstellung der Umgebung erforderlich ist.

      i. Zum Beispiel, um eine Beschreibung zu ändern.

         Wählen Sie Edit (Bearbeiten) aus.

      ii. Füllen Sie das Formular aus und wählen SieWeiter.

      iii. Überprüfe deine Bearbeitung und wähleAktualisieren.

   b. Um Aktualisierungen nur an Metadateneingaben vorzunehmen.

      i. WähleAktionenund dannAktualisieren.

      ii. Füllen Sie das Formular aus und wählen SieBearbeiten.

      iii. Füllen Sie die Formulare aus und wählen SieWeiterbis du das erreichstBewertungSeite.

      iv. Überprüfe deine Updates und wähleAktualisieren.

   c. Um ein Update auf eine neue Nebenversion seiner Umgebungsvorlage vorzunehmen.

      i. WähleAktionenund dannKleines Update.

      ii. Füllen Sie das Formular aus und wählen SieWeiter.

iii. Füllen Sie die Formulare aus und wählen SieWeiterbis du das erreichstBewertungSeite.

iv. Überprüfe deine Updates und wähleAktualisieren.

d. Um ein Update auf eine neue Hauptversion seiner Umgebungsvorlage vorzunehmen.

i. WähleAktionenund dannHauptfach aktualisieren.

ii. Füllen Sie das Formular aus und wählen SieWeiter.

iii. Füllen Sie die Formulare aus und wählen SieWeiterbis du das erreichstBewertungSeite.

iv. Überprüfe deine Updates und wähleAktualisieren.

AWS CLI

Benutze dieAWS Proton AWS CLIum eine Umgebung auf eine neue Nebenversion zu aktualisieren.

Führen Sie den folgenden Befehl aus, um Ihre Umgebung zu aktualisieren:

```
$ aws proton update-environment \
        --name "MySimpleEnv" \
        --deployment-type "MINOR_VERSION" \
        --template-major-version "1" \
        --template-minor-version "1" \
        --proton-service-role-arn arn:aws:iam::123456789012:role/service-
role/ProtonServiceRole \
        --spec "file:///spec.yaml"
```

Antwort:

```
{
    "environment": {
        "arn": "arn:aws:proton:region-id:123456789012:environment/MySimpleEnv",
        "createdAt": "2021-04-02T17:29:55.472000+00:00",
        "deploymentStatus": "IN_PROGRESS",
        "lastDeploymentAttemptedAt": "2021-04-02T17:48:26.307000+00:00",
        "lastDeploymentSucceededAt": "2021-04-02T17:29:55.472000+00:00",
        "name": "MySimpleEnv",
        "protonServiceRoleArn": "arn:aws:iam::123456789012:role/service-role/
ProtonServiceRole",
```

```
        "templateMajorVersion": "1",
        "templateMinorVersion": "0",
        "templateName": "simple-env"
    }
}
```

Führen Sie den folgenden Befehl aus, um den Status abzurufen und zu bestätigen:

```
$ aws proton get-environment \
        --name "MySimpleEnv"
```

Antwort:

```
{
    "environment": {
        "arn": "arn:aws:proton:region-id:123456789012:environment/MySimpleEnv",
        "createdAt": "2021-04-02T17:29:55.472000+00:00",
        "deploymentStatus": "SUCCEEDED",
        "environmentName": "MySimpleEnv",
        "lastDeploymentAttemptedAt": "2021-04-02T17:48:26.307000+00:00",
        "lastDeploymentSucceededAt": "2021-04-02T17:48:26.307000+00:00",
        "protonServiceRoleArn": "arn:aws:iam::123456789012:role/service-role/
ProtonServiceRole",
        "spec": "proton: EnvironmentSpec\n\nspec:\n  my_sample_input: hello\n
 my_other_sample_input: everybody\n",
        "templateMajorVersion": "1",
        "templateMinorVersion": "1",
        "templateName": "simple-env"
    }
}
```

Aktualisieren Sie eine selbstverwaltete Bereitstellungsumgebung

Selbstverwaltete Bereitstellung wird nur von Umgebungen unterstützt, die mit Terraform bereitstellen.

Benutze die Konsole oderAWS CLIum Ihre Umgebung zu aktualisieren.

AWS Management Console

Aktualisieren Sie eine Umgebung mithilfe der Konsole, wie in den folgenden Schritten gezeigt.

1. Wählen Sie einen der folgenden 2 Schritte aus.

   a. In der Liste der Umgebungen.

      i. In derAWS ProtonKonsole, wähleUmgebungen.

      ii. Wählen Sie in der Liste der Umgebungen das Optionsfeld links neben der Umgebungsvorlage aus, die Sie aktualisieren möchten.

   b. Auf der Detailseite der Konsolenumgebung.

      i. In derAWS ProtonKonsole, wähleUmgebungen.

      ii. Wählen Sie in der Liste der Umgebungen den Namen der Umgebung aus, die Sie aktualisieren möchten.

2. Wählen Sie einen der nächsten 4 Schritte, um Ihre Umgebung zu aktualisieren.

   a. Um eine Bearbeitung vorzunehmen, für die keine Bereitstellung der Umgebung erforderlich ist.

      i. Zum Beispiel, um eine Beschreibung zu ändern.

         Wählen Sie Edit (Bearbeiten) aus.

      ii. Füllen Sie das Formular aus und wählen SieWeiter.

      iii. Überprüfe deine Bearbeitung und wähleAktualisieren.

   b. Um Aktualisierungen nur an Metadateneingaben vorzunehmen.

      i. Wählen SieAktionenund dannAktualisieren.

      ii. Füllen Sie das Formular aus und wählen SieBearbeiten.

      iii. Füllen Sie die Formulare aus und wählen SieWeiterbis du das erreichstBewertungSeite.

      iv. Überprüfe deine Updates und wähleAktualisieren.

   c. Um ein Update auf eine neue Nebenversion seiner Umgebungsvorlage vorzunehmen.

      i. Wählen SieAktionenund dannKleines Update.

      ii. Füllen Sie das Formular aus und wählen SieWeiter.

iii. Füllen Sie die Formulare aus und wählen SieWeiterbis du das erreichstBewertungSeite.

iv. Überprüfe deine Updates und wähleAktualisieren.

d. Um ein Update auf eine neue Hauptversion seiner Umgebungsvorlage vorzunehmen.

i. Wählen SieAktionenund dannHauptfach aktualisieren.

ii. Füllen Sie das Formular aus und wählen SieWeiter.

iii. Füllen Sie die Formulare aus und wählen SieWeiterbis du das erreichstBewertungSeite.

iv. Überprüfe deine Updates und wähleAktualisieren.

AWS CLI

Benutze dieAWS CLIum eine Terraform-Umgebung auf eine neue Nebenversion mit selbstverwalteter Bereitstellung zu aktualisieren.

1. Führen Sie den folgenden Befehl aus, um Ihre Umgebung zu aktualisieren:

```
$ aws proton update-environment \
    --name "pr-environment" \
    --deployment-type "MINOR_VERSION" \
    --template-major-version "1" \
    --template-minor-version "1" \
    --provisioning-repository "branch=main,name=myrepos/env-
repo,provider=GITHUB" \
    --spec "file://env-spec-mod.yaml"
```

Antwort:

```
{
    "environment": {
        "arn": "arn:aws:proton:region-id:123456789012:environment/pr-
environment",
        "createdAt": "2021-11-18T21:09:15.745000+00:00",
        "deploymentStatus": "IN_PROGRESS",
        "lastDeploymentAttemptedAt": "2021-11-18T21:25:41.998000+00:00",
        "lastDeploymentSucceededAt": "2021-11-18T21:09:15.745000+00:00",
        "name": "pr-environment",
        "provisioningRepository": {
```

```
            "arn": "arn:aws:proton:region-id:123456789012:repository/
github:myrepos/env-repo",
            "branch": "main",
            "name": "myrepos/env-repo",
            "provider": "GITHUB"
        },
        "templateMajorVersion": "1",
        "templateMinorVersion": "0",
        "templateName": "pr-env-template"
    }
}
```

2. Führen Sie den folgenden Befehl aus, um den Status abzurufen und zu bestätigen:

```
$ aws proton get-environment \
    --name "pr-environment"
```

Antwort:

```
{
    "environment": {
        "arn": "arn:aws:proton:region-id:123456789012:environment/pr-
environment",
        "createdAt": "2021-11-18T21:09:15.745000+00:00",
        "deploymentStatus": "SUCCEEDED",
        "lastDeploymentAttemptedAt": "2021-11-18T21:25:41.998000+00:00",
        "lastDeploymentSucceededAt": "2021-11-18T21:25:41.998000+00:00",
        "name": "pr-environment",
        "provisioningRepository": {
            "arn": "arn:aws:proton:region-id:123456789012:repository/
github:myrepos/env-repo",
            "branch": "main",
            "name": "myrepos/env-repo",
            "provider": "GITHUB"
        },
        "spec": "proton: EnvironmentSpec\nspec:\n   ssm_parameter_value: \"test
\"\n ssm_another_parameter_value: \"update\"\n",
        "templateMajorVersion": "1",
        "templateMinorVersion": "1",
        "templateName": "pr-env-template"
    }
}
```

3. Überprüfe den Pull-Request, der gesendet wurde vonAWS Proton.

   - Wenn Sie die Anfrage genehmigen, wird die Bereitstellung durchgeführt.
   - Wenn Sie die Anfrage ablehnen, wird die Erstellung der Umgebung abgebrochen.
   - Wenn bei der Pull-Anfrage ein Timeout auftritt, ist die Erstellung der Umgebung nicht abgeschlossen.

4. Geben Sie den Bereitstellungsstatus anAWS Proton.

```
$ aws proton notify-resource-deployment-status-change \
    --resource-arn "arn:aws:proton:region-id:123456789012:environment/pr-environment" \
    --status "SUCCEEDED"
```

Eine laufende Umgebungsbereitstellung abbrechen

Sie können versuchen, die Bereitstellung eines Umgebungsupdates abzubrechen, wenn`deploymentStatus`ist in`IN_PROGRESS`.AWS Protonversucht, die Bereitstellung abzubrechen. Erfolgreiche Stornierungist nichtgarantiert.

Wenn Sie eine Update-Bereitstellung abbrechen,AWS Protonversucht, die Bereitstellung wie in den folgenden Schritten beschrieben abzubrechen.

MitAWS-verwaltete Bereitstellung,AWS Protonmacht das Folgende:

- Setzt den Bereitstellungsstatus auf`CANCELLING`.
- Stoppt die laufende Bereitstellung und löscht alle neuen Ressourcen, die durch das Deployment erstellt wurden, wenn`IN_PROGRESS`.
- Setzt den Bereitstellungsstatus auf`CANCELLED`.
- Setzt den Status der Ressource auf den Zustand vor dem Start der Bereitstellung zurück.

Mit selbstverwalteter BereitstellungAWS Protonmacht das Folgende:

- Versucht, den Pull-Request zu schließen, um zu verhindern, dass die Änderungen in Ihrem Repository zusammengeführt werden.
- Setzt den Bereitstellungsstatus auf`CANCELLED`wenn der Pull-Request erfolgreich geschlossen wurde.

Anweisungen zum Abbrechen einer Umgebungsbereitstellung finden Sie unterCancelEnvironmentDeploymentin derAWS ProtonAPI-Referenz.

Sie können die Konsole oder die CLI verwenden, um laufende Umgebungen abzubrechen.

AWS Management Console

Verwenden Sie die Konsole, um die Bereitstellung eines Umgebungsupdates abzubrechen, wie in den folgenden Schritten gezeigt.

1. In derAWS ProtonKonsole, wähleUmgebungenim Navigationsbereich.
2. Wählen Sie in der Liste der Umgebungen den Namen der Umgebung mit dem Bereitstellungsupdate aus, das Sie abbrechen möchten.
3. Wenn Ihr Update-Bereitstellungsstatus lautetIn Bearbeitung, wählen Sie auf der UmgebungsdetailseiteAktionenund dannBereitstellung abbrechen.
4. In einem Modal werden Sie aufgefordert, zu bestätigen, dass Sie stornieren möchten. Wählen SieBereitstellung abbrechen.
5. Ihr Update-Bereitstellungsstatus ist auf festgelegtStornierenund dannAbgesagtum die Stornierung abzuschließen.

AWS CLI

Benutze dieAWS Proton AWS CLIum die Bereitstellung eines IN_PROGRESS-Umgebungsupdates auf eine neue Nebenversion 2 abzubrechen.

Die für dieses Beispiel verwendete Vorlage enthält eine Wartebedingung, sodass der Abbruch beginnt, bevor das Update erfolgreich bereitgestellt wird.

Führen Sie den folgenden Befehl aus, um das Update abzubrechen:

```
$ aws proton cancel-environment-deployment \
        --environment-name "MySimpleEnv"
```

Antwort:

```
{
    "environment": {
        "arn": "arn:aws:proton:region-id:123456789012:environment/MySimpleEnv",
```

```
        "createdAt": "2021-04-02T17:29:55.472000+00:00",
        "deploymentStatus": "CANCELLING",
        "lastDeploymentAttemptedAt": "2021-04-02T18:15:10.243000+00:00",
        "lastDeploymentSucceededAt": "2021-04-02T17:48:26.307000+00:00",
        "name": "MySimpleEnv",
        "protonServiceRoleArn": "arn:aws:iam::123456789012:role/service-role/
ProtonServiceRole",
        "spec": "proton: EnvironmentSpec\n\nspec:\n  my_sample_input: hello\n
 my_other_sample_input: everybody\n",
        "templateMajorVersion": "1",
        "templateMinorVersion": "1",
        "templateName": "simple-env"
    }
}
```

Führen Sie den folgenden Befehl aus, um den Status abzurufen und zu bestätigen:“

```
$ aws proton get-environment \
        --name "MySimpleEnv"
```

Antwort:

```
{
    "environment": {
        "arn": "arn:aws:proton:region-id:123456789012:environment/MySimpleEnv",
        "createdAt": "2021-04-02T17:29:55.472000+00:00",
        "deploymentStatus": "CANCELLED",
        "deploymentStatusMessage": "User initiated cancellation.",
        "lastDeploymentAttemptedAt": "2021-04-02T18:15:10.243000+00:00",
        "lastDeploymentSucceededAt": "2021-04-02T17:48:26.307000+00:00",
        "name": "MySimpleEnv",
        "protonServiceRoleArn": "arn:aws:iam::123456789012:role/service-role/
ProtonServiceRole",
        "spec": "proton: EnvironmentSpec\n\nspec:\n  my_sample_input: hello\n
 my_other_sample_input: everybody\n",
        "templateMajorVersion": "1",
        "templateMinorVersion": "1",
        "templateName": "simple-env"
    }
}
```

Löschen Sie eine Umgebung

Sie können eine löschenAWS ProtonUmgebung mithilfe derAWS ProtonKonsole oder dieAWS CLI.

> **Note**
>
> Sie können keine Umgebung löschen, der eine Komponente zugeordnet ist. Um eine solche Umgebung zu löschen, sollten Sie zunächst alle Komponenten löschen, die in der Umgebung ausgeführt werden. Weitere Hinweise zu Komponenten finden Sie unterKomponenten.

AWS Management Console

Löschen Sie eine Umgebung mithilfe der Konsole, wie in den folgenden beiden Optionen beschrieben.

In der Liste der Umgebungen.

1. In derAWS ProtonKonsole, wähleUmgebungen.
2. Wählen Sie in der Liste der Umgebungen das Optionsfeld links neben der Umgebung aus, die Sie löschen möchten.
3. Wählen SieAktionenund dannLöschen.
4. Ein Modal fordert Sie auf, die Löschaktion zu bestätigen.
5. Folgen Sie den Anweisungen und wählen SieJa, löschen.

Auf der Seite mit den Umgebungsdetails.

1. In derAWS ProtonKonsole, wähleUmgebungen.
2. Wählen Sie in der Liste der Umgebungen den Namen der Umgebung aus, die Sie löschen möchten.
3. Wählen Sie auf der UmgebungsdetailseiteAktionenund dannLöschen.
4. Ein Modal fordert Sie auf, zu bestätigen, dass Sie löschen möchten.
5. Folgen Sie den Anweisungen und wählen SieJa, löschen.

AWS CLI

Benutze dieAWS CLIum eine Umgebung zu löschen.

Tun Sie es nichtlöscht eine Umgebung, wenn Dienste oder Dienstinstanzen in der Umgebung bereitgestellt werden.

Führen Sie den Befehl aus:

```
$ aws proton delete-environment \
    --name "MySimpleEnv"
```

Antwort:

```
{
    "environment": {
        "arn": "arn:aws:proton:region-id:123456789012:environment/MySimpleEnv",
        "createdAt": "2021-04-02T17:29:55.472000+00:00",
        "deploymentStatus": "DELETE_IN_PROGRESS",
        "lastDeploymentAttemptedAt": "2021-04-02T17:48:26.307000+00:00",
        "lastDeploymentSucceededAt": "2021-04-02T17:48:26.307000+00:00",
        "name": "MySimpleEnv",
        "protonServiceRoleArn": "arn:aws:iam::123456789012:role/ProtonServiceRole",
        "templateMajorVersion": "1",
        "templateMinorVersion": "1",
        "templateName": "simple-env"
    }
}
```

Verbindungen zu Umgebungskonten

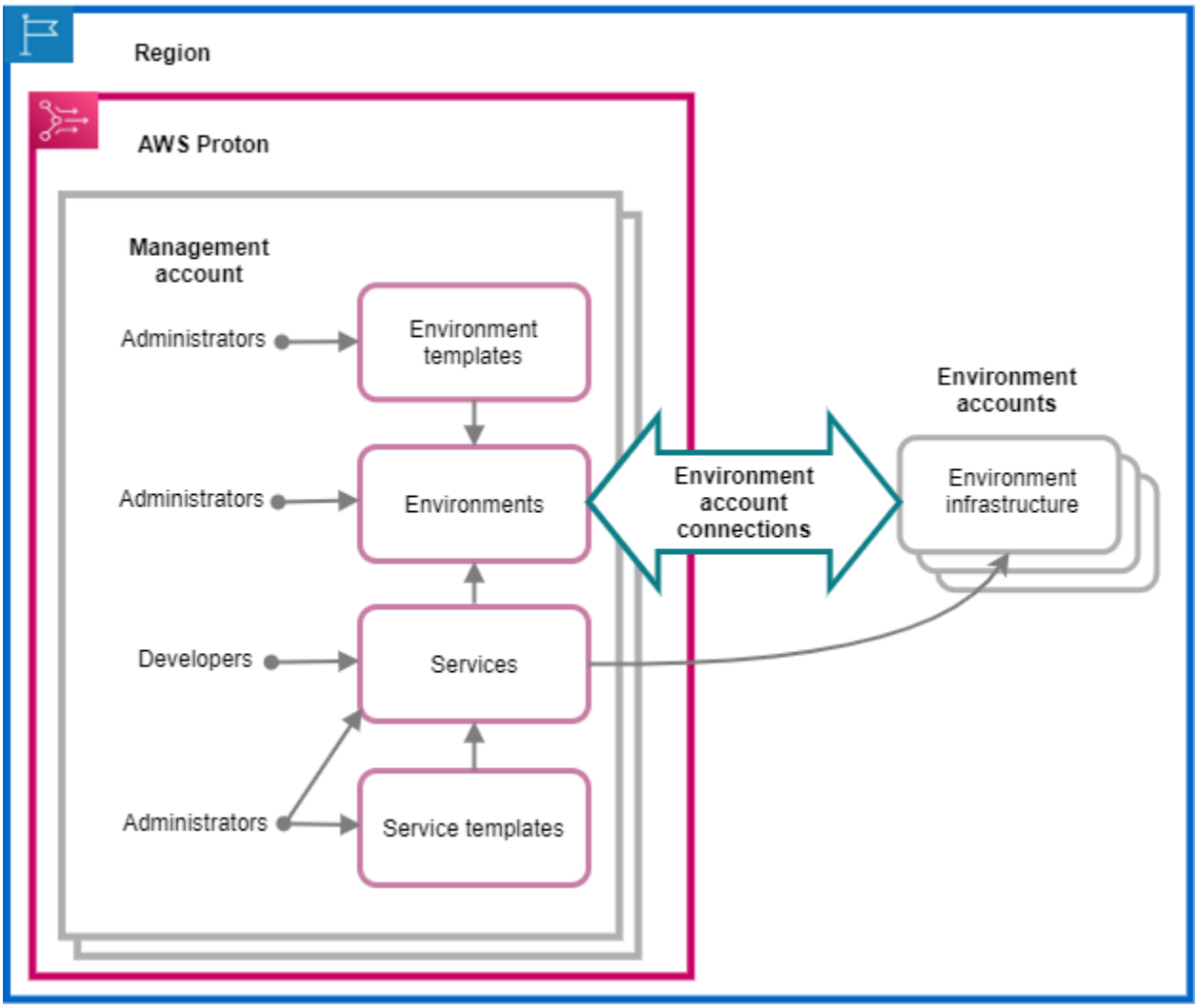
Übersicht

Erfahren Sie, wie Sie eine erstellen und verwaltenAWS ProtonUmgebung in einem Konto und Bereitstellung seiner Infrastrukturressourcen in einem anderen Konto. Dies kann dazu beitragen, die Sichtbarkeit und Effizienz im großen Maßstab zu verbessern. Verbindungen zu Umgebungskonten unterstützen nur die Standardbereitstellung mitAWS CloudFormationInfrastruktur als Code.

> **Note**
>
> Die Informationen in diesem Thema sind relevant für Umgebungen, die konfiguriert sind mitAWSverwaltete Bereitstellung. Mit Umgebungen, die konfiguriert sind mitselbstverwaltete Bereitstellung,AWS Protonstellt Ihre Infrastruktur nicht direkt bereit. Stattdessen sendet es

Pull-Requests (PRs) zur Bereitstellung an Ihr Repository. Es liegt in Ihrer Verantwortung sicherzustellen, dass Ihr Automatisierungscode die richtige Identität und Rolle annimmt. Weitere Hinweise zu Bereitstellungsmethoden finden Sie unterthe section called “Methoden der Provisioned”.

Terminologie



MitAWS Proton Verbindungen zu Umgebungskonten, Sie können eine erstellenAWS ProtonUmgebung von einem Konto aus und Bereitstellung der Infrastruktur in einem anderen Konto.

Verwaltungskonto

Das einzige Konto, in dem Sie als Administrator einAWS ProtonUmgebung, die Infrastrukturressourcen in einer anderen bereitstelltUmweltkonto.

Umweltkonto

Ein Konto, in dem die Umgebungsinfrastruktur bereitgestellt wird, wenn Sie einAWS ProtonUmgebung in einem anderen Konto.

Verbindung zum Umgebungskonto

Eine sichere bidirektionale Verbindung zwischen einemVerwaltungskontound einUmweltkonto. Es verwaltet Autorisierungen und Berechtigungen, wie in den folgenden Abschnitten weiter beschrieben.

Wenn Sie eine Umgebungskontoverbindung in einem Umgebungskonto in einer bestimmten Region erstellen, können nur die Verwaltungskonten in derselben Region die Umgebungskontoverbindung sehen und verwenden. Das bedeutet, dass derAWS ProtonDie im Verwaltungskonto erstellte Umgebung und die im Umgebungskonto bereitgestellte Umgebungsinfrastruktur müssen sich in derselben Region befinden.

Überlegungen zur Verbindung mit dem Umgebungskonto

- Sie benötigen eine Umgebungskontoverbindung für jede Umgebung, die Sie in einem Umgebungskonto bereitstellen möchten.
- Hinweise zu Kontingenten für Verbindungen von Umgebungskonten finden Sie unterAWS Proton-Kontingente.

Markieren

Verwenden Sie im Umgebungskonto die Konsole oderAWS CLIum von Kunden verwaltete Tags zur Umgebungskontoverbindung einzusehen und zu verwalten.AWSverwaltete Schlagwortesind nichtgeneriert für Verbindungen mit Umgebungskonten. Weitere Informationen finden Sie unter Markierung.

Erstellen Sie eine Umgebung in einem Konto und stellen Sie die zugehörige Infrastruktur in einem anderen Konto bereit

Um eine Umgebung von einem einzigen Verwaltungskonto aus zu erstellen und bereitzustellen, richten Sie ein Umgebungskonto für eine Umgebung ein, die Sie erstellen möchten.

Starten Sie im Umgebungskonto und stellen Sie eine Verbindung her.

Erstellen Sie im Umgebungskonto einAWS ProtonServicerolle, die nur auf die Berechtigungen beschränkt ist, die für die Bereitstellung Ihrer Umgebungsinfrastrukturressourcen erforderlich sind. Weitere Informationen finden Sie unter AWS ProtonServicerolle für die Bereitstellung mit AWS CloudFormation.

Erstellen Sie dann eine Anfrage zur Verbindung eines Umgebungskontos und senden Sie sie an Ihr Verwaltungskonto. Wenn die Anfrage akzeptiert wird,AWS Protonkann die zugehörige IAM-Rolle verwenden, die die Bereitstellung von Umgebungsressourcen im zugehörigen Umgebungskonto ermöglicht.

Akzeptieren oder lehnen Sie im Verwaltungskonto die Verbindung mit dem Umgebungskonto ab.

Akzeptieren oder lehnen Sie im Verwaltungskonto die Verbindungsanfrage für das Umgebungskonto ab. Dukann nichtlöschen Sie eine Umgebungskontoverbindung aus Ihrem Verwaltungskonto.

Wenn Sie die Anfrage annehmen,AWS Protonkann die zugehörige IAM-Rolle verwenden, die die Ressourcenbereitstellung im zugehörigen Umgebungskonto ermöglicht.

Die Ressourcen der Umgebungsinfrastruktur werden im zugehörigen Umgebungskonto bereitgestellt. Du kannst nur verwendenAWS ProtonAPIs für den Zugriff auf und die Verwaltung Ihrer Umgebung und ihrer Infrastrukturressourcen von Ihrem Verwaltungskonto aus. Weitere Informationen erhalten Sie unter Erstellen Sie eine Umgebung in einem Konto und stellen Sie in einem anderen Konto eine Bereitstellung bereit und Eine Umgebung aktualisieren.

Nachdem Sie eine Anfrage abgelehnt haben,kann nichtakzeptieren oder verwenden Sie die abgelehnte Umgebungskontoverbindung.

> **Note**
>
> Dukann nichtlehnt eine Verbindung mit einem Umgebungskonto ab, die mit einer Umgebung verbunden ist. Um die Verbindung mit dem Umgebungskonto abzulehnen, müssen Sie zuerst die zugehörige Umgebung löschen.

Greifen Sie im Umgebungskonto auf die bereitgestellten Infrastrukturressourcen zu.

Im Umgebungskonto können Sie die bereitgestellten Infrastrukturressourcen einsehen und darauf zugreifen. Sie können zum Beispiel verwendenCloudFormationAPI-Aktionen zur Überwachung und Bereinigung von Stacks, falls erforderlich. Du kannst das nicht benutzenAWS ProtonAPI-

Aktionen für den Zugriff auf oder die Verwaltung derAWS ProtonUmgebung, die zur Bereitstellung der Infrastrukturressourcen verwendet wurde.

Im Umgebungskonto können Sie Umgebungskontoverbindungen löschen, die Sie im Umgebungskonto erstellt haben. Dukann nichtakzeptiere oder lehne sie ab. Wenn Sie eine Umgebungskontoverbindung löschen, die von einem verwendet wirdAWS ProtonUmwelt,AWS Protonkann die Ressourcen der Umgebungsinfrastruktur erst verwalten, wenn eine neue Umgebungsverbindung für das Umgebungskonto und die benannte Umgebung akzeptiert wird. Sie sind dafür verantwortlich, bereitgestellte Ressourcen zu bereinigen, die keine Umgebungsverbindung haben.

Verwenden Sie die Konsole oder CLI, um Verbindungen zu Umgebungskonten zu verwalten

Sie können die Konsole oder die CLI verwenden, um Umgebungskontoverbindungen zu erstellen und zu verwalten.

AWS Management Console

Verwenden Sie die Konsole, um eine Verbindung zu einem Umgebungskonto herzustellen, und senden Sie eine Anfrage an das Verwaltungskonto, wie in den nächsten Schritten gezeigt.

1. Entscheiden Sie sich für einen Namen für die Umgebung, die Sie in Ihrem Verwaltungskonto erstellen möchten, oder wählen Sie den Namen einer vorhandenen Umgebung, für die eine Verbindung mit dem Umgebungskonto erforderlich ist.
2. In einem Umweltkonto, in derAWS ProtonKonsole, wähleVerbindungen zu Umgebungskontenim Navigationsbereich.
3. In derVerbindungen zu UmgebungskontenSeite, wählenAnfrage zur Verbindung.

   > **Note**
   >
   > Überprüfen Sie die Konto-ID, die imVerbindung zum UmgebungskontoSeitenüberschrift. Stellen Sie sicher, dass sie mit der Konto-ID des Umgebungskontos übereinstimmt, in dem Ihre benannte Umgebung bereitgestellt werden soll.

4. In derAnfrage zur Verbindungseite:

a. In derStellen Sie eine Verbindung zum Verwaltungskonto herAbschnitt, geben Sie den einID des Verwaltungskontosund derName der Umgebungdie Sie in Schritt 1 eingegeben haben.

b. In derRolle UmweltAbschnitt, wählenNeue ServicerolleundAWS Protonerstellt automatisch eine neue Rolle für Sie. Oder wählen SieBestehende Servicerolleund der Name der Servicerolle, die Sie zuvor erstellt haben.

> **Note**
>
> Die Rolle, dieAWS Protonerstellt automatisch für Sie und verfügt über weitreichende Berechtigungen. Wir empfehlen, dass Sie die Rolle auf die Berechtigungen beschränken, die für die Bereitstellung Ihrer Umgebungsinfrastrukturressourcen erforderlich sind. Weitere Informationen finden Sie unter AWS ProtonServicerolle für die Bereitstellung mit AWS CloudFormation.

c. (Optional) In derSchlagworteAbschnitt, wählenNeues Schlagwort hinzufügenum ein vom Kunden verwaltetes Tag für Ihre Umgebungskontoverbindung zu erstellen.

d. Wählen SieAnfrage zur Verbindung.

5. Ihre Anfrage wird als ausstehend angezeigt in derUmgebungsverbindungen, die an ein Verwaltungskonto gesendet wurdenEine Tabelle und ein Modal informieren Sie darüber, wie Sie die Anfrage vom Verwaltungskonto aus annehmen können.

Eine Anfrage zur Verbindung eines Umgebungskontos annehmen oder ablehnen.

1. In einem Verwaltungskonto, in derAWS ProtonKonsole, wähleVerbindungen zu Umgebungskontenim Navigationsbereich.
2. In derVerbindungen zu UmgebungskontenSeite, in derVerbindungsanfragen für UmgebungskontenTabelle, wählen Sie die Umgebungsverbindungsanfrage aus, die akzeptiert oder abgelehnt werden soll.

> **Note**
>
> Überprüfen Sie die Konto-ID, die imVerbindung zum UmgebungskontoSeitenüberschrift. Vergewissern Sie sich, dass es mit der Konto-ID des Verwaltungskontos übereinstimmt, das mit der zurückzuweisenden

Umgebungskontoverbindung verknüpft ist. Nachdem Sie diese Verbindung mit dem Umgebungskonto abgelehnt haben,kann nichtakzeptieren oder verwenden Sie die abgelehnte Umgebungskontoverbindung.

3. Wählen SieAblehnenoderAkzeptieren.

   - Wenn du ausgewählt hastAblehnen, der Status ändert sich vonausstehendzuzurückgewiesen.
   - Wenn du ausgewählt hastAkzeptieren, der Status ändert sich vonausstehendzuverbunden.

Löscht eine Verbindung mit einem Umgebungskonto.

1. In einem Umweltkonto, in derAWS ProtonKonsole, wähleVerbindungen zu Umgebungskontenim Navigationsbereich.

   > **Note**
   >
   > Überprüfen Sie die Konto-ID, die imVerbindung zum UmgebungskontoSeitenüberschrift. Vergewissern Sie sich, dass es mit der Konto-ID des Verwaltungskontos übereinstimmt, das mit der zurückzuweisenden Umgebungskontoverbindung verknüpft ist. Nachdem Sie diese Umgebungskontoverbindung gelöscht haben,AWS Proton kann nichtverwalten Sie die Ressourcen der Umgebungsinfrastruktur im Umgebungskonto. Es kann es erst verwalten, nachdem eine neue Umgebungskontoverbindung für das Umgebungskonto und die benannte Umgebung vom Verwaltungskonto akzeptiert wurden.

2. In derVerbindungen zu UmgebungskontenSeite, in derGesendete Anfragen zur Verbindung mit dem VerwaltungskontoAbschnitt, wählenLöschen.
3. Ein Modal fordert Sie auf, zu bestätigen, dass Sie löschen möchten. Wählen Sie Löschen.

AWS CLI

Entscheiden Sie sich für einen Namen für die Umgebung, die Sie in Ihrem Verwaltungskonto erstellen möchten, oder wählen Sie den Namen einer vorhandenen Umgebung, für die eine Verbindung mit dem Umgebungskonto erforderlich ist.

Erstellen Sie eine Umgebungskontoverbindung in einem Umgebungskonto.

Führen Sie den Befehl aus:

```
$ aws proton create-environment-account-connection \
    --environment-name "simple-env-connected" \
    --role-arn "arn:aws:iam::222222222222:role/service-role/env-account-proton-service-role" \
    --management-account-id "111111111111"
```

Antwort:

```
{
    "environmentAccountConnection": {
        "arn": "arn:aws:proton:region-id:222222222222:environment-account-connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "environmentAccountId": "222222222222",
        "environmentName": "simple-env-connected",
        "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "lastModifiedAt": "2021-04-28T23:13:50.847000+00:00",
        "managementAccountId": "111111111111",
        "requestedAt": "2021-04-28T23:13:50.847000+00:00",
        "roleArn": "arn:aws:iam::222222222222:role/service-role/env-account-proton-service-role",
        "status": "PENDING"
    }
}
```

Akzeptieren oder lehnen Sie eine Verbindung mit einem Umgebungskonto in einem Verwaltungskonto ab, wie im folgenden Befehl und in der folgenden Antwort dargestellt.

> **Note**
>
> Wenn Sie diese Umgebungskontoverbindung ablehnen, können Sie die abgelehnte Umgebungskontoverbindung nicht akzeptieren oder verwenden.

Wenn Sie angebenAblehnen, der Status ändert sich vonausstehendzuzurückgewiesen.

Wenn Sie angebenAkzeptieren, der Status ändert sich vonausstehendzuverbunden.

Führen Sie den folgenden Befehl aus, um die Verbindung mit dem Umgebungskonto zu akzeptieren:

```
$ aws proton accept-environment-account-connection \
    --id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Antwort:

```
{
    "environmentAccountConnection": {
        "arn": "arn:aws:proton:region-id:222222222222:environment-account-
connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "environmentAccountId": "222222222222",
        "environmentName": "simple-env-connected",
        "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "lastModifiedAt": "2021-04-28T23:15:33.486000+00:00",
        "managementAccountId": "111111111111",
        "requestedAt": "2021-04-28T23:13:50.847000+00:00",
        "roleArn": "arn:aws:iam::222222222222:role/service-role/env-account-proton-
service-role",
        "status": "CONNECTED"
    }
}
```

Führen Sie den folgenden Befehl aus, um die Verbindung mit dem Umgebungskonto abzulehnen:

```
$ aws proton reject-environment-account-connection \
    --id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Antwort:

```
{
    "environmentAccountConnection": {
        "arn": "arn:aws:proton:us-east-1:222222222222:environment-account-
connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "status": "REJECTED",
        "environmentAccountId": "222222222222",
        "environmentName": "simple-env-reject",
        "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "lastModifiedAt": "2021-04-28T23:13:50.847000+00:00",
        "managementAccountId": "111111111111",
        "requestedAt": "2021-04-28T23:13:50.847000+00:00",
        "roleArn": "arn:aws:iam::222222222222:role/service-role/env-account-proton-
service-role"
    }
```

```
}
```

Sehen Sie sich die Verbindungen eines Umgebungskontos an. Du kannsterhaltenoderListeVerbindungen zu Umgebungskonten.

Führen Sie den folgenden Befehl get aus:

```
$ aws proton get-environment-account-connection \
    --id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Antwort:

```
{
    "environmentAccountConnection": {
        "arn": "arn:aws:proton:region-id:222222222222:environment-account-
connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "environmentAccountId": "222222222222",
        "environmentName": "simple-env-connected",
        "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "lastModifiedAt": "2021-04-28T23:15:33.486000+00:00",
        "managementAccountId": "111111111111",
        "requestedAt": "2021-04-28T23:13:50.847000+00:00",
        "roleArn": "arn:aws:iam::222222222222:role/service-role/env-account-proton-
service-role",
        "status": "CONNECTED"
    }
}
```

Löschen Sie eine Umgebungskontoverbindung in einem Umgebungskonto.

> **Note**
>
> Wenn Sie diese Umgebungskontoverbindung löschen,AWS Protonkann die Umgebungsinfrastrukturressourcen im Umgebungskonto erst verwalten, wenn eine neue Umgebungsverbindung für das Umgebungskonto und die benannte Umgebung akzeptiert wurde. Sie sind dafür verantwortlich, bereitgestellte Ressourcen zu bereinigen, die keine Umgebungsverbindung haben.

Führen Sie den Befehl aus:

```
$ aws proton delete-environment-account-connection \
    --id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Antwort:

```
{
    "environmentAccountConnection": {
        "arn": "arn:aws:proton:us-east-1:222222222222:environment-account-
connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "environmentAccountId": "222222222222",
        "environmentName": "simple-env-connected",
        "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "lastModifiedAt": "2021-04-28T23:13:50.847000+00:00",
        "managementAccountId": "111111111111",
        "requestedAt": "2021-04-28T23:13:50.847000+00:00",
        "roleArn": "arn:aws:iam::222222222222:role/service-role/env-account-proton-
service-role",
        "status": "CONNECTED"
    }
}
```

Vom Kunden verwaltete Umgebungen

In vom Kunden verwalteten Umgebungen können Sie die vorhandene Infrastruktur verwenden, z. B. eine VPC, die Sie bereits als IhreAWS ProtonUmwelt. Bei der Verwendung von kundenverwalteten Umgebungen können Sie Ihre eigenen gemeinsam genutzten Ressourcen außerhalb von bereitstellenAWS Proton. Sie können jedoch immer noch zulassenAWS Protonum relevante Bereitstellungsausgaben als Eingaben zu nutzen fürAWS ProtonDienste, wenn sie bereitgestellt werden. Wenn sich die Ausgänge ändern können,AWS Protonkann Updates akzeptieren.AWS Protonkann die Umgebung jedoch nicht direkt ändern, da die Bereitstellung außerhalb von verwaltet wirdAWS Proton.

Nachdem die Umgebung erstellt wurde, sind Sie dafür verantwortlich, dieselben Ausgaben fürAWS Protondas wäre entstanden, wennAWS Protonhatte die Umgebung erstellt, z. B. Amazon ECS-Clusternamen oder Amazon VPC-IDs.

Mit dieser Funktion können Sie bereitstellen und aktualisierenAWS ProtonServiceressourcen von einemAWS ProtonDienstvorlage für diese Umgebung. Die Umgebung selbst wird jedoch nicht durch

Vorlagenaktualisierungen in geändertAWS Proton. Sie sind verantwortlich für die Ausführung von Updates für die Umgebung und die Aktualisierung dieser Ausgaben inAWS Proton.

Sie können mehrere Umgebungen in einem einzigen Konto haben, die eine Mischung ausAWS Protonverwaltete und vom Kunden verwaltete Umgebungen. Sie können auch ein zweites Konto verknüpfen und ein verwendenAWS ProtonVorlage im Hauptkonto zur Ausführung von Bereitstellungen und Updates für Umgebungen und Dienste in diesem zweiten, verknüpften Konto.

So verwenden Sie von Kunden verwaltete Umgebungen

Als Erstes müssen Administratoren eine importierte, vom Kunden verwaltete Umgebungsvorlage registrieren. Stellen Sie im Vorlagenpaket keine Manifeste oder Infrastrukturdateien bereit. Geben Sie nur das Schema an.

Das folgende Schema umreißt eine Liste von Ausgaben, die das offene API-Format verwenden, und repliziert die Ausgaben von einemAWS CloudFormationVorlage.

> **Important**
>
> Für die Ausgaben sind nur Zeichenketteneingaben zulässig.

Das folgende Beispiel ist ein Ausschnitt aus den Ausgabeabschnitten einesAWS CloudFormationVorlage für ein entsprechendes Fargate-Template.

```
Outputs:
  ClusterName:
    Description: The name of the ECS cluster
    Value: !Ref 'ECSCluster'
  ECSTaskExecutionRole:
    Description: The ARN of the ECS role
    Value: !GetAtt 'ECSTaskExecutionRole.Arn'
  VpcId:
    Description: The ID of the VPC that this stack is deployed in
    Value: !Ref 'VPC'
[...]
```

Das Schema für das entsprechendeAWS ProtonDie importierte Umgebung ähnelt der folgenden. Geben Sie keine Standardwerte im Schema an.

```
schema:
```

```
  format:
    openapi: "3.0.0"
  environment_input_type: "EnvironmentOutput"
  types:
    EnvironmentOutput:
      type: object
      description: "Outputs of the environment"
      properties:
        ClusterName:
          type: string
          description: "The name of the ECS cluster"
        ECSTaskExecutionRole:
          type: string
          description: "The ARN of the ECS role"
        VpcId:
          type: string
          description: "The ID of the VPC that this stack is deployed in"
[...]
```

Bei der Registrierung der Vorlage geben Sie an, dass diese Vorlage importiert wurde und den Amazon S3-Bucket-Speicherort für das Paket bereitstellt.AWS Protonbestätigt, dass das Schema nur enthält`environment_input_type`und neinAWS CloudFormationVorlagenparameter, bevor die Vorlage in den Entwurf aufgenommen wird.

Sie geben Folgendes an, um eine importierte Umgebung zu erstellen.

- Eine IAM-Rolle, die bei Bereitstellungen verwendet werden kann.
- Eine Spezifikation mit den Werten für die erforderlichen Ausgänge.

Sie können beide entweder über die Konsole oder über dieAWS CLImithilfe eines Prozesses, der der Bereitstellung einer regulären Umgebung ähnelt.

CodeBuildErstellung von Bereitstellungsrollen

Tools für Infrastruktur als Code (IaaC) wieAWS CloudFormationund Terraform benötigen Genehmigungen für die vielen verschiedenen Arten vonAWSRessourcen. Wenn eine IaaC-Vorlage beispielsweise einen Amazon S3-Bucket deklariert, benötigt sie Berechtigungen zum Erstellen, Lesen, Aktualisieren und Löschen von Amazon S3-Buckets. Es wird als bewährte Sicherheitsmethode angesehen, Rollen auf die erforderlichen Mindestberechtigungen zu beschränken. Angesichts der Breite vonAWSRessourcen, es ist schwierig, Least-Privilege-Richtlinien

für IaaC-Vorlagen zu erstellen, insbesondere, wenn sich die Ressourcen, die mit diesen Vorlagen verwaltet werden, später ändern können. Zum Beispiel in Ihren letzten Änderungen an einer Vorlage, die verwaltet wird vonAWS Proton, fügen Sie eine RDS-Datenbankressource hinzu.

Die Konfiguration der richtigen Berechtigungen trägt dazu bei, dass die Bereitstellung Ihres IaC reibungslos verläuft.AWS Proton CodeBuildProvisioning führt beliebige vom Kunden bereitgestellte CLI-Befehle in einem ausCodeBuildProjekt, das sich im Kundenkonto befindet. In der Regel erstellen und löschen diese Befehle eine Infrastruktur mithilfe eines IaaC-Tool (Infrastructure as Code) wieAWS CDK. Wenn einAWSRessourcen-Bereitstellungen, deren Vorlage verwendetCodeBuildBereitstellung,AWSwird einen Build in einem startenCodeBuildProjekt geleitet vonAWS. Eine Rolle wird übergeben anCodeBuild, welchesCodeBuildgeht davon aus, Befehle auszuführen. Diese Rolle, genannt dieCodeBuildDie Bereitstellungsrolle wird vom Kunden bereitgestellt und enthält die für die Bereitstellung der Infrastruktur erforderlichen Berechtigungen. Es soll nur angenommen werden vonCodeBuildund sogarAWS Protonkann es nicht annehmen.

Erstellen der -Rolle

DerCodeBuildDie Bereitstellungsrolle kann in der IAM-Konsole oder in derAWS CLI. Um es zu erstellen in derAWS CLI:

```
aws iam create-role --role-name AWSProtonCodeBuildProvisioning --assume-role-
policy-document '{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Principal":
{"Service":"codebuild.amazonaws.com"},"Action":"sts:AssumeRole"}]}'
aws iam attach-role-policy --role-name AWSProtonCodeBuildProvisioning --policy-arn
 arn:aws:iam::aws:policy/AWSProtonCodeBuildProvisioningBasicAccess
```

Dies fügt auch die`AWSProtonCodeBuildProvisioningBasicAccess`, das die Mindestberechtigungen enthält, die für dieCodeBuildDienst zum Ausführen eines Builds.

Wenn Sie es vorziehen, die Konsole zu verwenden, stellen Sie beim Erstellen der Rolle Folgendes sicher:

1. Wählen Sie für vertrauenswürdige EntitätAWSService und wählen Sie dannCodeBuild.
2. Wählen Sie im Schritt „Berechtigungen hinzufügen“`AWSProtonCodeBuildProvisioningBasicAccess`und alle anderen Richtlinien, die Sie anhängen möchten.

Administratorzugriff

Wenn Sie das anhängen`AdministratorAccess`Politik gegenüber demCodeBuildProvisioning Role garantiert, dass keine IaaC-Vorlage aufgrund fehlender Berechtigungen fehlschlägt. Dies bedeutet auch, dass jeder, der eine Umgebungs- oder Dienstvorlage erstellen kann, Aktionen auf Administratorebene ausführen kann, auch wenn dieser Benutzer kein Administrator ist.AWS Protonempfiehlt nicht die Verwendung`AdministatorAccess`mit demCodeBuildRolle zur Bereitstellung. Wenn Sie sich für die Verwendung entscheiden`AdministratorAccess`mit demCodeBuildProvisioning Role, tun Sie dies in einer Sandbox-Umgebung.

Sie können eine Rolle erstellen mit`AdministratorAccess`in der IAM-Konsole oder indem Sie diesen Befehl ausführen:

```
aws iam create-role --role-name AWSProtonCodeBuildProvisioning --assume-role-
policy-document '{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Principal":
{"Service":"codebuild.amazonaws.com"},"Action":"sts:AssumeRole"}]}'
aws iam attach-role-policy --role-name AWSProtonCodeBuildProvisioning --policy-arn
 arn:aws:iam::aws:policy/AdministratorAccess
```

Eine Rolle mit minimalem Umfang erstellen

Wenn Sie eine Rolle mit Mindestberechtigungen erstellen möchten, gibt es mehrere Möglichkeiten:

- Stellen Sie die Bereitstellung mit Administratorberechtigungen bereit und beschränken Sie dann den Umfang der Rolle. Wir empfehlen die VerwendungIAM Access Analyzer.
- Verwenden Sie verwaltete Richtlinien, um Zugriff auf die Dienste zu gewähren, die Sie nutzen möchten.

AWS CDK

Wenn du verwendestAWS CDKmitAWS Proton, und du bist geranntcdk bootstrapauf jedem Umgebungskonto/jeder Region, dann gibt es bereits eine Rolle fürcdk deploy. Fügen Sie in diesem Fall die folgende Richtlinie an dieCodeBuildRolle der Bereitstellung:

```
{
    "Action": "sts:AssumeRole",
    "Resource": [
        "arn:aws:iam::account-id:role/cdk-*-deploy-role-*",
        "arn:aws:iam::account-id:role/cdk-*-file-publishing-role-*"
    ],
    "Effect": "Allow"
```

```
}
```

Benutzerdefinierte VPC

Wenn du dich entscheidest zu rennenCodeBuildin einembenutzerdefinierte VPC, Sie benötigen die folgenden Berechtigungen in IhremCodeBuildRolle:

```
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateNetworkInterface"
    ],
    "Resource": [
        "arn:aws:ec2:region:account-id:network-interface/*",
        "arn:aws:ec2:region:account-id:subnet/*",
        "arn:aws:ec2:region:account-id:security-group/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:DeleteNetworkInterface"
    ],
    "Resource": [
        "arn:aws:ec2:region:account-id:*/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcs"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateNetworkInterfacePermission"
    ],
```

```
    "Resource": "arn:aws:ec2:region:account-id:network-interface/*",
    "Condition": {
        "StringEquals": {
            "ec2:AuthorizedService": "codebuild.amazonaws.com"
        }
    }
}
```

Sie könnten auch den verwendenAmazonEC2FullAccessverwaltete Richtlinie, obwohl diese Berechtigungen beinhaltet, die Sie möglicherweise nicht benötigen. Um die verwaltete Richtlinie mit der CLI anzuhängen:

```
aws iam create-role --role-name AWSProtonCodeBuildProvisioning --assume-role-
policy-document '{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Principal":
{"Service":"codebuild.amazonaws.com"},"Action":"sts:AssumeRole"}]}'
aws iam attach-role-policy --role-name AWSProtonCodeBuildProvisioning --policy-arn
 arn:aws:iam::aws:policy/AdministratorAccess
```

AWS Proton-Services

EinAWS Proton Service ist eine Instanziierung einer Service-Vorlage, die normalerweise mehrere Dienstinstanzen und eine Pipeline umfasst. EineAWS Proton Dienstinstanz ist eine Instanziierung einer Dienstvorlage in einer bestimmten Umgebung. Eine Service-Vorlage ist eine vollständige Definition der Infrastruktur und der optionalen Service-Pipeline für einenAWS Proton Service.

Nachdem Sie Ihre Service-Instanzen bereitgestellt haben, können Sie sie durch Quellcode-Pushes aktualisieren, die die CI/CD-Pipeline aufrufen, oder indem Sie den Service auf neue Versionen seiner Service-Vorlage aktualisieren. AWS Protonfordert Sie auf, wenn neue Versionen der Service-Vorlage verfügbar sind, damit Sie Ihre Dienste auf eine neue Version aktualisieren können. Wenn Ihr Service aktualisiert ist, werden der DienstAWS Proton und die Dienstinstanzen erneut bereitgestellt.

Dieses Kapitel zeigt, wie Sie Dienste mithilfe von Erstellungs-, Anzeigen-, Aktualisierungs- und Löschvorgängen verwalten. Weitere Informationen finden Sie in derAWS Proton Service API Reference.

Themen

Einen Service erstellen

Um eine Anwendung bereitzustellenAWS Proton, erstellen Sie als Entwickler einen Dienst und geben die folgenden Eingaben ein.

1. Der Name einerAWS Proton Service-Vorlage, die vom Plattformteam veröffentlicht wurde.
2. Ein Name für den Service.
3. Die Anzahl der Service-Instances, die Sie bereitstellen möchten.

4. Eine Auswahl von Umgebungen, die Sie verwenden möchten.
5. Eine Verbindung zu Ihrem Code-Repository, wenn Sie eine Service-Vorlage verwenden, die eine Service-Pipeline enthält (optional).

Was ist in einem Service enthalten?

Wenn Sie einenAWS Proton Service erstellen, können Sie aus zwei verschiedenen Typen von Servicevorlagen wählen:

- Eine Service-Vorlage, die eine Service-Pipeline enthält (Standard).
- Eine Service-Vorlage, die keine Service-Pipeline enthält.

Sie müssen mindestens eine Service-Instance erstellen, wenn Sie Ihren Service erstellen.

Eine Dienstinstanz und eine optionale Pipeline sind einem Dienst zugeordnet. Sie können eine Pipeline nur im Zusammenhang mit Aktionen zum Erstellen und Löschen von Diensten erstellen oder löschen. Wie Sie Instances zu einem Service hinzufügen und daraus entfernen, erfahren Sie unterDienst bearbeiten.

> **Note**
>
> Ihre Umgebung ist entweder für die Bereitstellung oderAWS für die selbstverwaltete Bereitstellung konfiguriert. AWS Protonstellt Dienste in einer Umgebung bereit, die dieselbe Bereitstellungsmethode wie die Umgebung verwendet. Der Entwickler, der Service-Instanzen erstellt oder aktualisiert, sieht den Unterschied nicht und seine Erfahrung ist in beiden Fällen dieselbe.
> Weitere Informationen zu Bereitstellungsmethoden finden Sie unterthe section called “Methoden der Provisioned”.

Servicevorlagen

Es sind sowohl Haupt- als auch Nebenversionen von Service-Templates verfügbar. Wenn Sie die Konsole verwenden, wählen Sie die neueste`Recommended` Haupt- und Nebenversion der Service-Vorlage aus. Wenn Sie das verwendenAWS CLI und nur die Hauptversion der Service-Vorlage angeben, geben Sie implizit die neueste`Recommended` Nebenversion an.

Im Folgenden werden der Unterschied zwischen Haupt- und Nebenversionen der Vorlagen und deren Verwendung beschrieben.

- Neue Versionen einer Vorlage werden verfügbar,`Recommended` sobald sie von einem Mitglied des Plattformteams genehmigt wurden. Das bedeutet, dass neue Dienste mit dieser Version erstellt werden und Sie aufgefordert werden, vorhandene Dienste auf die neue Version zu aktualisieren.
- DadurchAWS Proton kann das Plattformteam Service-Instanzen automatisch auf eine neue Nebenversion einer Service-Vorlage aktualisieren. Kleinere Versionen müssen abwärtskompatibel sein.
- Da bei Hauptversionen im Rahmen des Aktualisierungsprozesses neue Eingaben erforderlich sind, müssen Sie Ihren Service auf eine Hauptversion seiner Service-Vorlage aktualisieren. Hauptversionen sind nicht abwärtskompatibel.

Einen Service erstellen

Die folgenden Verfahren zeigen, wie Sie dieAWS Proton Konsole verwenden oderAWS CLI einen Dienst mit oder ohne Service-Pipeline erstellen.

AWS Management Console

Erstellen Sie einen Dienst, wie in den folgenden Konsolenschritten gezeigt.

1. Wählen Sie in der AWS ProtonKonsole Dienste aus.
2. Wählen Sie Create service.
3. Wählen Sie auf der Seite „Dienstvorlage auswählen“ eine Vorlage aus und wählen Sie „Konfigurieren“.

   Wenn Sie keine aktivierte Pipeline verwenden möchten, wählen Sie eine Vorlage aus, die mit Excludes-Pipeline für Ihren Service gekennzeichnet ist.
4. Geben Sie auf der Seite Dienst konfigurieren im Abschnitt Diensteinstellungen einen Dienstnamen ein.
5. (Optional) Geben Sie eine Beschreibung für den Service ein.
6. Gehen Sie im Abschnitt Einstellungen für das Service-Repository wie folgt vor:

   a. Wählen Sie unter CodeStar Verbindung Ihre Verbindung aus der Liste aus.

   b. Wählen Sie als Repository-ID den Namen Ihres Quellcode-Repositorys aus der Liste aus.

c. Wählen Sie als Branch-Name den Namen Ihres Quellcode-Repository-Zweigs aus der Liste aus.

7. (Optional) Wählen Sie im Abschnitt „Stichwörter“ die Option „Neuen Tag hinzufügen“ und geben Sie einen Schlüssel und einen Wert ein, um ein vom Kunden verwaltetes Tag zu erstellen.
8. Wählen Sie Next (Weiter).
9. Auf der Seite Benutzerdefinierte Einstellungen konfigurieren, im Abschnitt Dienstinstanzen, im Abschnitt Neue Instanz. Sie müssen Werte für die`required` Parameter eingeben. Sie können Werte für die`optional` Parameter eingeben oder die Standardwerte verwenden, sofern angegeben.
10. Im Abschnitt Pipeline-Eingaben müssen Sie Werte für die`required` Parameter eingeben. Sie können Werte für die`optional` Parameter eingeben oder die Standardwerte verwenden, sofern angegeben.
11. Wählen Sie Weiter und überprüfen Sie Ihre Eingaben.
12. Wählen Sie Create (Erstellen) aus.

    Sehen Sie sich die Servicedetails und den Status sowie dieAWS verwalteten Tags und vom Kunden verwalteten Tags für Ihren Service an.
13. Wählen Sie im Navigationsbereich -Services aus.

    Auf einer neuen Seite wird eine Liste Ihrer Dienste zusammen mit dem Status und anderen Servicedetails angezeigt.

AWS CLI

Wenn Sie den verwendenAWS CLI, geben Sie Diensteingaben in einer YAML-formatierten`spec` Datei an`.aws-proton/service.yaml`, die sich in Ihrem Quellcodeverzeichnis befindet.

Sie können den`get-service-template-minor-version` CLI-Befehl verwenden, um das erforderliche Schema und die optionalen Parameter anzuzeigen, für die Sie Werte in Ihrer Spezifikationsdatei angeben.

Wenn Sie eine Service-Vorlage verwenden möchten, die hat`pipelineProvisioning: "CUSTOMER_MANAGED"`, nehmen Sie den`pipeline:` Abschnitt nicht in Ihre Spezifikation auf und schließen *`-repository-connection-arn`*Sie keine`-branch-name` Parameter in Ihren`create-service` Befehl ein.`-repository-id`

Erstellen Sie einen Service mit einer Service-Pipeline, wie in den folgenden CLI-Schritten gezeigt.

1. Richten Sie die Servicerolle für die Pipeline ein, wie im folgenden CLI-Beispielbefehl gezeigt.

   Befehl:

```
$ aws proton update-account-settings \
        --pipeline-service-role-arn
 "arn:aws:iam::123456789012:role/AWSProtonServiceRole"
```

2. Die folgende Liste zeigt eine Beispielspezifikation, die auf dem Service-Template-Schema basiert und die Service-Pipeline und Instanzeingaben enthält.

   Spezifikation:

```
proton: ServiceSpec

pipeline:
  my_sample_pipeline_required_input: "hello"
  my_sample_pipeline_optional_input: "bye"

instances:
  - name: "acme-network-dev"
    environment: "ENV_NAME"
    spec:
      my_sample_service_instance_required_input: "hi"
      my_sample_service_instance_optional_input: "ho"
```

   Erstellen Sie einen Dienst mit einer Pipeline, wie im folgenden CLI-Beispiel für Befehl und Antwort gezeigt.

   Befehl:

```
$ aws proton create-service \
        --name "MySimpleService" \
        --branch-name "mainline" \
        --template-major-version "1" \
        --template-name "fargate-service" \
        --repository-connection-arn "arn:aws:codestar-connections:region-
id:123456789012:connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
        --repository-id "myorg/myapp" \
        --spec "file://spec.yaml"
```

Antwort:

```
{
    "service": {
        "arn": "arn:aws:proton:region-id:123456789012:service/MySimpleService",
        "createdAt": "2020-11-18T19:50:27.460000+00:00",
        "lastModifiedAt": "2020-11-18T19:50:27.460000+00:00",
        "name": "MySimpleService",
        "repositoryConnectionArn": "arn:aws:codestar-connections:region-
id:123456789012:connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "repositoryId": "myorg/myapp",
        "status": "CREATE_IN_PROGRESS",
        "templateName": "fargate-service"
    }
}
```

Erstellen Sie einen Dienst ohne Service-Pipeline, wie im folgenden CLI-Beispiel für Befehl und Antwort gezeigt.

Im Folgenden wird eine Beispielspezifikation gezeigt, die keine Service-Pipeline-Eingaben enthält.

Spezifikation:

```
proton: ServiceSpec

instances:
  - name: "acme-network-dev"
    environment: "ENV_NAME"
    spec:
      my_sample_service_instance_required_input: "hi"
      my_sample_service_instance_optional_input: "ho"
```

Um einen Service ohne bereitgestellte Service-Pipeline zu erstellen, geben Sie den Pfad zu einem**`spec.yaml`** und Sie schließen keine Repository-Parameter ein, wie im folgenden CLI-Beispiel für Befehl und Antwort gezeigt.

Befehl:

```
$ aws proton create-service \
        --name "MySimpleServiceNoPipeline" \
```

```
        --template-major-version "1" \
        --template-name "fargate-service" \
        --spec "file://spec-no-pipeline.yaml"
```

Antwort:

```
{
    "service": {
        "arn": "arn:aws:proton:region-id:123456789012:service/
MySimpleServiceNoPipeline",
        "createdAt": "2020-11-18T19:50:27.460000+00:00",
        "lastModifiedAt": "2020-11-18T19:50:27.460000+00:00",
        "name": "MySimpleServiceNoPipeline",
        "status": "CREATE_IN_PROGRESS",
        "templateName": "fargate-service-no-pipeline"
    }
}
```

Anzeigen von Servicedaten

Sie können Dienstdetaildaten mit derAWS Proton Konsole oder der anzeigen und auflistenAWS CLI.

AWS Management Console

Listet Servicedetails mithilfe der AWS ProtonKonsole auf und zeigt sie an, wie in den folgenden Schritten gezeigt.

1. Um eine Liste Ihrer Dienste anzuzeigen, wählen Sie im Navigationsbereich Dienste aus.
2. Um Detaildaten anzuzeigen, wählen Sie den Namen eines Dienstes.

   Anzeigen Ihrer ServiceDetails.

AWS CLI

Sehen Sie sich die Details eines Dienstes mit einer Service-Pipeline an, wie im folgenden CLI-Beispiel für Befehl und Antwort gezeigt.

Befehl:

```
$ aws proton get-service \
```

```
    --name "simple-svc"
```

Antwort:

```
{
    "service": {
        "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc",
        "branchName": "mainline",
        "createdAt": "2020-11-28T22:40:50.512000+00:00",
        "lastModifiedAt": "2020-11-28T22:44:51.207000+00:00",
        "name": "simple-svc",
        "pipeline": {
            "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc/
pipeline/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "createdAt": "2020-11-28T22:40:50.512000+00:00",
            "deploymentStatus": "SUCCEEDED",
            "lastDeploymentAttemptedAt": "2020-11-28T22:40:50.512000+00:00",
            "lastDeploymentSucceededAt": "2020-11-28T22:40:50.512000+00:00",
            "spec": "proton: ServiceSpec\npipeline:\n
 my_sample_pipeline_required_input: hello\n  my_sample_pipeline_optional_input:
 bye\ninstances:\n- name: instance-svc-simple\n  environment: my-simple-
env\n  spec:\n    my_sample_service_instance_required_input: hi\n
 my_sample_service_instance_optional_input: ho\n",
            "templateMajorVersion": "1",
            "templateMinorVersion": "1",
            "templateName": "svc-simple"
        },
        "repositoryConnectionArn": "arn:aws:codestar-connections:region-
id:123456789012:connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
        "repositoryId": "myorg/myapp",
        "spec": "proton: ServiceSpec\npipeline:\n
 my_sample_pipeline_required_input: hello\n  my_sample_pipeline_optional_input:
 bye\ninstances:\n- name: instance-svc-simple\n  environment: my-simple-
env\n  spec:\n    my_sample_service_instance_required_input: hi\n
 my_sample_service_instance_optional_input: ho\n",
        "status": "ACTIVE",
        "templateName": "svc-simple"
    }
}
```

Sehen Sie sich die Details eines Dienstes ohne Service-Pipeline an, wie im folgenden CLI-Beispiel für Befehl und Antwort gezeigt.

Befehl:

```
$ aws proton get-service \
    --name "simple-svc-no-pipeline"
```

Antwort:

```
{
    "service": {
        "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc-without-
pipeline",
        "createdAt": "2020-11-28T22:40:50.512000+00:00",
        "lastModifiedAt": "2020-11-28T22:44:51.207000+00:00",
        "name": "simple-svc-without-pipeline",
        "spec": "proton: ServiceSpec\ninstances:\n- name: instance-svc-simple\n
 environment: my-simple-env\n  spec:\n    my_sample_service_instance_required_input:
 hi\n    my_sample_service_instance_optional_input: ho\n",
        "status": "ACTIVE",
        "templateName": "svc-simple-no-pipeline"
    }
}
```

Dienst bearbeiten

Sie können die folgenden Änderungen an einemAWS Proton Dienst vornehmen.

- Bearbeiten der Servicebeschreibung.
- Bearbeiten Sie einen Dienst, indem Sie Dienstinstanzen hinzufügen und entfernen.

Servicebeschreibung bearbeiten

Sie können über die Konsole oder überAWS CLI eine Servicebeschreibung bearbeiten.

AWS Management Console

Bearbeiten Sie einen Service mithilfe der Konsole wie in den folgenden Schritten beschrieben.

In der Liste der Dienste.

1. Wählen Sie in der AWS ProtonKonsole Dienste aus.

2. Wählen Sie in der Liste der Services das Optionsfeld links neben dem Dienst aus, den Sie aktualisieren möchten.
3. Wählen Sie Edit (Bearbeiten) aus.
4. Füllen Sie auf der Seite Service konfigurieren das Formular aus und wählen Sie Weiter.
5. Wählen Sie auf der Seite Benutzerdefinierte Einstellungen konfigurieren die Option Weiter.
6. Überprüfen Sie Ihre Änderungen und wählen Sie Änderungen speichern.

Auf der Seite mit den Servicedetails.

1. Wählen Sie in der AWS ProtonKonsole Dienste aus.
2. Wählen Sie in der Liste der Services den Namen des anzuzeigenden Service.
3. Wählen Sie auf der Seite mit den Servicedetails die Option Bearbeiten aus.
4. Füllen Sie auf der Seite Service konfigurieren das Formular aus und wählen Sie Weiter.
5. Füllen Sie auf der Seite Benutzerdefinierte Einstellungen konfigurieren das Formular aus und wählen Sie Weiter.
6. Überprüfen Sie Ihre Änderungen und wählen Sie Änderungen speichern.

AWS CLI

Bearbeiten Sie eine Beschreibung wie im folgenden CLI-Beispiel für Befehl und Antwort gezeigt.

Befehl:

```
$ aws proton update-service \
    --name "MySimpleService" \
    --description "Edit by updating description"
```

Antwort:

```
{
    "service": {
        "arn": "arn:aws:proton:region-id:123456789012:service/MySimpleService",
        "branchName": "main",
        "createdAt": "2021-03-12T22:39:42.318000+00:00",
        "description": "Edit by updating description",
        "lastModifiedAt": "2021-03-12T22:44:21.975000+00:00",
```

```
        "name": "MySimpleService",
        "repositoryConnectionArn": "arn:aws:codestar-connections:region-
id:123456789012:connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "repositoryId": "my-repository/myorg-myapp",
        "status": "ACTIVE",
        "templateName": "fargate-service"
    }
}
```

Bearbeiten Sie einen Dienst, um Dienstinstanzen hinzuzufügen oder zu entfernen

Für einenAWS Proton Service können Sie Dienstinstanzen hinzufügen oder löschen, indem Sie eine bearbeitete Spezifikation einreichen. Für eine erfolgreiche Anfrage müssen die folgenden Bedingungen erfüllt sei:

- Ihr Service und Ihre Pipeline wurden nicht bereits bearbeitet oder gelöscht, als Sie die Bearbeitungsanfrage einreichen.
- Ihre bearbeitete Spezifikation umfasst keine Änderungen, die die Service-Pipeline ändern, oder Änderungen an vorhandenen Service-Instanzen, die nicht gelöscht werden sollen.
- Ihre bearbeitete Spezifikation entfernt keine vorhandene Dienstinstanz, die über eine angehängte Komponente verfügt. Um eine solche Dienstinstanz zu löschen, sollten Sie zuerst die Komponente aktualisieren, um sie von ihrer Dienstinstanz zu trennen. Weitere Informationen zu Komponenten finden Sie unterKomponenten.

Instanzen, bei denen das Löschen fehlgeschlagen ist, sind Dienstinstanzen im`DELETE_FAILED` Bundesstaat. Wenn Sie eine Service-Bearbeitung anfordern, wird im Rahmen des BearbeitungsprozessesAWS Proton versucht, die Instanzen, bei denen der Löschvorgang fehlgeschlagen ist, für Sie zu entfernen. Wenn eine Ihrer Service-Instanzen nicht gelöscht werden konnte, sind möglicherweise immer noch Ressourcen mit den Instanzen verknüpft, auch wenn sie von der Konsole oder aus nicht sichtbar sindAWS CLI. Überprüfen Sie die Infrastrukturressourcen Ihrer Instance, bei denen das Löschen fehlgeschlagen ist, und bereinigen Sie sie, damit sie für Sie entfernt werdenAWS Proton können.

Das Kontingent an Service-Instanzen für einen Service finden Sie unterAWS Proton-Kontingente. Sie müssen außerdem mindestens eine Service-Instance für Ihren Service verwalten, nachdem er erstellt wurde. Zählt während des Aktualisierungsvorgangs die vorhandenen Dienstinstanzen und

die Instanzen, die hinzugefügt oder entfernt werden sollen.AWS Proton Instanzen, bei denen das Löschen fehlgeschlagen ist, sind in dieser Anzahl enthalten. Sie müssen sie berücksichtigen, wenn Sie Ihre Instanzen bearbeitenspec.

Verwenden Sie die Konsole oderAWS CLI um Service-Instanzen hinzuzufügen oder zu entfernen

AWS Management Console

Bearbeiten Sie Ihren Service, um mithilfe der Konsole Service-Instanzen hinzuzufügen oder zu entfernen.

In der AWS ProtonKonsole

1. Wählen Sie im Navigationsbereich -Services aus.
2. Wählen Sie den Service aus, den Sie bearbeiten möchten.
3. Wählen Sie Edit (Bearbeiten) aus.
4. (Optional) Bearbeiten Sie auf der Seite „Service konfigurieren“ den Dienstnamen oder die Beschreibung und wählen Sie dann Weiter.
5. Wählen Sie auf der Seite Benutzerdefinierte Einstellungen konfigurieren die Option Löschen, um eine Dienstinstanz zu löschen, und wählen Sie Neue Instanz hinzufügen, um eine Dienstinstanz hinzuzufügen, und füllen Sie das Formular aus.
6. Wählen Sie Next (Weiter).
7. Überprüfen Sie Ihr Update und wählen Sie Änderungen speichern.
8. Ein Modal fordert Sie auf, das Löschen von Service-Instanzen zu überprüfen. Folgen Sie den Anweisungen und wählen Sie Ja, löschen.
9. Sehen Sie sich auf der Seite mit den Servicedetails die Statusdetails für Ihren Service an.

AWS CLI

Fügen Sie Dienstinstanzen hinzu und löschen Sie sie,**spec** wie im folgendenAWS CLI Beispiel gezeigt, Befehle und Antworten.

Wenn Sie die CLI verwenden,spec müssen Sie die zu löschenden Service-Instanzen ausschließen und sowohl die hinzuzufügenden Service-Instanzen als auch die vorhandenen Service-Instanzen, die Sie nicht zum Löschen markiert haben, einbeziehen.

Die folgende Liste zeigt das Beispiel`spec` vor der Bearbeitung und eine Liste der von der Spezifikation bereitgestellten Service-Instanzen. Diese Spezifikation wurde im vorherigen Beispiel für die Bearbeitung einer Servicebeschreibung verwendet.

Spezifikation:

```
proton: ServiceSpec

pipeline:
  my_sample_pipeline_optional_input: "abc"
  my_sample_pipeline_required_input: "123"

instances:
  - name: "my-instance"
    environment: "simple-env"
    spec:
      my_sample_service_instance_optional_input: "def"
      my_sample_service_instance_required_input: "456"
  - name: "my-other-instance"
    environment: "simple-env"
    spec:
      my_sample_service_instance_required_input: "789"
```

Der folgende`list-service-instances` CLI-Beispielbefehl mit Antwort zeigt die aktiven Instanzen vor dem Hinzufügen oder Löschen einer Dienstinstanz.

Befehl:

```
$ aws proton list-service-instances \
    --service-name "MySimpleService"
```

Antwort:

```
{
    "serviceInstances": [
        {
            "arn": "arn:aws:proton:region-id:123456789012:service/MySimpleService/
service-instance/my-other-instance",
            "createdAt": "2021-03-12T22:39:42.318000+00:00",
            "deploymentStatus": "SUCCEEDED",
            "environmentName": "simple-env",
            "lastDeploymentAttemptedAt": "2021-03-12T22:39:43.109000+00:00",
```

```
            "lastDeploymentSucceededAt": "2021-03-12T22:39:43.109000+00:00",
            "name": "my-other-instance",
            "serviceName": "example-svc",
            "templateMajorVersion": "1",
            "templateMinorVersion": "0",
            "templateName": "fargate-service"
        },
        {
            "arn": "arn:aws:proton:region-id:123456789012:service/MySimpleService/
service-instance/my-instance",
            "createdAt": "2021-03-12T22:39:42.318000+00:00",
            "deploymentStatus": "SUCCEEDED",
            "environmentName": "simple-env",
            "lastDeploymentAttemptedAt": "2021-03-12T22:39:43.160000+00:00",
            "lastDeploymentSucceededAt": "2021-03-12T22:39:43.160000+00:00",
            "name": "my-instance",
            "serviceName": "example-svc",
            "serviceTemplateArn": "arn:aws:proton:region-id:123456789012:service-
template/fargate-service",
            "templateMajorVersion": "1",
            "templateMinorVersion": "0",
            "templateName": "fargate-service"
        }
    ]
}
```

Die folgende Liste zeigt das bearbeitete Beispiel, das zum Löschen und Hinzufügen einer Instanz`spec` verwendet wurde. Die vorhandene Instanz mit dem Namen`my-instance` wird entfernt und eine neue Instanz mit dem Namen`yet-another-instance` wird hinzugefügt.

Spezifikation:

```
proton: ServiceSpec

pipeline:
  my_sample_pipeline_optional_input: "abc"
  my_sample_pipeline_required_input: "123"

instances:
  - name: "my-other-instance"
    environment: "simple-env"
    spec:
      my_sample_service_instance_required_input: "789"
```

```
  - name: "yet-another-instance"
    environment: "simple-env"
    spec:
      my_sample_service_instance_required_input: "789"
```

Sie können`"${Proton::CURRENT_VAL}"` damit angeben, welche Parameterwerte gegenüber dem Original beibehalten werden`spec` sollen, sofern die Werte in vorhanden sind`spec`.
Wird verwendet`get-service`, um das Original`spec` für einen Dienst anzuzeigen, wie unter beschriebenAnzeigen von Servicedaten.

Die folgende Liste zeigt, wie Sie sicherstellen können`"${Proton::CURRENT_VAL}"`, dass Ihre Parameterwerte`spec` nicht enthalten, damit die vorhandenen Services-Instanzen erhalten bleiben.

Spezifikation:

```
proton: ServiceSpec

pipeline:
  my_sample_pipeline_optional_input: "${Proton::CURRENT_VAL}"
  my_sample_pipeline_required_input: "${Proton::CURRENT_VAL}"

instances:
  - name: "my-other-instance"
    environment: "simple-env"
    spec:
      my_sample_service_instance_required_input: "${Proton::CURRENT_VAL}"
  - name: "yet-another-instance"
    environment: "simple-env"
    spec:
      my_sample_service_instance_required_input: "789"
```

Die nächste Liste zeigt den CLI-Befehl und die Antwort zum Bearbeiten des Dienstes.

Befehl:

```
$ aws proton update-service
    --name "MySimpleService" \
    --description "Edit by adding and deleting a service instance" \
    --spec "file://spec.yaml"
```

Antwort:

```
{
    "service": {
        "arn": "arn:aws:proton:region-id:123456789012:service/MySimpleService",
        "branchName": "main",
        "createdAt": "2021-03-12T22:39:42.318000+00:00",
        "description": "Edit by adding and deleting a service instance",
        "lastModifiedAt": "2021-03-12T22:55:48.169000+00:00",
        "name": "MySimpleService",
        "repositoryConnectionArn": "arn:aws:codestar-connections:region-
id:123456789012:connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "repositoryId": "my-repository/myorg-myapp",
        "status": "UPDATE_IN_PROGRESS",
        "templateName": "fargate-service"
    }
}
```

Der folgende`list-service-instances` Befehl und die folgende Antwort bestätigen, dass die vorhandene benannte`my-instance` Instanz entfernt und eine neue Instanz mit dem Name`yet-another-instance` hinzugefügt wurde.

Befehl:

```
$ aws proton list-service-instances \
    --service-name "MySimpleService"
```

Antwort:

```
{
    "serviceInstances": [
        {
            "arn": "arn:aws:proton:region-id:123456789012:service/MySimpleService/
service-instance/yet-another-instance",
            "createdAt": "2021-03-12T22:39:42.318000+00:00",
            "deploymentStatus": "SUCCEEDED",
            "environmentName": "simple-env",
            "lastDeploymentAttemptedAt": "2021-03-12T22:56:01.565000+00:00",
            "lastDeploymentSucceededAt": "2021-03-12T22:56:01.565000+00:00",
            "name": "yet-another-instance",
            "serviceName": "MySimpleService",
            "templateMajorVersion": "1",
            "templateMinorVersion": "0",
            "templateName": "fargate-service"
```

```
        },
        {
            "arn": "arn:aws:proton:region-id:123456789012:service/MySimpleService/
service-instance/my-other-instance",
            "createdAt": "2021-03-12T22:39:42.318000+00:00",
            "deploymentStatus": "SUCCEEDED",
            "environmentName": "simple-env",
            "lastDeploymentAttemptedAt": "2021-03-12T22:39:43.109000+00:00",
            "lastDeploymentSucceededAt": "2021-03-12T22:39:43.109000+00:00",
            "name": "my-other-instance",
            "serviceName": "MySimpleService",
            "templateMajorVersion": "1",
            "templateMinorVersion": "0",
            "templateName": "fargate-service"
        }
    ]
}
```

Was geschieht, wenn Sie Service-Instances hinzufügen oder entfernen

Nachdem Sie eine Service-Bearbeitung zum Löschen und Hinzufügen von Service-Instanzen eingereicht haben,AWS Proton werden die folgenden Aktionen ausgeführt.

- Setzt den Dienst auf`UPDATE_IN_PROGRESS`.
- Wenn der Dienst über eine Pipeline verfügt, setzt dessen Status auf`IN_PROGRESS` und blockiert Pipeline-Aktionen.
- Legt alle Service-Instanzen fest, auf die gelöscht werden soll`DELETE_IN_PROGRESS`.
- Sperrt Serviceaktionen.
- Sperrt Aktionen auf Service-Instanzen, die zum Löschen markiert sind.
- Erzeugt neue Dienstinstanzen.
- Löscht Instanzen, die Sie zum Löschen aufgelistet haben.
- Versuche, Instanzen zu entfernen, bei denen der Löschvorgang fehlgeschlagen ist.
- Nachdem das Hinzufügen und Löschen abgeschlossen ist, stellen Sie die Service-Pipeline erneut bereit (falls vorhanden), setzen Ihren Service auf`ACTIVE` und aktivieren Service- und Pipeline-Aktionen.

AWS Protonversucht, Fehlermodi wie folgt zu beheben.

- Wenn eine oder mehrere Dienstinstanzen nicht erstellt werden konnten, wirdAWS Proton versucht, die Bereitstellung aller neu erstellten Dienstinstanzen`spec` aufzuheben, und der vorherige Status wird wiederhergestellt. Es löscht keine Service-Instanzen und ändert die Pipeline in keiner Weise.
- Wenn eine oder mehrere Dienstinstanzen nicht gelöscht werden konnten, wird die Pipeline ohne die gelöschten InstanzenAWS Proton erneut bereitgestellt. Die`spec` wurde aktualisiert, um die hinzugefügten Instanzen einzubeziehen und die Instanzen auszuschließen, die zum Löschen markiert wurden.
- Wenn die Bereitstellung der Pipeline fehlschlägt, wird kein Rollback versucht, und sowohl der Service als auch die Pipeline geben den Status eines fehlgeschlagenen Updates an.

Tagging und Bearbeitungen von Diensten

Wenn Sie im Rahmen Ihrer Service-Bearbeitung Service-Instanzen hinzufügen, werdenAWS verwaltete Tags an die neuen Instanzen und bereitgestellten Ressourcen weitergegeben und automatisch für diese erstellt. Wenn Sie neue Tags erstellen, werden diese Tags nur auf die neuen Instanzen angewendet. Bestehende vom Service, vom Kunden verwaltete Tags, werden ebenfalls auf die neuen Instanzen übertragen. Weitere Informationen finden Sie unter AWS ProtonRessourcen und Tagging.

Einen Service löschen

Sie können einenAWS Proton Dienst mit seinen Instanzen und seiner Pipeline löschen, indem Sie dieAWS Proton Konsole oder dieAWS CLI.

Sie können keinen Dienst löschen, der über eine Dienstinstanz mit einer angefügten Komponente verfügt. Um einen solchen Dienst zu löschen, sollten Sie zuerst alle angeschlossenen Komponenten aktualisieren, um sie von ihren Service-Instanzen zu trennen. Weitere Informationen zu Komponenten finden Sie unterKomponenten.

AWS Management Console

Löschen Sie einen Service über die Konsole wie in den folgenden Schritten beschrieben.

Auf der Seite mit den Servicedetails.

1. Wählen Sie in der AWS ProtonKonsole Dienste aus.
2. Wählen Sie in der Liste der Services den Namen des anzuzeigenden Service.

3. Wählen Sie auf der Seite mit den Servicedetails Aktionen und dann Löschen aus.
4. Ein Modal fordert Sie auf, die Löschaktion zu bestätigen.
5. Folgen Sie den Anweisungen und wählen Sie Ja, löschen.

AWS CLI

Löschen Sie einen Dienst, wie im folgenden CLI-Beispiel für Befehl und Antwort gezeigt.

Befehl:

```
$ aws proton delete-service \
    --name "simple-svc"
```

Antwort:

```
{
    "service": {
        "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc",
        "branchName": "mainline",
        "createdAt": "2020-11-28T22:40:50.512000+00:00",
        "description": "Edit by updating description",
        "lastModifiedAt": "2020-11-29T00:30:39.248000+00:00",
        "name": "simple-svc",
        "repositoryConnectionArn": "arn:aws:codestar-connections:region-
id:123456789012:connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "repositoryId": "myorg/myapp",
        "status": "DELETE_IN_PROGRESS",
        "templateName": "fargate-service"
    }
}
```

Dienstinstanzdaten anzeigen

Erfahren Sie, wie SieAWS Proton Service-Instanz-Detaildaten anzeigen können. Sie können die Konsole oder die verwendenAWS CLI.

Eine Dienstinstanz gehört zu einem Dienst. Sie können eine Instanz nur im Rahmen von Aktionen zum Bearbeiten, Erstellen und Löschen von Diensten erstellen oder löschen. Wie Sie Instances zu einem Service hinzufügen und daraus entfernen, erfahren Sie unterDienst bearbeiten.

AWS Management Console

Listet die Details der Dienstinstanz mithilfe der AWS ProtonKonsole auf und zeigt sie an, wie in den folgenden Schritten gezeigt.

1. Um eine Liste Ihrer Service-Instanzen anzuzeigen, wählen Sie im Navigationsbereich Services-Instanzen aus.
2. Um Detaildaten anzuzeigen, wählen Sie den Namen einer Dienstinstanz.

   Sehen Sie sich die Detaildaten Ihrer Service-Instance an.

AWS CLI

Listet die Details der Dienstinstanz auf und zeigt sie an, wie in den folgenden CLI-Beispielbefehlen und -antworten gezeigt.

Befehl:

```
$ aws proton list-service-instances
```

Antwort:

```
{
    "serviceInstances": [
        {
            "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc/
service-instance/instance-one",
            "createdAt": "2020-11-28T22:40:50.512000+00:00",
            "deploymentStatus": "SUCCEEDED",
            "environmentArn": "arn:aws:proton:region-id:123456789012:environment/
simple-env",
            "lastDeploymentAttemptedAt": "2020-11-28T22:40:50.512000+00:00",
            "lastDeploymentSucceededAt": "2020-11-28T22:40:50.512000+00:00",
            "name": "instance-one",
            "serviceName": "simple-svc",
            "templateMajorVersion": "1",
            "templateMinorVersion": "0",
            "templateName": "fargate-service"
        }
    ]
}
```

Befehl:

```
$ aws proton get-service-instance \
    --name "instance-one" \
    --service-name "simple-svc"
```

Antwort:

```
{
    "serviceInstance": {
        "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc/service-
instance/instance-one",
        "createdAt": "2020-11-28T22:40:50.512000+00:00",
        "deploymentStatus": "SUCCEEDED",
        "environmentName": "simple-env",
        "lastDeploymentAttemptedAt": "2020-11-28T22:40:50.512000+00:00",
        "lastDeploymentSucceededAt": "2020-11-28T22:40:50.512000+00:00",
        "name": "instance-one",
        "serviceName": "simple-svc",
        "spec": "proton: ServiceSpec\npipeline:\n
 my_sample_pipeline_optional_input: hello world\n
 my_sample_pipeline_required_input: pipeline up\ninstances:\n- name: instance-one\n
 environment: my-simple-env\n  spec:\n    my_sample_service_instance_optional_input:
 Ola\n    my_sample_service_instance_required_input: Ciao\n",
        "templateMajorVersion": "1",
        "templateMinorVersion": "0",
        "templateName": "svc-simple"
    }
}
```

Aktualisierung einer Serviceinstance-Instance

Erfahren Sie, wie Sie eineAWS Proton Service-Instance aktualisieren und das Update abbrechen.

Eine Dienstinstanz gehört zu einem Dienst. Sie können eine Instanz nur im Rahmen von Aktionen zum Bearbeiten, Erstellen und Löschen von Diensten erstellen oder löschen. Wie Sie Instances zu einem Service hinzufügen und daraus entfernen, erfahren Sie unterDienst bearbeiten.

Es gibt vier Modi für die Aktualisierung einer Dienstinstanz, wie in der folgenden Liste beschrieben. Bei Verwendung von definiert das`deployment-type` Feld den Modus.AWS CLI Wenn Sie die Konsole verwenden, werden diese Modi den Aktionen Bearbeiten und Auf neueste Nebenversion

aktualisieren und Auf neueste Hauptversion aktualisieren zugeordnet, die unter Aktionen auf der Service-Instanz-Detailseite angezeigt werden.

`NONE`

In diesem Modus findet keine Bereitstellung statt. Nur die angeforderten Metadatenparameter werden aktualisiert.

`CURRENT_VERSION`

In diesem Modus wird die Dienstinstanz bereitgestellt und mit der neuen Spezifikation, die Sie angeben, aktualisiert. Nur angeforderte Parameter werden aktualisiert. Geben Sie keine Parameter für Neben- oder Hauptversionen an, wenn Sie dies verwenden`deployment-type`.

`MINOR_VERSION`

In diesem Modus wird die Dienstinstanz bereitgestellt und mit der veröffentlichten, empfohlenen (neuesten) Nebenversion der aktuell verwendeten Hauptversion aktualisiert, die standardmäßig verwendet wird. Sie können auch eine andere Nebenversion der aktuell verwendeten Hauptversion angeben.

`MAJOR_VERSION`

In diesem Modus wird die Dienstinstanz standardmäßig mit der veröffentlichten, empfohlenen (neuesten) Haupt- und Nebenversion der aktuellen Vorlage bereitgestellt und aktualisiert. Sie können auch eine andere Hauptversion angeben, die höher ist als die verwendete Hauptversion und eine Nebenversion (optional).

Sie können versuchen, die Bereitstellung eines Service-Instance-Updates abzubrechen, falls dies der Fall`deploymentStatus` ist`IN_PROGRESS`. AWS Protonversucht, die Bereitstellung abzubrechen. Eine erfolgreiche Stornierung ist nicht garantiert.

Wenn Sie eine Update-Bereitstellung stornieren, wirdAWS Proton versucht, die Bereitstellung abzubrechen, wie in den folgenden Schritten aufgeführt.

- Setzt den Bereitstellungsstatus auf`CANCELLING`.
- Stoppt die laufende Bereitstellung und löscht alle neuen Ressourcen, die durch die Bereitstellung erstellt wurden, wenn`IN_PROGRESS`.

- Setzt den Bereitstellungsstatus auf`CANCELLED`.
- Setzt den Zustand der Ressource auf den Zustand zurück, den er vor dem Start der Bereitstellung hatte.

Weitere Informationen zum Abbrechen einer Service-Instance-Bereitstellung finden Sie CancelServiceInstanceDeploymentin der AWS ProtonAPI-Referenz.

Verwenden Sie die Konsole oderAWS CLI um Updates vorzunehmen oder die Bereitstellung von Updates abzubrechen.

AWS Management Console

Aktualisieren Sie eine Dienstinstanz mithilfe der Konsole, indem Sie die folgenden Schritte ausführen.

1. Wählen Sie in der AWS ProtonKonsole im Navigationsbereich Service-Instanzen aus.
2. Wählen Sie in der Liste der Service-Instances den Namen der Service-Instance aus, die Sie aktualisieren möchten.
3. Wählen Sie Aktionen und dann eine der Aktualisierungsoptionen, Bearbeiten, um die Spezifikation zu aktualisieren oder Aktionen und dann Auf neueste Nebenversion aktualisieren oder Auf neueste Hauptversion aktualisieren.
4. Füllen Sie jedes Formular aus und wählen Sie Weiter, bis Sie die Seite „Bewertung“ erreichen.
5. Überprüfe deine Änderungen und wähle Aktualisieren.

AWS CLI

Aktualisieren Sie eine Dienstinstanz auf eine neue Nebenversion, wie in den CLI-Beispielbefehlen und -Antworten gezeigt.

Wenn Sie Ihre Service-Instance mit einer Änderung aktualisieren`spec`, können Sie`"${Proton::CURRENT_VAL}"` damit angeben, welche Parameterwerte gegenüber dem Original beibehalten werden sollen`spec`, sofern die Werte in der vorhanden sind`spec`. Wird verwendet`get-service`, um das Original`spec` für eine Dienstinstanz anzuzeigen, wie unter beschriebenAnzeigen von Servicedaten.

Das folgende Beispiel zeigt, wie Sie`"${Proton::CURRENT_VAL}"` in einen verwenden können`spec`.

Spezifikation:

```
proton: ServiceSpec

pipeline:
  my_sample_pipeline_optional_input: "${Proton::CURRENT_VAL}"
  my_sample_pipeline_required_input: "${Proton::CURRENT_VAL}"

instances:
  - name: "my-instance"
    environment: "simple-env"
    spec:
      my_sample_service_instance_optional_input: "${Proton::CURRENT_VAL}"
      my_sample_service_instance_required_input: "${Proton::CURRENT_VAL}"
  - name: "my-other-instance"
    environment: "simple-env"
    spec:
      my_sample_service_instance_required_input: "789"
```

Befehl: zum Aktualisieren

```
$ aws proton update-service-instance \
    --name "instance-one" \
    --service-name "simple-svc" \
    --spec "file://service-spec.yaml" \
    --template-major-version "1" \
    --template-minor-version "1" \
    --deployment-type "MINOR_VERSION"
```

Antwort:

```
{
    "serviceInstance": {
        "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc/service-
instance/instance-one",
        "createdAt": "2021-04-02T21:29:59.962000+00:00",
        "deploymentStatus": "IN_PROGRESS",
        "environmentName": "arn:aws:proton:region-id:123456789012:environment/
simple-env",
        "lastDeploymentAttemptedAt": "2021-04-02T21:38:00.823000+00:00",
        "lastDeploymentSucceededAt": "2021-04-02T21:29:59.962000+00:00",
        "name": "instance-one",
        "serviceName": "simple-svc",
```

```
        "templateMajorVersion": "1",
        "templateMinorVersion": "0",
        "templateName": "svc-simple"
    }
}
```

Befehl: um den Status abzurufen und zu bestätigen

```
$ aws proton get-service-instance \
    --name "instance-one" \
    --service-name "simple-svc"
```

Antwort:

```
{
    "serviceInstance": {
        "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc/service-
instance/instance-one",
        "createdAt": "2021-04-02T21:29:59.962000+00:00",
        "deploymentStatus": "SUCCEEDED",
        "environmentName": "simple-env",
        "lastDeploymentAttemptedAt": "2021-04-02T21:38:00.823000+00:00",
        "lastDeploymentSucceededAt": "2021-04-02T21:38:00.823000+00:00",
        "name": "instance-one",
        "serviceName": "simple-svc",
        "spec": "proton: ServiceSpec\n\npipeline:\n
 my_sample_pipeline_optional_input: \"abc\"\n  my_sample_pipeline_required_input:
 \"123\"\n\ninstances:\n  - name: \"instance-one\"\n    environment: \"simple-
env\"\n    spec:\n      my_sample_service_instance_optional_input: \"def\"\n
      my_sample_service_instance_required_input: \"456\"\n  - name: \"my-
other-instance\"\n    environment: \"kls-simple-env\"\n    spec:\n
 my_sample_service_instance_required_input: \"789\"\n",
        "templateMajorVersion": "1",
        "templateMinorVersion": "1",
        "templateName": "svc-simple"
    }
}
```

AWS Management Console

Brechen Sie die Bereitstellung einer Service-Instance mithilfe der Konsole ab, wie in den folgenden Schritten gezeigt.

1. Wählen Sie in der AWS ProtonKonsole im Navigationsbereich Service-Instanzen aus.
2. Wählen Sie in der Liste der Service-Instances den Namen der Service-Instance aus, die das Bereitstellungsupdate enthält, das Sie abbrechen möchten.
3. Wenn Ihr Update-Bereitstellungsstatus In Bearbeitung ist, wählen Sie auf der Service-Instanz-Detailseite Aktionen und dann Bereitstellung abbrechen aus.
4. Ein Modal fordert Sie auf, den Abbruch zu bestätigen. Wählen Sie Bereitstellung stornieren aus.
5. Ihr Update-Bereitstellungsstatus ist auf Storniert und dann auf Storniert gesetzt, um die Stornierung abzuschließen.

AWS CLI

Brechen Sie ein Update der IN_PROGRESS-Dienstinstanzbereitstellung auf die neue Nebenversion 2 ab, wie in den folgenden CLI-Beispielbefehlen und -antworten gezeigt.

Die für dieses Beispiel verwendete Vorlage enthält eine Wartebedingung, sodass die Stornierung beginnt, bevor die Aktualisierung erfolgreich bereitgestellt wird.

Befehl: stornieren

```
$ aws proton cancel-service-instance-deployment \
    --service-instance-name "instance-one" \
    --service-name "simple-svc"
```

Antwort:

```
{
    "serviceInstance": {
        "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc/service-
instance/instance-one",
        "createdAt": "2021-04-02T21:29:59.962000+00:00",
        "deploymentStatus": "CANCELLING",
        "environmentName": "simple-env",
        "lastDeploymentAttemptedAt": "2021-04-02T21:45:15.406000+00:00",
        "lastDeploymentSucceededAt": "2021-04-02T21:38:00.823000+00:00",
        "name": "instance-one",
        "serviceName": "simple-svc",
        "spec": "proton: ServiceSpec\npipeline:\n
 my_sample_pipeline_optional_input: abc\n  my_sample_pipeline_required_input:
 '123'\ninstances:\n- name: my-instance\n  environment: MySimpleEnv
```

```
\n  spec:\n    my_sample_service_instance_optional_input: def\n
 my_sample_service_instance_required_input: '456'\n- name: my-other-instance\n
 environment: MySimpleEnv\n  spec:\n    my_sample_service_instance_required_input:
 '789'\n",
        "templateMajorVersion": "1",
        "templateMinorVersion": "1",
        "templateName": "svc-simple"
    }
}
```

Befehl: um den Status abzurufen und zu bestätigen

```
$ aws proton get-service-instance \
    --name "instance-one" \
    --service-name "simple-svc"
```

Antwort:

```
{
    "serviceInstance": {
        "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc/service-
instance/instance-one",
        "createdAt": "2021-04-02T21:29:59.962000+00:00",
        "deploymentStatus": "CANCELLED",
        "deploymentStatusMessage": "User initiated cancellation.",
        "environmentName": "simple-env",
        "lastDeploymentAttemptedAt": "2021-04-02T21:45:15.406000+00:00",
        "lastDeploymentSucceededAt": "2021-04-02T21:38:00.823000+00:00",
        "name": "instance-one",
        "serviceName": "simple-svc",
        "spec": "proton: ServiceSpec\n\npipeline:\n
 my_sample_pipeline_optional_input: \"abc\"\n  my_sample_pipeline_required_input:
 \"123\"\n\ninstances:\n  - name: \"instance-one\"\n    environment: \"simple-
env\"\n    spec:\n      my_sample_service_instance_optional_input: \"def\"\n
      my_sample_service_instance_required_input: \"456\"\n  - name: \"my-
other-instance\"\n    environment: \"kls-simple-env\"\n    spec:\n
 my_sample_service_instance_required_input: \"789\"\n",
        "templateMajorVersion": "1",
        "templateMinorVersion": "1",
        "templateName": "svc-simple"
    }
}
```

Aktualisierung einer Service-Pipeline

Erfahren Sie, wie Sie eineAWS Proton Service-Pipeline aktualisieren und das Update abbrechen.

Eine Service-Pipeline gehört zu einem Dienst. Sie können eine Pipeline nur im Zusammenhang mit Aktionen zum Erstellen und Löschen von Diensten erstellen oder löschen.

Es gibt vier Modi zum Aktualisieren einer Service-Pipeline, wie in der folgenden Liste beschrieben. Bei Verwendung von definiert das`deployment-type` Feld den Modus.AWS CLI Wenn Sie die Konsole verwenden, werden diese Modi der Bearbeitungspipeline und der Option Auf empfohlene Version aktualisieren zugeordnet.

`NONE`

In diesem Modus findet keine Bereitstellung statt. Nur die angeforderten Metadatenparameter werden aktualisiert.

`CURRENT_VERSION`

In diesem Modus wird die Service-Pipeline bereitgestellt und mit der von Ihnen bereitgestellten neuen Spezifikation aktualisiert. Nur angeforderte Parameter werden aktualisiert. Geben Sie keine Parameter für Neben- oder Hauptversionen an, wenn Sie dies verwenden`deployment-type`.

`MINOR_VERSION`

In diesem Modus wird die Service-Pipeline bereitgestellt und mit der veröffentlichten, empfohlenen (neuesten) Nebenversion der aktuell verwendeten Hauptversion aktualisiert, die standardmäßig verwendet wird. Sie können auch eine andere Nebenversion der aktuell verwendeten Hauptversion angeben.

`MAJOR_VERSION`

In diesem Modus wird die Service-Pipeline bereitgestellt und standardmäßig mit der veröffentlichten, empfohlenen (neuesten) Haupt- und Nebenversion der aktuellen Vorlage aktualisiert. Sie können auch eine andere Hauptversion angeben, die höher ist als die verwendete Hauptversion und eine Nebenversion (optional).

Sie können versuchen, die Bereitstellung eines Service Pipeline-Updates abzubrechen, falls dies der`deploymentStatus` Fall ist`IN_PROGRESS`. AWS Protonversucht, die Bereitstellung abzubrechen. Eine erfolgreiche Stornierung ist nicht garantiert.

Wenn Sie eine Update-Bereitstellung stornieren, wirdAWS Proton versucht, die Bereitstellung abzubrechen, wie in den folgenden Schritten aufgeführt.

- Setzt den Bereitstellungsstatus auf`CANCELLING`.
- Stoppt die laufende Bereitstellung und löscht alle neuen Ressourcen, die durch die Bereitstellung erstellt wurden, wenn`IN_PROGRESS`.
- Setzt den Bereitstellungsstatus auf`CANCELLED`.
- Setzt den Zustand der Ressource auf den Zustand zurück, den er vor dem Start der Bereitstellung hatte.

Weitere Informationen zum Abbrechen einer Service-Pipeline-Bereitstellung finden Sie CancelServicePipelineDeploymentin der AWS ProtonAPI-Referenz.

Verwenden Sie die Konsole oderAWS CLI um Updates vorzunehmen oder die Bereitstellung von Updates abzubrechen.

AWS Management Console

Aktualisieren Sie eine Service-Pipeline mithilfe der Konsole wie in den folgenden Schritten beschrieben.

1. Wählen Sie in der AWS ProtonKonsole Dienste aus.
2. Wählen Sie in der Liste der Services den Namen des anzuzeigenden Service.
3. Auf der Seite mit den Servicedetails gibt es zwei Tabs: Übersicht und Pipeline. Wählen Sie Pipeline.
4. Wenn Sie Spezifikationen aktualisieren möchten, wählen Sie Pipeline bearbeiten und füllen Sie jedes Formular aus. Wählen Sie Weiter, bis Sie das endgültige Formular ausgefüllt haben, und wählen Sie dann Pipeline aktualisieren.

   Wenn Sie auf eine neue Version aktualisieren möchten und es ein Informationssymbol gibt, das darauf hinweist, dass eine neue Version unter Pipeline-Vorlage verfügbar ist, wählen Sie den Namen der neuen Vorlagenversion.

   a. Wählen Sie Auf empfohlene Version aktualisieren.

b. Füllen Sie jedes Formular aus und wählen Sie Weiter, bis Sie das endgültige Formular ausgefüllt haben und Aktualisieren wählen.

AWS CLI

Aktualisieren Sie eine Service-Pipeline auf eine neue Nebenversion, wie in den folgenden CLI-Beispielbefehlen und -antworten gezeigt.

Wenn Sie Ihre Service-Pipeline mit einer Änderung aktualisieren`spec`, können`"${Proton::CURRENT_VAL}"` Sie angeben, welche Parameterwerte gegenüber dem Original beibehalten werden sollen`spec`, sofern die Werte in der vorhanden sind`spec`. Wird verwendet`get-service`, um das Original`spec` für eine Service-Pipeline anzuzeigen, wie unter beschriebenAnzeigen von Servicedaten.

Das folgende Beispiel zeigt, wie Sie`"${Proton::CURRENT_VAL}"` in einen verwenden können`spec`.

Spezifikation:

```
proton: ServiceSpec

pipeline:
  my_sample_pipeline_optional_input: "${Proton::CURRENT_VAL}"
  my_sample_pipeline_required_input: "${Proton::CURRENT_VAL}"

instances:
  - name: "my-instance"
    environment: "simple-env"
    spec:
      my_sample_service_instance_optional_input: "${Proton::CURRENT_VAL}"
      my_sample_service_instance_required_input: "${Proton::CURRENT_VAL}"
  - name: "my-other-instance"
    environment: "simple-env"
    spec:
      my_sample_service_instance_required_input: "789"
```

Befehl: zum Aktualisieren

```
$ aws proton update-service-pipeline \
    --service-name "simple-svc" \
    --spec "file://service-spec.yaml" \
```

```
    --template-major-version "1" \
    --template-minor-version "1" \
    --deployment-type "MINOR_VERSION"
```

Antwort:

```
{
    "pipeline": {
        "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc/pipeline/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "createdAt": "2021-04-02T21:29:59.962000+00:00",
        "deploymentStatus": "IN_PROGRESS",
        "lastDeploymentAttemptedAt": "2021-04-02T21:39:28.991000+00:00",
        "lastDeploymentSucceededAt": "2021-04-02T21:29:59.962000+00:00",
        "spec": "proton: ServiceSpec\n\npipeline:\n
 my_sample_pipeline_optional_input: \"abc\"\n  my_sample_pipeline_required_input:
 \"123\"\n\ninstances:\n  - name: \"my-instance\"\n    environment: \"MySimpleEnv
\"\n    spec:\n      my_sample_service_instance_optional_input: \"def
\"\n      my_sample_service_instance_required_input: \"456\"\n  - name:
 \"my-other-instance\"\n    environment: \"MySimpleEnv\"\n    spec:\n
 my_sample_service_instance_required_input: \"789\"\n",
        "templateMajorVersion": "1",
        "templateMinorVersion": "0",
        "templateName": "svc-simple"
    }
}
```

Befehl: um den Status abzurufen und zu bestätigen

```
$ aws proton get-service \
    --name "simple-svc"
```

Antwort:

```
{
    "service": {
        "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc",
        "branchName": "main",
        "createdAt": "2021-04-02T21:29:59.962000+00:00",
        "lastModifiedAt": "2021-04-02T21:30:54.364000+00:00",
        "name": "simple-svc",
        "pipeline": {
```

```
            "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc/
pipeline",
            "createdAt": "2021-04-02T21:29:59.962000+00:00",
            "deploymentStatus": "SUCCEEDED",
            "lastDeploymentAttemptedAt": "2021-04-02T21:39:28.991000+00:00",
            "lastDeploymentSucceededAt": "2021-04-02T21:39:28.991000+00:00",
            "spec": "proton: ServiceSpec\n\npipeline:\n
 my_sample_pipeline_optional_input: \"abc\"\n  my_sample_pipeline_required_input:
 \"123\"\n\ninstances:\n  - name: \"instance-one\"\n    environment: \"simple-
env\"\n    spec:\n      my_sample_service_instance_optional_input: \"def
\"\n      my_sample_service_instance_required_input: \"456\"\n  - name:
 \"my-other-instance\"\n    environment: \"simple-env\"\n    spec:\n
 my_sample_service_instance_required_input: \"789\"\n",
            "templateMajorVersion": "1",
            "templateMinorVersion": "1",
            "templateName": "svc-simple"
        },
        "repositoryConnectionArn": "arn:aws:codestar-connections:region-
id:123456789012:connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "repositoryId": "repo-name/myorg-myapp",
        "spec": "proton: ServiceSpec\n\npipeline:\n
 my_sample_pipeline_optional_input: \"abc\"\n  my_sample_pipeline_required_input:
 \"123\"\n\ninstances:\n  - name: \"instance-one\"\n    environment: \"simple-
env\"\n    spec:\n      my_sample_service_instance_optional_input: \"def
\"\n      my_sample_service_instance_required_input: \"456\"\n  - name:
 \"my-other-instance\"\n    environment: \"simple-env\"\n    spec:\n
 my_sample_service_instance_required_input: \"789\"\n",
        "status": "ACTIVE",
        "templateName": "svc-simple"
    }
}
```


AWS Management Console

Brechen Sie eine Service-Pipeline-Bereitstellung mithilfe der Konsole ab, wie in den folgenden Schritten gezeigt.

1. Wählen Sie in der AWS ProtonKonsole im Navigationsbereich Dienste aus.
2. Wählen Sie in der Liste der Services den Namen des anzuzeigenden Service.
3. Wählen Sie auf der Servicedetailseite den Tab Pipeline (Pipeline) aus.

4. Wenn Ihr Update-Bereitstellungsstatus In Bearbeitung ist, wählen Sie auf der Detailseite der Service Pipeline die Option Bereitstellung abbrechen aus.
5. Ein Modal fordert Sie auf, den Abbruch zu bestätigen. Wählen Sie Bereitstellung stornieren aus.
6. Ihr Update-Bereitstellungsstatus ist auf Storniert und dann auf Storniert gesetzt, um die Stornierung abzuschließen.

AWS CLI

Brechen Sie ein Update der IN_PROGRESS-Dienstpipeline auf die Nebenversion 2 ab, wie in den folgenden CLI-Beispielbefehlen und -antworten gezeigt.

Die für dieses Beispiel verwendete Vorlage enthält eine Wartebedingung, sodass die Stornierung beginnt, bevor die Aktualisierung erfolgreich bereitgestellt wird.

Befehl: stornieren

```
$ aws proton cancel-service-pipeline-deployment \
    --service-name "simple-svc"
```

Antwort:

```
{
    "pipeline": {
        "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc/pipeline",
        "createdAt": "2021-04-02T21:29:59.962000+00:00",
        "deploymentStatus": "CANCELLING",
        "lastDeploymentAttemptedAt": "2021-04-02T22:02:45.095000+00:00",
        "lastDeploymentSucceededAt": "2021-04-02T21:39:28.991000+00:00",
        "templateMajorVersion": "1",
        "templateMinorVersion": "1",
        "templateName": "svc-simple"
    }
}
```

Befehl: um den Status abzurufen und zu bestätigen

```
$ aws proton get-service \
    --name "simple-svc"
```

Antwort:


```
{
    "service": {
        "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc",
        "branchName": "main",
        "createdAt": "2021-04-02T21:29:59.962000+00:00",
        "lastModifiedAt": "2021-04-02T21:30:54.364000+00:00",
        "name": "simple-svc",
        "pipeline": {
            "arn": "arn:aws:proton:region-id:123456789012:service/simple-svc/
pipeline",
            "createdAt": "2021-04-02T21:29:59.962000+00:00",
            "deploymentStatus": "CANCELLED",
            "deploymentStatusMessage": "User initiated cancellation.",
            "lastDeploymentAttemptedAt": "2021-04-02T22:02:45.095000+00:00",
            "lastDeploymentSucceededAt": "2021-04-02T21:39:28.991000+00:00",
            "spec": "proton: ServiceSpec\n\npipeline:\n
 my_sample_pipeline_optional_input: \"abc\"\n  my_sample_pipeline_required_input:
 \"123\"\n\ninstances:\n  - name: \"instance-one\"\n    environment: \"simple-
env\"\n    spec:\n      my_sample_service_instance_optional_input: \"def
\"\n      my_sample_service_instance_required_input: \"456\"\n  - name:
 \"my-other-instance\"\n    environment: \"simple-env\"\n    spec:\n
 my_sample_service_instance_required_input: \"789\"\n",
            "templateMajorVersion": "1",
            "templateMinorVersion": "1",
            "templateName": "svc-simple"
        },
        "repositoryConnectionArn": "arn:aws:codestar-connections:region-
id:123456789012:connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
        "repositoryId": "repo-name/myorg-myapp",
        "spec": "proton: ServiceSpec\n\npipeline:\n
 my_sample_pipeline_optional_input: \"abc\"\n  my_sample_pipeline_required_input:
 \"123\"\n\ninstances:\n  - name: \"instance-one\"\n    environment: \"simple-
env\"\n    spec:\n      my_sample_service_instance_optional_input: \"def
\"\n      my_sample_service_instance_required_input: \"456\"\n  - name:
 \"my-other-instance\"\n    environment: \"simple-env\"\n    spec:\n
 my_sample_service_instance_required_input: \"789\"\n",
        "status": "ACTIVE",
        "templateName": "svc-simple"
    }
}
```

AWS Proton-Komponenten

Komponenten sind eine Art vonAWS Proton Ressource. Sie verleihen Service-Vorlagen mehr Flexibilität. Komponenten bieten Plattformteams einen Mechanismus zur Erweiterung der Kerninfrastrukturmuster und zur Definition von Schutzmaßnahmen, die es Entwicklern ermöglichen, Aspekte ihrer Anwendungsinfrastruktur zu verwalten.

Definieren Sie inAWS Proton Administratoren eine Standardinfrastruktur, die in allen Entwicklungsteams und Anwendungen verwendet wird. Entwicklungsteams müssen jedoch möglicherweise zusätzliche Ressourcen für ihre spezifischen Anwendungsfälle hinzufügen, wie Amazon Simple Queue Service (Amazon SQS) -Warteschlangen oder Amazon DynamoDB-Tabellen. Diese anwendungsspezifischen Ressourcen können sich häufig ändern, insbesondere während der frühen Anwendungsentwicklung. Die Aufrechterhaltung dieser häufigen Änderungen an von Administratoren erstellten Vorlagen könnte schwierig zu verwalten und zu skalieren sein. Administratoren müssten viel mehr Vorlagen verwalten, ohne dass der Administrator einen echten Mehrwert bietet. Die Alternative, Anwendungsentwickler Vorlagen für ihre Anwendungen erstellen zu lassen, ist ebenfalls nicht ideal, da sie Administratoren die Möglichkeit nimmt, die wichtigsten Architekturkomponenten wieAWS Fargate Aufgaben zu standardisieren. Hier kommen Komponenten ins Spiel.

Mit einer Komponente kann ein Entwickler seiner Anwendung zusätzliche Ressourcen hinzufügen, die über das hinausgehen, was Administratoren in Umgebungs- und Dienstvorlagen definiert haben. Der Entwickler hängt die Komponente dann an eine Dienstinstanz an. AWS Protonstellt Infrastrukturressourcen bereit, die von der Komponente definiert werden, genauso wie sie Ressourcen für Umgebungen und Dienstinstanzen bereitstellt.

Eine Komponente kann Service-Instance-Eingaben lesen und Ausgaben für die Service-Instance bereitstellen, um ein vollständig integriertes Erlebnis zu gewährleisten. Wenn die Komponente beispielsweise einen Amazon Simple Storage Service (Amazon S3) -Bucket zur Verwendung durch eine Service-Instance hinzufügt, kann die Komponentenvorlage die Umgebungs- und Service-Instance-Namen bei der Benennung des Buckets berücksichtigen. WennAWS Proton die Dienstvorlage zur Bereitstellung einer Dienstinstanz gerendert wird, kann die Dienstinstanz auf den Bucket verweisen und ihn verwenden.

Die Komponenten, dieAWS Proton derzeit unterstützt werden, sind direkt definierte Komponenten. Sie übergeben die Infrastructure as Code (IaC) -Datei, die die Infrastruktur der Komponente definiert, direkt an dieAWS Proton API oder Konsole. Dies unterscheidet sich von einer Umgebung oder einem

Dienst, bei dem Sie IaC in einem Vorlagenpaket definieren und das Paket als Vorlagenressource registrieren und dann eine Vorlagenressource verwenden, um die Umgebung oder den Dienst zu erstellen.

> **Note**
>
> Direkt definierte Komponenten ermöglichen es Entwicklern, zusätzliche Infrastrukturen zu definieren und bereitzustellen. AWS Protonstellt alle direkt definierten Komponenten bereit, die in derselben Umgebung laufen und dieselbeAWS Identity and Access Management (IAM-) Rolle verwenden.

Ein Administrator kann auf zwei Arten steuern, was Entwickler mit Komponenten tun können:

- Unterstützte Komponentenquellen — Ein Administrator kann das Anhängen von Komponenten an Service-Instanzen auf der Grundlage einer Eigenschaft vonAWS Proton Service-Template-Versionen zulassen. Standardmäßig können Entwickler keine Komponenten an Service-Instanzen anhängen.

  Weitere Informationen zu dieser Eigenschaft finden Sie im supportedComponentSourcesParameter der CreateServiceTemplateVersionAPI-Aktion in der AWS ProtonAPI-Referenz.

  > **Note**
  >
  > Wenn Sie die Vorlagensynchronisierung verwenden, werden automatisch Service-Template-VersionenAWS Proton erstellt, wenn Sie Änderungen an einem Service-Template-Paket in einem Repository übertragen. In diesem Fall geben Sie diese Eigenschaft in einer Datei an, die jeder Service-Template-Hauptversion zugeordnet ist, anstatt unterstützte Komponentenquellen bei der Erstellung der Service-Template-Version anzugeben. Weitere Informationen finden Sie unter the section called “Synchronisieren von Dienstvorlagen”.

- Komponentenrollen — Ein Administrator kann einer Umgebung eine Komponentenrolle zuweisen. AWS Protonübernimmt diese Rolle, wenn es eine Infrastruktur bereitstellt, die durch eine direkt definierte Komponente in der Umgebung definiert ist. Daher umfasst die Komponentenrolle die Infrastruktur, die Entwickler mithilfe direkt definierter Komponenten in der Umgebung hinzufügen können. Ohne die Komponentenrolle können Entwickler keine direkt definierten Komponenten in der Umgebung erstellen.

Weitere Informationen zum Zuweisen einer Komponentenrolle finden Sie im componentRoleArnParameter der CreateEnvironmentAPI-Aktion in der AWS ProtonAPI-Referenz.

> **Note**
>
> Komponentenrollen werden inSelbstverwaltetes Provisioned Umgebungen nicht verwendet.

Themen

Wie schneiden Komponenten im Vergleich zu anderenAWS Proton Ressourcen ab?

In vielerlei Hinsicht ähneln Komponenten anderenAWS Proton Ressourcen. Ihre Infrastruktur ist in einer IaC-Vorlagendatei definiert, die entweder imAWS CloudFormation YAML- oder Terraform-HCL-Format verfasst wurde. AWS Protonkann die Komponenteninfrastruktur entweder mithilfe von AWS-Managed Provisioning oder Self-Managed Provisioning bereitstellen.

Komponenten unterscheiden sich jedoch in einigen Punkten von anderenAWS Proton Ressourcen:

- Getrennter Zustand — Komponenten sind so konzipiert, dass sie an Service-Instances angefügt werden und ihre Infrastruktur erweitern, können sich aber auch in einem getrennten Zustand befinden, in dem sie keiner Service-Instance zugeordnet sind. Weitere Informationen zum Komponenten-Status finden Sie unterthe section called “Komponenten-Zustände”.
- Kein Schema — Komponenten haben kein zugeordnetes Schema, wie es bei Vorlagenpaketen der Fall ist. Komponenteneingaben werden durch einen Service definiert. Eine Komponente kann Eingaben verbrauchen, wenn sie an eine Service-Instance angehängt ist.

- Keine vom Kunden verwalteten Komponenten —AWS Proton stellt immer die Komponenteninfrastruktur für Sie bereit. Es gibt keine „Bring Your Own Resources“ -Version von Komponenten. Weitere Informationen über vom Kunden verwaltete Umgebungen finden Sie unterthe section called “Erstellen”.
- Keine Vorlagenressource — Direkt definierten Komponenten ist keine Vorlagenressource zugeordnet, ähnlich wie Umgebungs- und Dienstvorlagen. Sie stellen eine IAc-Vorlagendatei direkt für die Komponente bereit. In ähnlicher Weise stellen Sie direkt ein Manifest bereit, das die Vorlagensprache und die Rendering-Engine für die Bereitstellung der Infrastruktur der Komponente definiert. Sie erstellen die Vorlagendatei und das Manifest auf ähnliche Weise wie beim Erstellen eines Vorlagenpakets. Bei direkt definierten Komponenten ist es jedoch nicht erforderlich, IaC-Dateien als Pakete an bestimmten Speicherorten zu speichern, und Sie erstellen keine VorlagenressourceAWS Proton aus IaC-Dateien.
- Keine CodeBuild basierte Bereitstellung — Sie können keine direkt definierten Komponenten mithilfe Ihres eigenen benutzerdefinierten Bereitstellungsskripts bereitstellen, das als CodeBuildbasiertes Provisioning bezeichnet wird. Weitere Informationen finden Sie unter the section called “CodeBuildBereitstellung”.

Komponenten in derAWS Proton Konsole

Verwenden Sie dieAWS Proton Konsole, umAWS Proton Komponenten zu erstellen, zu aktualisieren, anzuzeigen und zu verwenden.

Die folgenden Konsolenseiten beziehen sich auf Komponenten. Wir fügen direkte Links zu Konsolenseiten der obersten Ebene hinzu.

- Komponenten — Sehen Sie sich die Liste der Komponenten in IhremAWS Konto an. Sie können neue Komponenten erstellen und vorhandene Komponenten aktualisieren oder löschen. Wählen Sie einen Komponenten-Namen in der Liste, um die Detailseite anzuzeigen.

  Ähnliche Listen gibt es auch auf den Seiten Umgebungsdetails und Service-Instanz-Details. In diesen Listen werden nur die Komponenten angezeigt, die der betrachteten Ressource zugeordnet sind. Wenn Sie eine Komponente aus einer dieser Listen erstellen, wählen Sie dieAWS Proton zugehörige Umgebung auf der Seite Komponente erstellen vorab aus.
- Komponentendetails — Um die Seite mit den Komponentendetails anzuzeigen, wählen Sie einen Komponentennamen in der Komponentenliste aus.

Sehen Sie sich auf der Detailseite die Komponentendetails und den Status an und aktualisieren oder löschen Sie die Komponente. Listen mit Ausgaben (z. B. bereitgestellten Ressourcen-ARNs), bereitgestelltenAWS CloudFormation Stacks und zugewiesenen Tags anzeigen und verwalten.

- Komponente erstellen — Erstellen Sie eine Komponente. Geben Sie den Namen und die Beschreibung der Komponente ein, wählen Sie die zugehörigen Ressourcen aus, geben Sie die IaC-Quelldatei der Komponente an und weisen Sie Tags zu.
- Komponente aktualisieren — Um eine Komponente zu aktualisieren, wählen Sie die Komponente in der Komponentenliste aus und wählen Sie dann im Menü Aktionen die Option Komponente aktualisieren aus. Wählen Sie alternativ auf den Seiten mit den Komponentendetails die Option Aktualisieren aus.

  Sie können die meisten Details der Komponente aktualisieren. Sie können den Komponenten-Namen nicht aktualisieren. Und Sie können wählen, ob Sie die Komponente nach einem erfolgreichen Update erneut bereitstellen möchten oder nicht.
- Umgebung konfigurieren — Wenn Sie eine Umgebung erstellen oder aktualisieren, können Sie eine Komponentenrolle angeben. Diese Rolle steuert die Fähigkeit, direkt definierte Komponenten in der Umgebung auszuführen, und gewährt Berechtigungen für deren Bereitstellung.
- Neue Service-Vorlagenversion erstellen — Wenn Sie eine Service-Template-Version erstellen, können Sie Unterstützte Komponentenquellen für die Vorlagenversion angeben. Dies steuert die Fähigkeit, Komponenten an Dienstinstanzen von Diensten anzuhängen, die auf dieser Vorlagenversion basieren.

Komponenten in derAWS Proton API undAWS CLI

Verwenden Sie dieAWS Proton API oder die,AWS CLI umAWS Proton Komponenten zu erstellen, zu aktualisieren, anzuzeigen und zu verwenden.

Mit den folgenden API-Aktionen werdenAWS Proton Komponentenressourcen direkt verwaltet.

- CreateComponent— Erstellen Sie eineAWS Proton Komponente.
- DeleteComponent— Löscht eineAWS Proton Komponente.
- GetComponent— Holen Sie sich detaillierte Daten für eine Komponente.
- ListComponentOutputs— Ruft eine Liste der Komponentenausgaben (Infrastructure as Code) ab.
- ListComponentProvisionedResources— Listet bereitgestellte Ressourcen für eine Komponente mit Details auf.

- ListComponents— Listet Komponenten mit zusammenfassenden Daten auf. Sie können die Ergebnisliste nach Umgebung, Dienst oder einer einzelnen Dienstinstanz filtern.

Die folgenden API-Aktionen andererAWS Proton Ressourcen haben einige Funktionen, die sich auf Komponenten beziehen.

- CreateEnvironment, UpdateEnvironment— Wird verwendet,`componentRoleArn` um den Amazon-Ressourcennamen (ARN) der IAM-Servicerolle anzugeben, die bei der Bereitstellung direkt definierter Komponenten in dieser UmgebungAWS Proton verwendet wird. Sie bestimmt den Umfang der Infrastruktur, die eine direkt definierte Komponente bereitstellen kann.
- CreateServiceTemplateVersion— Wird verwendet`supportedComponentSources`, um unterstützte Komponentenquellen anzugeben. Komponenten mit unterstützten Quellen können auf Basis dieser Service-Template-Version an Service-Instanzen angehängt werden.

Häufig gestellte Fragen zur Komponente

Was ist der Lebenszyklus einer Komponente?

Komponenten können sich in einem angeschlossenen oder getrennten Zustand befinden. Sie sind so konzipiert, dass sie an eine Service-Instance angefügt werden können und deren Infrastruktur in den meisten Fällen verbessern. Getrennte Komponenten befinden sich in einem Übergangszustand, der es Ihnen ermöglicht, eine Komponente zu löschen oder sie auf kontrollierte und sichere Weise an eine andere Service-Instance anzuhängen. Weitere Informationen finden Sie unter the section called “Komponenten-Zustände”.

Warum kann ich meine angehängten Komponenten nicht löschen?

Lösung: Um eine angehängte Komponente zu löschen, aktualisieren Sie die Komponente, um sie von der Dienstinstanz zu trennen, überprüfen Sie die Stabilität der Dienstinstanz und löschen Sie dann die Komponente.

Warum ist das erforderlich? Angehängte Komponenten bieten zusätzliche Infrastruktur, die Ihre Anwendung benötigt, um ihre Laufzeitfunktionen auszuführen. Die Dienstinstanz verwendet möglicherweise Komponentenausgaben, um Ressourcen dieser Infrastruktur zu erkennen und zu nutzen. Das Löschen der Komponente und damit das Entfernen ihrer Infrastrukturressourcen könnte die angehängte Dienstinstanz stören.

Als zusätzliche SicherheitsmaßnahmeAWS Proton müssen Sie die Komponente aktualisieren und von ihrer Dienstinstanz trennen, bevor Sie sie löschen können. Anschließend können Sie Ihre Dienstinstanz validieren, um sicherzustellen, dass sie weiterhin ordnungsgemäß bereitgestellt und funktioniert. Wenn Sie ein Problem feststellen, können Sie die Komponente schnell wieder an die Dienstinstanz anhängen und dann daran arbeiten, das Problem zu beheben. Wenn Sie sicher sind, dass Ihre Service-Instance keine Abhängigkeit von der Komponente hat, können Sie die Komponente problemlos löschen.

Warum kann ich die angehängte Dienstinstanz einer Komponente nicht direkt ändern?

Lösung: Um den Anhang zu ändern, aktualisieren Sie die Komponente, um sie von der Dienstinstanz zu trennen, überprüfen Sie die Stabilität von Komponenten und Dienstinstanzen und hängen Sie die Komponente dann an die neue Dienstinstanz an.

Warum ist das erforderlich? Eine Komponente ist so konzipiert, dass sie an eine Dienstinstanz angehängt werden kann. Ihre Komponente verwendet möglicherweise Dienstinstanzeingaben für die Benennung und Konfiguration von Infrastrukturressourcen. Das Ändern der angefügten Service-Instance könnte die Komponente unterbrechen (zusätzlich zu einer möglichen Störung der Service-Instance, wie in den vorherigen häufig gestellten Fragen beschrieben, Warum kann ich meine angeschlossenen Komponenten nicht löschen?). Dies kann beispielsweise dazu führen, dass Ressourcen, die in der IaC-Vorlage der Komponente definiert sind, umbenannt und möglicherweise sogar ersetzt werden.

Als zusätzliche SicherheitsmaßnahmeAWS Proton müssen Sie die Komponente aktualisieren und von ihrer Dienstinstanz trennen, bevor Sie sie an eine andere Service-Instance anhängen können. Sie können dann die Stabilität sowohl der Komponente als auch der Dienstinstanz überprüfen, bevor Sie die Komponente an die neue Dienstinstanz anhängen.

Komponenten-Zustände

AWS ProtonKomponenten können sich in zwei grundlegend unterschiedlichen Zuständen befinden:

- Angefügt — Die Komponente ist an eine Dienstinstanz angehängt. Es definiert eine Infrastruktur, die die Laufzeitfunktionalität der Dienstinstanz unterstützt. Die Komponente erweitert die in den Umgebungs- und Dienstvorlagen definierte Infrastruktur um eine vom Entwickler definierte Infrastruktur.

  Eine typische Komponente befindet sich während des größten Teils ihres Lebenszyklus im zugefügten Zustand.

- Getrennt — Die Komponente ist einerAWS Proton Umgebung zugeordnet und an keine Dienstinstanz in der Umgebung angehängt.

  Dies ist ein Übergangszustand zur Verlängerung der Lebensdauer einer Komponente über eine einzelne Dienstinstanz hinaus.

Die folgende Tabelle bietet einen Vergleich der verschiedenen Komponentenzustände auf oberster Ebene.

	Attached (Angefügt)	Detached (Getrennt)
Hauptzweck des Staates	Um die Infrastruktur einer Service-Instance zu erweitern.	Zur Aufrechterhaltung der Infrastruktur der Komponente zwischen Service-Instance-Anhängen.
Verbunden mit	Eine Dienstinstanz und eine Umgebung	Eine -Umgebung
Wichtige spezifische Eigenschaften	• Service-Name • Servicevorlage • Spezifikation	• Environment name
Kann gelöscht werden	✗ Nein	✓ Ja
Kann auf eine andere Dienstinstanz aktualisiert werden	✗ Nein	✓ Ja
Kann Eingaben lesen	✓ Ja	✗ Nein

Der Hauptzweck einer Komponente besteht darin, einer Service-Instance zugeordnet zu werden und deren Infrastruktur um zusätzliche Ressourcen zu erweitern. Eine angehängte Komponente kann gemäß der Spezifikation Eingaben von der Dienstinstanz lesen. Sie können die Komponente nicht direkt löschen oder an eine andere Dienstinstanz anhängen. Sie können auch nicht die zugehörige

Dienstinstanz oder den zugehörigen Dienst und die zugehörige Umgebung löschen. Um eines dieser Dinge zu tun, aktualisieren Sie die Komponente, um sie zuerst von ihrer Dienstinstanz zu trennen.

Um die Infrastruktur der Komponente über die Lebensdauer einer einzelnen Dienstinstanz hinaus aufrechtzuerhalten, aktualisieren Sie die Komponente und trennen sie von ihrer Dienstinstanz, indem Sie die Service- und Dienstinstanznamen entfernen. Dieser abgegrenzte Zustand ist ein Übergangszustand. Die Komponente hat keine Eingänge. Die Infrastruktur bleibt verfügbar und Sie können sie aktualisieren. Sie können Ressourcen löschen, mit denen die Komponente verknüpft war, als sie angefügt wurde (Dienstinstanz, Dienst). Sie können die Komponente löschen oder aktualisieren, sodass sie erneut an eine Dienstinstanz angehängt wird.

Komponenteninfrastruktur als Codedateien

IaC-Dateien (Component Infrastructure as Code) ähneln denen für andereAWS Proton Ressourcen. Erfahren Sie hier einige Details, die spezifisch für Komponenten sind. Vollständige Informationen zur Erstellung von IaC-Dateien fürAWS Proton finden Sie unterVorlagenerstellung und Pakete.

Parameter mit Komponenten verwenden

DerAWS Proton Parameter-Namespace enthält einige Parameter, auf die eine Service-IAC-Datei verweisen kann, um den Namen und die Ausgaben einer zugehörigen Komponente abzurufen. Der Namespace enthält auch Parameter, auf die eine Komponenten-IAC-Datei verweisen kann, um Eingaben, Ausgaben und Ressourcenwerte aus der Umgebung, dem Dienst und der Dienstinstanz abzurufen, mit der die Komponente verknüpft ist.

Eine Komponente hat keine eigenen Eingaben — sie erhält ihre Eingaben von der Service-Instance, an die sie angehängt ist. Eine Komponente kann auch Umgebungsausgaben lesen.

Weitere Hinweise zur Verwendung von Parametern in Komponenten- und zugehörigen Service-IAC-Dateien finden Sie unterthe section called “Komponenten- CloudFormation IaC-Parameter”. Allgemeine Hinweise zuAWS Proton Parametern und eine vollständige Referenz zum Parameter-Namespace finden Sie unterthe section called “Parameter”.

Erstellung robuster IaC-Dateien

Als Administrator können Sie beim Erstellen einer Service-Template-Version entscheiden, ob Sie zulassen möchten, dass Service-Instanzen, die aus der Vorlagenversion erstellt wurden, angehängte Komponenten haben. Den supportedComponentSourcesParameter der

CreateServiceTemplateVersionAPI-Aktion finden Sie in der AWS ProtonAPI-Referenz. Bei jeder future Service-Instance entscheidet jedoch die Person, die die Instance erstellt, ob sie ihr eine Komponente anfügt oder nicht, und (im Fall von direkt definierten Komponenten) erstellt die Komponente. IaC ist in der Regel eine andere Person — ein Entwickler, der Ihre Service-Vorlage verwendet. Daher können Sie nicht garantieren, dass eine Komponente an eine Service-Instance angehängt wird. Sie können auch nicht die Existenz bestimmter Komponentenausgabenamen oder die Gültigkeit und Sicherheit der Werte dieser Ausgaben garantieren.

AWS Protonund die Jinja-Syntax helfen Ihnen, diese Probleme zu umgehen und robuste Service-Vorlagen zu erstellen, die auf folgende Weise fehlerfrei gerendert werden:

- AWS ProtonParameterfilter — Wenn Sie auf die Ausgabeigenschaften von Komponenten verweisen, können Sie Parameterfilter verwenden — Modifikatoren, die Parameterwerte validieren, filtern und formatieren. Weitere Informationen und Beispiele finden Sie unter the section called “CloudFormation Parameterfilter”.
- Standardwert für einzelne Eigenschaften — Wenn Sie auf eine einzelne Ressource oder Ausgabe-Eigenschaft einer Komponente verweisen, können Sie sicherstellen, dass das Rendern Ihrer Service-Vorlage nicht fehlschlägt, indem Sie den`default` Filter mit oder ohne Standardwert verwenden. Wenn die Komponente oder ein bestimmter Ausgabeparameter, auf den Sie sich beziehen, nicht existiert, wird stattdessen der Standardwert (oder eine leere Zeichenfolge, falls Sie keinen Standardwert angegeben haben) gerendert, und das Rendern ist erfolgreich. Weitere Informationen finden Sie unter the section called “Standardwerte angeben”.

  Beispiele:

  - `{{ service_instance.components.default.name | default("") }}`
  - `{{ service_instance.components.default.outputs.my-output | default("17") }}`

  > **Note**
  >
  > Verwechseln Sie nicht den`.default` Teil des Namespaces, der direkt definierte Komponenten bezeichnet, mit dem`default` Filter, der einen Standardwert bereitstellt, wenn die referenzierte Eigenschaft nicht existiert.

- Vollständige Objektreferenz — Wenn Sie auf die gesamte Komponente oder auf die Sammlung der Ausgaben einer Komponente verweisen, wird ein leeres ObjektAWS Proton zurückgegeben und somit garantiert`{}`, dass das Rendern Ihrer Service-Vorlage nicht fehlschlägt. Sie müssen keinen

Filter verwenden. Stellen Sie sicher, dass Sie die Referenz in einem Kontext erstellen, der ein leeres Objekt annehmen kann, oder verwenden Sie eine`{{ if .. }}` Bedingung, um zu testen, ob ein leeres Objekt vorhanden ist.

Beispiele:

- `{{ service_instance.components.default }}`
- `{{ service_instance.components.default.outputs }}`

AWS CloudFormationBeispiel für eine Komponente

Hier ist ein vollständiges Beispiel für eineAWS Proton direkt definierte Komponente und wie Sie sie in einemAWS Proton Service verwenden können. Die Komponente stellt einen Amazon-Simple-Storage-Service Simple Storage Service (Amazon S3) -Bucket und die zugehörige Zugriffsrichtlinie bereit. Die Dienstinstanz kann auf diesen Bucket verweisen und ihn verwenden. Der Bucket-Name basiert auf den Namen der Umgebung, des Dienstes, der Dienstinstanz und der Komponente, was bedeutet, dass der Bucket mit einer bestimmten Instanz der Komponentenvorlage gekoppelt ist, die eine bestimmte Dienstinstanz erweitert. Entwickler können auf der Grundlage dieser Komponentenvorlage mehrere Komponenten erstellen, um Amazon S3 S3-Buckets für unterschiedliche Service-Instances und funktionale Anforderungen bereitzustellen.

Das Beispiel behandelt das Erstellen der verschiedenen erforderlichenAWS CloudFormation Infrastructure-as-Code-Dateien (IaC) und das Erstellen einer erforderlichen RolleAWS Identity and Access Management (IAM). Das Beispiel gruppiert die Schritte nach den Rollen der Besitzer.

Administratorschritte

Um Entwicklern die Verwendung von Komponenten mit einem Dienst zu ermöglichen

1. Erstellen Sie eineAWS Identity and Access Management (IAM-) Rolle, die die Ressourcen einschränkt, die direkt definierte Komponenten, die in Ihrer Umgebung ausgeführt werden, bereitstellen können. AWS Protonübernimmt diese Rolle später, um direkt definierte Komponenten in der Umgebung bereitzustellen.

   Verwenden Sie für dieses Beispiels die folgende Richtlinie:

   Example direkt definierte Komponentenrolle

   ```
   {
   ```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "cloudformation:CancelUpdateStack",
      "cloudformation:CreateChangeSet",
      "cloudformation:DeleteChangeSet",
      "cloudformation:DescribeStacks",
      "cloudformation:ContinueUpdateRollback",
      "cloudformation:DetectStackResourceDrift",
      "cloudformation:DescribeStackResourceDrifts",
      "cloudformation:DescribeStackEvents",
      "cloudformation:CreateStack",
      "cloudformation:DeleteStack",
      "cloudformation:UpdateStack",
      "cloudformation:DescribeChangeSet",
      "cloudformation:ExecuteChangeSet",
      "cloudformation:ListChangeSets",
      "cloudformation:ListStackResources"
    ],
    "Resource": "arn:aws:cloudformation:*:123456789012:stack/AWSProton-*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:CreateBucket",
      "s3:DeleteBucket",
      "s3:GetBucket",
      "iam:CreatePolicy",
      "iam:DeletePolicy",
      "iam:GetPolicy",
      "iam:ListPolicyVersions",
      "iam:DeletePolicyVersion"
    ],
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "cloudformation.amazonaws.com"
      }
    }
  }
]
```

```
}
```

2. Geben Sie die Rolle an, die Sie im vorherigen Schritt erstellt haben, wenn Sie die Umgebung erstellen oder aktualisieren. Geben Sie in derAWS Proton Konsole auf der Seite „Umgebung konfigurieren“ eine Komponentenrolle an. Wenn Sie dieAWS Proton API verwenden oderAWS CLI geben Sie`componentRoleArn` die CreateEnvironmentoder UpdateEnvironmentAPI-Aktionen an.
3. Erstellen Sie eine Service-Vorlage, die sich auf eine direkt definierte Komponente bezieht, die an die Dienstinstanz angehängt ist.

   Das Beispiel zeigt, wie ein robustes Service-Template geschrieben wird, das nicht kaputt geht, wenn eine Komponente nicht an die Service-Instance angehängt ist.

   Example CloudFormation IAC-Datei mit einer Komponente bedienen

```
# service/instance_infrastructure/cloudformation.yaml

Resources:
  TaskDefinition:
    Type: AWS::ECS::TaskDefinition
    Properties:
      TaskRoleArn: !Ref TaskRole
      ContainerDefinitions:
        - Name: '{{service_instance.name}}'
          # ...
          {% if service_instance.components.default.outputs | length > 0 %}
          Environment:
            {{ service_instance.components.default.outputs |
                proton_cfn_ecs_task_definition_formatted_env_vars }}
          {% endif %}

  # ...

  TaskRole:
    Type: AWS::IAM::Role
    Properties:
      # ...
      ManagedPolicyArns:
        - !Ref BaseTaskRoleManagedPolicy
        {{ service_instance.components.default.outputs
            | proton_cfn_iam_policy_arns }}
```

```
  # Basic permissions for the task
  BaseTaskRoleManagedPolicy:
    Type: AWS::IAM::ManagedPolicy
    Properties:
      # ...
```

4. Erstellen Sie eine neue Service-Template-Nebenversion, die direkt definierte Komponenten als unterstützt deklariert.

   - Vorlagenpaket in Amazon S3 — Wählen Sie in derAWS Proton Konsole, wenn Sie eine Service-Template-Version erstellen, für Unterstützte Komponentenquellen die Option Direkt definiert aus. Wenn Sie dieAWS Proton API verwenden oderAWS CLI geben Sie`DIRECTLY_DEFINED` im`supportedComponentSources` Parameter der CreateServiceTemplateVersionoder UpdateServiceTemplateVersionAPI-Aktionen an.
   - Vorlagensynchronisierung — Übernehmen Sie eine Änderung in Ihr Service Template-Bundle-Repository, das Sie`DIRECTLY_DEFINED` als Element von`supported_component_sources:` in der`.template-registration.yaml` Datei im Hauptversionsverzeichnis angeben. Weitere Informationen über diese Datei finden Sie unter the section called “Synchronisieren von Dienstvorlagen”.

5. Veröffentlichen Sie die Nebenversion der Servicevorlage Weitere Informationen finden Sie unter the section called “Veröffentlichen”.
6. Stellen Sie sicher, dass Entwickler, die dieses Service-Template verwenden, die IAM-Rolle übernehmen.`proton:CreateComponent`

Schritte für Entwickler

Um eine direkt definierte Komponente mit einer Dienstinstanz zu verwenden

1. Erstellen Sie einen Dienst, der die Dienstvorlagenversion verwendet, die der Administrator mit Komponentenunterstützung erstellt hat. Alternativ können Sie eine Ihrer vorhandenen Service-Instanzen aktualisieren, um die neueste Vorlagenversion zu verwenden.
2. Schreiben Sie eine IaC-Vorlagendatei für Komponenten, die einen Amazon S3 S3-Bucket und eine zugehörige Zugriffsrichtlinie bereitstellt und diese Ressourcen als Ausgaben bereitstellt.

   Example CloudFormation Komponenten-IAC-Datei

   ```
   # cloudformation.yaml
   ```

```
# A component that defines an S3 bucket and a policy for accessing the bucket.
Resources:
  S3Bucket:
    Type: 'AWS::S3::Bucket'
    Properties:
      BucketName: '{{environment.name}}-{{service.name}}-{{service_instance.name}}-
{{component.name}}'
  S3BucketAccessPolicy:
    Type: AWS::IAM::ManagedPolicy
    Properties:
      PolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Action:
              - 's3:Get*'
              - 's3:List*'
              - 's3:PutObject'
            Resource: !GetAtt S3Bucket.Arn
Outputs:
  BucketName:
    Description: "Bucket to access"
    Value: !GetAtt S3Bucket.Arn
  BucketAccessPolicyArn:
    Value: !Ref S3BucketAccessPolicy
```

3. Wenn Sie dieAWS Proton API verwenden oderAWS CLI schreiben Sie eine Manifestdatei für die Komponente.

   Example direkt definiertes Komponentenmanifest

   ```
   infrastructure:
     templates:
       - file: "cloudformation.yaml"
         rendering_engine: jinja
         template_language: cloudformation
   ```

4. Erstellen Sie eine direkt definierte Komponente. AWS Protonübernimmt die Komponentenrolle, die der Administrator für die Bereitstellung der Komponente definiert hat.

   Wählen Sie in derAWS Proton Konsole auf der Seite Komponenten die Option Komponente erstellen aus. Geben Sie für Komponenteneinstellungen einen Komponentennamen und eine optionale Komponentenbeschreibung ein. Wählen Sie für Komponentenanhang die Option

Komponente an eine Dienstinstanz anhängen aus. Wählen Sie Ihre Umgebung, Ihren Dienst und Ihre Dienstinstanz aus. Wählen Sie als Komponentenquelle die Komponenten-IAC-Datei aus AWS CloudFormation, und wählen Sie dann aus.

> **Note**
>
> Sie müssen kein Manifest bereitstellen — die Konsole erstellt eines für Sie.

Wenn Sie dieAWS Proton API oder verwendenAWS CLI, verwenden Sie die CreateComponentAPI-Aktion. Stellen Sie eine Komponente`name` und optional ein`description`. Se`environmentName``serviceName`, und`serviceInstanceName`. Legen Sie`templateSourcemanifest` die Pfade der von Ihnen erstellten Dateien fest.

> **Note**
>
> Die Angabe eines Umgebungsnamens ist optional, wenn Sie Service- und Dienstinstanznamen angeben. Die Kombination dieser beiden ist in IhremAWS Konto einzigartig undAWS Proton kann die Umgebung anhand der Dienstinstanz bestimmen.

5. Aktualisieren Sie Ihre Service-Instance, um sie erneut bereitzustellen. AWS Protonverwendet Ausgaben Ihrer Komponente in der Vorlage für gerenderte Service-Instances, damit Ihre Anwendung den Amazon S3 S3-Bucket verwenden kann, den die Komponente bereitgestellt hat.

Verwenden von Git-Repositorys mitAWS Proton

AWS Protonverwendet Git-Repositorys für eine Vielzahl von Zwecken. In der folgenden Liste werden die Repository-Typen kategorisiert, dieAWS Proton Ressourcen zugeordnet sind. FürAWS Proton Funktionen, die wiederholt eine Verbindung zu deinem Repository herstellen, um entweder Inhalte dorthin zu pushen oder Inhalte daraus abzurufen, musst duAWS Proton in deinemAWS Konto einen Repository-Link mit registrieren. Ein Repository-Link besteht aus einer Reihe von Eigenschaften, die verwendetAWS Proton werden können, wenn er eine Verbindung zu einem Repository herstellt. AWS Protonunterstützt derzeitGitHub,GitHub Enterprise undBitBucket.

Repositorys für Entwickler

Code-Repository — Ein Repository, das Entwickler zum Speichern von Anwendungscode verwenden. Wird für die Codebereitstellung verwendet. AWS Protoninteragiert nicht direkt mit diesem Repository. Wenn ein Entwickler einen Dienst bereitstellt, der eine Pipeline enthält, gibt er den Namen des Repositorys und den Branch an, aus dem der Anwendungscode gelesen werden soll. AWS Protonleitet diese Informationen an die bereitgestellte Pipeline weiter.

Weitere Informationen finden Sie unter the section called “Erstellen”.

Administrator-Repositorys

Vorlagen-Repository — Ein Repository, in dem AdministratorenAWS Proton Vorlagenpakete speichern. Wird für die Vorlagensynchronisierung verwendet. Wenn ein Administrator eine Vorlage in erstelltAWS Proton, kann er auf ein Vorlagen-Repository verweisen undAWS Proton die neue Vorlage damit synchronisieren. Wenn der Administrator das Vorlagenpaket im Repository aktualisiert,AWS Proton wird automatisch eine neue Vorlagenversion erstellt. Verknüpfen Sie ein Vorlagen-Repository mit,AWS Proton bevor Sie es für die Synchronisierung verwenden können.

Weitere Informationen finden Sie unter the section called “Konfigurationen für die Vorlagensynchronisierung”.

> **Note**
>
> Ein Vorlagen-Repository ist nicht erforderlich, wenn Sie Ihre Vorlagen weiterhin auf Amazon Simple Storage Service (Amazon S3) hochladen und dieAWS Proton Vorlagenverwaltungs-APIs aufrufen, um neue Vorlagen oder Vorlagenversionen zu erstellen.

Selbstverwaltete Redie

Infrastruktur-Repository — Ein Repository, das gerenderte Infrastrukturvorlagen hostet. Wird für die selbstverwaltete Bereitstellung der Ressourceninfrastruktur verwendet. Wenn ein Administrator eine Umgebung für die selbstverwaltete Bereitstellung erstellt, stellt er ein Repository bereit. AWS Protonsendet Pull-Requests (PRs) an dieses Repository, um die Infrastruktur für die Umgebung und für jede in der Umgebung bereitgestellte Dienstinstanz zu erstellen. Verknüpfen Sie ein Infrastruktur-Repository mit,AWS Proton bevor Sie es für die selbstverwaltete Infrastrukturbereitstellung verwenden können.

Pipeline-Repository — Ein Repository, das zum Erstellen von Pipelines verwendet wird. Wird für die selbstverwaltete Bereitstellung von Pipelines verwendet. Die Verwendung eines zusätzlichen Repositorys zur Bereitstellung von Pipelines ermöglichtAWS Proton das Speichern von Pipeline-Konfigurationen unabhängig von einer einzelnen Umgebung oder einem einzelnen Dienst. Sie müssen nur ein einziges Pipeline-Repository für all Ihre selbstverwalteten Bereitstellungsdienste bereitstellen. Verknüpfen Sie ein Pipeline-Repository mit,AWS Proton bevor Sie es für die selbstverwaltete Pipeline-Bereitstellung verwenden können.

Weitere Informationen finden Sie unter the section called “AWS-verwaltete Bereitstellung”.

Themen

Erstelle einen Link zu deinem Repository

Sie können mit der Konsole oder CLI einen Link zu Ihrem Redie. Wenn Sie einen Repository-Link erstellen,AWS Proton wird eine serviceverknüpfte Rolle für Sie erstellt.

AWS Management Console

Erstellen Sie einen Link zu Ihrem Repository, wie in den folgenden Konsolenschritten gezeigt.

1. Wählen Sie in der AWS ProtonKonsole Repositories aus.
2. Wählen Sie Repository erstellen aus.

3. Gehen Sie auf der Seite Neues Repository verknüpfen im Abschnitt Repository-Details wie folgt vor:

   a. Wählen Sie Ihren Repository-Anbieter.

   b. Wählen Sie eine Ihrer bestehenden Verbindungen. Wenn Sie noch keine haben, wählen Sie NeueCodeStar Verbindung hinzufügen, um eine Verbindung herzustellen, und kehren Sie dann zurAWS Proton Konsole zurück, aktualisieren Sie die Verbindungsliste und wählen Sie Ihre neue Verbindung aus.

   c. Wählen Sie aus Ihren verbundenen Quellcode-Repositorys.

4. [optional] Wählen Sie im Abschnitt „Tags“ die Option „Neues Tag einmal oder mehrmals hinzufügen“ und geben Sie Schlüssel - und Wertepaare ein.

5. Wählen Sie Repository erstellen aus.

6. Sehen Sie sich die Detaildaten für Ihr verknüpftes Repository an.

AWS CLI

Erstellen und registrieren Sie einen Link zu Ihrem Repository.

Führen Sie den Befehl aus:

```
$ aws proton create-repository \
    --name myrepos/environments \
    --connection-arn "arn:aws:codestar-connections:region-
id:123456789012:connection/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
    --provider "GITHUB" \
    --encryption-key "arn:aws:kms:region-id:123456789012:key/bPxRfiCYEXAMPLEKEY" \
    --tags key=mytag1,value=value1 key=mytag2,value=value2
```

Die letzten beiden Parameter--encryption-key und--tags, sind optional.

Antwort:

```
{
    "repository": {
        "arn": "arn:aws:proton:region-id:123456789012:repository/github:myrepos/
environments",
        "connectionArn": "arn:aws:codestar-connections:region-
id:123456789012:connection/2ad03b28-a7c4-EXAMPLE11111",
        "encryptionKey": "arn:aws:kms:region-id:123456789012:key/
bPxRfiCYEXAMPLEKEY",
```

```
        "name": "myrepos/environments",
        "provider": "GITHUB"
    }
}
```

Nachdem Sie einen Repository-Link erstellt haben, können Sie eine Liste derAWS vom Kunden verwalteten Tags anzeigen, wie im folgenden Beispielbefehl gezeigt. AWS Protongeneriert automatischAWS verwaltete Tags für Sie. Sie können auch vom Kunden verwaltete Tags ändern und erstellen, indem Sie die verwendenAWS CLI. Weitere Informationen finden Sie unter AWS ProtonRessourcen und Tagging.

Befehl:

```
$ aws proton list-tags-for-resource \
    --resource-arn "arn:aws:proton:region-id:123456789012:repository/github:myrepos/
environments"
```

Verlinkte Repository-Daten anzeigen

Sie können verknüpfte Repository-Details mithilfe der Konsole oder der auflisten und anzeigenAWS CLI. Für Repository-Links, mit denen Git-Repositorys synchronisiert werdenAWS Proton, können Sie die Definition und den Status der Repository-Synchronisierung mithilfe von abrufenAWS CLI.

AWS Management Console

Mit der AWS ProtonKonsole können Sie verknüpfte Repository-Details auflisten und anzeigen.

1. Um eine Liste Ihrer verknüpften Repositorys anzuzeigen, wählen Sie im Navigationsbereich Repositorys aus.
2. Um Detaildaten anzuzeigen, wählen Sie den Namen eines Repositorys.

AWS CLI

Listen Sie Ihre verknüpften Repositorys auf.

Führen Sie den Befehl aus:

```
$ aws proton list-repositories
```

Antwort:

```
{
    "repositories": [
        {
            "arn": "arn:aws:proton:region-id:123456789012:repository/github:myrepos/
templates",
            "name": "myrepos/templates",
            "provider": "GITHUB"
        },
        {
            "arn": "arn:aws:proton:region-id:123456789012:repository/github:myrepos/
environments",
            "name": "myrepos/environments",
            "provider": "GITHUB"
        }
    ]
}
```

Sehen Sie sich die Details eines verknüpften Repositorys an.

Führen Sie den Befehl aus:

```
$ aws proton get-repository \
    --name myrepos/templates \
    --provider "GITHUB"
```

Antwort:

```
{
    "repository": {
        "arn": "arn:aws:proton:region-id:123456789012:repository/github:myrepos/
templates",
        "name": "myrepos/templates",
        "provider": "GITHUB"
    }
}
```

Listen Sie Ihre synchronisierten Repositorys auf.

Das folgende Beispiel listet Repositorys auf, die Sie für die Vorlagensynchronisierung konfiguriert haben.

Führen Sie den Befehl aus:

```
$ aws proton list-repository-sync-definitions \
    --branch "main" \
    --repository-name myrepos/templates \
    --repository-provider "GITHUB" \
    --sync-type "TEMPLATE_SYNC"
```

Zeigt den Repository-Synchronisierungsstatus an.

Das folgende Beispiel ruft den Synchronisierungsstatus eines Temdie für die Abfrage.

Führen Sie den Befehl aus:

```
$ aws proton get-repository-sync-status \
    --branch "main" \
    --repository-name myrepos/templates \
    --repository-provider "GITHUB" \
    --sync-type "TEMPLATE_SYNC"
```

Antwort:

```
{
    "latestSync": {
        "events": [
            {
                "event": "Clone started",
                "time": "2021-11-21T00:26:35.883000+00:00",
                "type": "CLONE_STARTED"
            },
            {
                "event": "Updated configuration",
                "time": "2021-11-21T00:26:41.894000+00:00",
                "type": "CONFIG_UPDATED"
            },
            {
                "event": "Starting syncs for commit 62c03ff86eEXAMPLE1111111",
                "externalId": "62c03ff86eEXAMPLE1111111",
                "time": "2021-11-21T00:26:44.861000+00:00",
                "type": "STARTING_SYNC"
            }
        ],
```

```
        "startedAt": "2021-11-21T00:26:29.728000+00:00",
        "status": "SUCCEEDED"
    }
}
```

Löschen eines Redie

Sie können einen RedieAWS CLI.

> **Note**
>
> Durch das Löschen eines Repository-Links wird nur der registrierte Link entfernt, derAWS Proton sich in IhremAWS Konto befindet. Sie löscht keine Informationen aus Ihrem Redie.

AWS Management Console

Löschen Sie einen Repository-Link mithilfe der Konsole.

Auf der Repository-Detailseite.

1. Wählen Sie in der AWS ProtonKonsole Repositories aus.
2. Wählen Sie in der Liste die Schaltfläche links neben dem Redie Schaltfläche links neben dem Redie Schaltfläche links neben dem Redie Schaltfläche links neben dem ReTdie.
3. Wählen Sie Löschen.
4. Sie werden in einem Optionsfeld zur Bestätigung der Aktion Löschen aufgefordert.
5. Folgen Sie den Anweisungen und wählen Sie Ja, löschen.

AWS CLI

Löscht einen Repository-Link.

Führen Sie den Befehl aus:

```
$ aws proton delete-repository \
    --name myrepos/templates \
    --provider"GITHUB"
```

Antwort:

```
{
    "repository": {
        "arn": "arn:aws:proton:region-id:123456789012:repository/github:myrepos/
templates",
        "name": "myrepos/templates",
        "provider": "GITHUB"
    }
}
```

Überwachung AWS Proton

Die Überwachung ist wichtig, um die Zuverlässigkeit, Verfügbarkeit und Leistung von AWS Proton und Ihren - AWS Lösungen aufrechtzuerhalten. Im folgenden Abschnitt werden Überwachungstools beschrieben, die Sie mit verwenden können AWS Proton.

Automatisieren AWS Proton mit EventBridge

Sie können AWS Proton Ereignisse in Amazon überwachen EventBridge. EventBridge stellt einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, software-as-a-service (SaaS)-Anwendungen und bereit AWS-Services. Sie können Ereignisse so konfigurieren, dass sie auf Änderungen des AWS Ressourcenstatus reagieren. EventBridge leitet diese Daten dann an Zielservices wie AWS Lambda und Amazon Simple Notification Service weiter. Diese Ereignisse sind dieselben, die in Amazon CloudWatch Events angezeigt werden. CloudWatch Events stellt einen Stream von Systemereignissen in nahezu Echtzeit bereit, der Änderungen an - AWS Ressourcen beschreibt. Weitere Informationen finden Sie unter Was ist Amazon EventBridge? im Amazon-EventBridge Benutzerhandbuch.

Verwenden Sie EventBridge , um über Statusänderungen in den AWS Proton Bereitstellungsworkflows benachrichtigt zu werden.

Ereignistypen

Ereignisse bestehen aus Regeln, die ein Ereignismuster und Ziele enthalten. Sie konfigurieren eine Regel, indem Sie Ereignismuster und Zielobjekte auswählen:

Ereignismuster

Jede Regel wird als Ereignismuster mit der Quelle und dem Typ der zu überwachenden Ereignisse und den Ereigniszielen ausgedrückt. Um Ereignisse zu überwachen, erstellen Sie eine Regel mit dem Service, den Sie als Ereignisquelle überwachen. Sie können beispielsweise eine Regel mit einem Ereignismuster erstellen, das als Ereignisquelle verwendet AWS Proton , um eine Regel auszulösen, wenn es Änderungen an einem Bereitstellungsstatus gibt.

Targets (Ziele)

Die Regel erhält einen ausgewählten Service als Ereignisziel. Sie können einen Zielservice einrichten, um Benachrichtigungen zu senden, Statusinformationen zu erfassen, Korrekturmaßnahmen zu ergreifen, Ereignisse zu initiieren oder andere Maßnahmen zu ergreifen.

Ereignisobjekte enthalten Standardfelder von ID, Konto, AWS-Region Detailtyp, Quelle, Version, Ressource, Uhrzeit (optional). Das Detailfeld ist ein verschachteltes Objekt, das benutzerdefinierte Felder für das Ereignis enthält.

AWS Proton -Ereignisse werden nach bestem Bemühen ausgegeben. Best-Effort-Zustellung bedeutet, dass der Service versucht, alle Ereignisse an zu senden EventBridge, aber in einigen seltenen Fällen wird ein Ereignis möglicherweise nicht zugestellt.

Für jede AWS Proton Ressource, die Ereignisse ausgeben kann, werden in der folgenden Tabelle der Detailtypwert, die Detailfelder und (falls verfügbar) ein Verweis auf eine Liste von Werten für die `previousStatus` Detailfelder `status` und aufgeführt. Wenn eine Ressource gelöscht wird, ist der Wert des `status` Detailfeldes `DELETED`.

Ressource	Detail-Typ-Wert	Detailfelder

`EnvironmentTemplate`	AWS Proton Statusänderung der Umgebungsvorlage	`name`
		`status`
		`previousStatus`

`EnvironmentTemplateVersion`	AWS Proton Statusänderung der Umgebungsvorlagenversion	`name`
		`majorVersion`
		`minorVersion`
		`status`
		`previousStatus`
		Statuswerte

`ServiceTemplate`	AWS Proton Statusänderung der Servicevorlage	`name` `status`

Ressource	Detail-Typ-Wert	Detailfelder
		`previousStatus`

`ServiceTemplateVersion`	AWS Proton Statusänderung der Servicevorlagenversion	`name`
		`majorVersion`
		`minorVersion`
		`status`
		`previousStatus`
		Statuswerte

`Environment`	AWS Proton Änderung des Umgebungsstatus	`name`
		`status`
		`previousStatus`

`Service`	AWS Proton Änderung des Servicestatus	`name`
		`status`
		`previousStatus`
		Statuswerte

Ressource	Detail-Typ-Wert	Detailfelder

`ServiceInstance`	AWS Proton Statusänderung der Service-Instance	`name`
		`serviceName`
		`status`
		`previousStatus`

`ServicePipeline`	AWS Proton Statusänderung der Service-Pipeline	`serviceName`
		`status`
		`previousStatus`

`EnvironmentAccountConnection`	AWS Proton Änderung des Verbindungsstatus des Umgebungskontos	`id`
		`status`
		`previousStatus`
		Statuswerte

`Component`	AWS Proton Änderung des Komponentenstatus	`name`
		`status`
		`previousStatus`

AWS Proton -Ereignisbeispiele

Die folgenden Beispiele zeigen, wie Ereignisse an senden AWS Proton kann EventBridge.

Servicevorlage

```
{
```

```
    "source": "aws.proton",
    "detail-type": ["AWS Proton Service Template Status Change"],
    "time": "2021-03-22T23:21:40.734Z",
    "resources": ["arn:aws:proton:region_id:123456789012:service-template/sample-
service-template-name"],
    "detail": {
        "name": "sample-service-template-name",
        "status": "PUBLISHED",
        "previousStatus": "DRAFT"
    }
}
```

Servicevorlagenversion

```
{
    "source": "aws.proton",
    "detail-type": ["AWS Proton Service Template Version Status Change"],
    "time": "2021-03-22T23:21:40.734Z",
    "resources": ["arn:aws:proton:region_id:123456789012:service-template/sample-
service-template-name:1.0"],
    "detail": {
        "name": "sample-service-template-name",
        "majorVersion": "1",
        "minorVersion": "0",
        "status": "REGISTRATION_FAILED",
        "previousStatus": "REGISTRATION_IN_PROGRESS"
    }
}
```

Umgebung

```
{
    "source": "aws.proton",
    "detail-type": ["AWS Proton Environment Status Change"],
    "time": "2021-03-22T23:21:40.734Z",
    "resources": ["arn:aws:proton:region_id:123456789012:environment/sample-
environment"],
    "detail": {
        "name": "sample-environment",
        "status": "DELETE_FAILED",
        "previousStatus": "DELETE_IN_PROGRESS"
    }
```

```
}
```

EventBridgeTutorial: Senden von Amazon Simple Notification Service-Warnungen für Änderungen des AWS Proton Servicestatus

In diesem Tutorial verwenden Sie eine AWS Proton vorkonfigurierte Ereignisregel, die Statusänderungen für Ihren AWS Proton Service erfasst. EventBridge sendet die Statusänderungen an ein Amazon SNS-Thema. Sie abonnieren das Thema und Amazon SNS sendet Ihnen Statusänderungs-E-Mails für Ihren AWS Proton Service.

Voraussetzungen

Sie haben einen vorhandenen AWS Proton Service mit dem `Active` Status . Im Rahmen dieses Tutorials können Sie diesem Service Service-Instances hinzufügen und dann die Instances löschen.

Informationen zum Erstellen eines - AWS Proton Service finden Sie unter Erste Schritte. Weitere Informationen finden Sie unter AWS Proton-Kontingente und the section called “Edit (Bearbeiten)”.

Schritt 1: Erstellen und Abonnieren eines Amazon-SNS-Themas

Erstellen Sie ein Amazon SNS-Thema, das als Ereignisziel für die in Schritt 2 erstellte Ereignisregel dient.

Erstellen Sie ein Amazon SNS-Thema.

1. Melden Sie sich an und öffnen Sie die Amazon SNS-Konsole .
2. Wählen Sie im Navigationsbereich Themen, Thema erstellen aus.
3. Auf der Seite Thema erstellen:
    a. Wählen Sie Type Standard aus.
    b. Geben Sie für Name **`tutorial-service-status-change`** einund wählen Sie Thema erstellen aus.
4. Wählen Sie auf der tutorial-service-status-change Detailseite Abonnement erstellen aus.
5. Gehen Sie auf der Seite Abonnement erstellen wie folgt vor:
    a. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus.

b. Geben Sie für Endpunkt eine E-Mail-Adresse ein, auf die Sie aktuell Zugriff haben, und wählen Sie Abonnement erstellen aus.

6. Überprüfen Sie Ihr E-Mail-Konto und warten Sie auf eine E-Mail-Nachricht zur Bestätigung Ihres Abonnements. Wenn Sie es erhalten, öffnen Sie es und wählen Sie Abonnement bestätigen aus.

Schritt 2: Registrieren von Ereignisregeln

Registrieren Sie eine Ereignisregel, die Statusänderungen für Ihren AWS Proton Service erfasst. Weitere Informationen finden Sie unter Voraussetzungen.

Erstellen Sie eine Ereignisregel.

1. Öffnen Sie die Amazon- EventBridge Konsole .
2. Wählen Sie im Navigationsbereich Events (Ereignisse) und Rules (Regeln) aus.
3. Wählen Sie auf der Seite Regeln im Abschnitt Regeln die Option Regel erstellen aus.
4. Gehen Sie auf der Seite Regel erstellen wie folgt vor:

   a. Geben Sie im Abschnitt Name und Beschreibung für Name ein**`tutorial-rule`**.

   b. Wählen Sie im Abschnitt Muster definieren die Option Ereignismuster aus.

      i. Wählen Sie unter Event matching pattern (Ereignisübereinstimmungsmuster) die Option Pre-defined by service (Vordefiniertes Muster nach Service) aus.

      ii. Wählen Sie für Service provider (Serviceanbieter) die Option AWS aus.

      iii. Wählen Sie für Service name (Servicename) AWS Proton aus.

      iv. Wählen Sie für Ereignistyp die Option AWS Proton Servicestatusänderung aus.

      Das Ereignismuster wird in einem Texteditor angezeigt.

      v. Öffnen Sie die AWS Proton -Konsole.

      vi. Wählen Sie im Navigationsbereich Services.

      vii. Wählen Sie auf der Seite Services den Namen Ihres AWS Proton Services aus.

      viii. Kopieren Sie auf der Seite Servicedetails den Amazon-Ressourcennamen (ARN) des Service.

      ix. Navigieren Sie zurück zur EventBridge Konsole und zu Ihrer Tutorial-Regel und wählen Sie im Texteditor Bearbeiten aus.

x. Geben Sie im Texteditor für den Service-ARN ein`"resources":`, den Sie in Schritt v kopiert haben.

```
{
    "source": ["aws.proton"],
    "detail-type": ["AWS Proton Service Status Change"],
    "resources": ["arn:aws:proton:region-id:123456789012:service/your-service"]
}
```

xi. Speichern Sie das Ereignismuster.

c. Im Abschnitt Ziele auswählen:

i. Wählen Sie in Target (Ziel) die Option SNS topic (SNS-Thema) aus.

ii. Wählen Sie für Thema die Option austutorial-service-status-change.

d. Wählen Sie Erstellen.

Schritt 3: Testen Ihrer Ereignisregel

Stellen Sie sicher, dass Ihre Ereignisregel funktioniert, indem Sie Ihrem AWS Proton Service eine Instance hinzufügen.

1. Wechseln Sie zur AWS Proton Konsole .
2. Wählen Sie im Navigationsbereich Services.
3. Wählen Sie auf der Seite Services den Namen Ihres Services aus.
4. Wählen Sie auf der Seite Servicedetails die Option Bearbeiten aus.
5. Wählen Sie auf der Seite Service konfigurieren die Option Weiter aus.
6. Wählen Sie auf der Seite Benutzerdefinierte Einstellungen konfigurieren im Abschnitt Service-Instances die Option Neue Instance hinzufügen aus.
7. Füllen Sie das Formular für Ihre neue Instance aus:

a. Geben Sie einen Name nfür Ihre neue Instance ein.

b. Wählen Sie dieselben kompatiblen Umgebungen aus, die Sie für Ihre vorhandenen Instances ausgewählt haben.

c. Geben Sie Werte für die erforderlichen Eingaben ein.

d. Wählen Sie Weiter aus.

8. Überprüfen Sie Ihre Eingaben und wählen Sie Aktualisieren aus.
9. Nachdem der Servicestatus lautet`Active`, überprüfen Sie Ihre E-Mail, um zu überprüfen, ob Sie AWS Benachrichtigungen erhalten haben, die Statusaktualisierungen enthalten.

```
{
    "version": "0",
    "id": "af76c382-2b3c-7a0a-cf01-936dff228276",
    "detail-type": "AWS Proton Service Status Change",
    "source": "aws.proton",
    "account": "123456789012",
    "time": "2021-06-29T20:40:16Z",
    "region": "region-id",
    "resources": ["arn:aws:proton:region-id:123456789012:service/your-service"],
    "detail": {
        "previousStatus": "ACTIVE",
        "status": "UPDATE_IN_PROGRESS",
        "name": "your-service"
    }
}
```

```
{
    "version": "0",
    "id": "87131e29-ad95-bda2-cd30-0ce825dfb0cd",
    "detail-type": "AWS Proton Service Status Change",
    "source": "aws.proton",
    "account": "123456789012",
    "time": "2021-06-29T20:42:27Z",
    "region": "region-id",
    "resources": ["arn:aws:proton:region-id:123456789012:service/your-service"],
    "detail": {
        "previousStatus": "UPDATE_IN_PROGRESS",
        "status": "ACTIVE",
        "name": "your-service"
    }
}
```

Schritt 4: Bereinigen

Löschen Sie Ihr Amazon SNS-Thema und -Abonnement und löschen Sie Ihre EventBridge Regel.

Löschen Sie Ihr Amazon SNS-Thema und -Abonnement.

1. Navigieren Sie zur Amazon SNS-Konsole .
2. Wählen Sie im Navigationsbereich Subscriptions (Abonnements) aus.
3. Wählen Sie auf der Seite Abonnements das Abonnement aus, das Sie für das Thema mit dem Namen erstellt haben, `tutorial-service-status-change` und wählen Sie dann Löschen aus.
4. Wählen Sie im Navigationsbereich Themen aus.
5. Wählen Sie auf der Seite Themen das Thema mit dem Namen `tutorial-service-status-change` und dann Löschen aus.
6. Ein Modal fordert Sie auf, den Löschvorgang zu überprüfen. Folgen Sie den Anweisungen und wählen Sie Löschen aus.

Löschen Sie Ihre EventBridge Regel.

1. Navigieren Sie zur Amazon- EventBridge Konsole .
2. Wählen Sie im Navigationsbereich Events (Ereignisse) und Rules (Regeln) aus.
3. Wählen Sie auf der Seite Regeln die Regel mit dem Namen `tutorial-rule` und dann Löschen aus.
4. Ein Modal fordert Sie auf, den Löschvorgang zu überprüfen. Wählen Sie Löschen aus.

Löschen Sie die hinzugefügte Service-Instance.

1. Navigieren Sie zur AWS Proton -Konsole.
2. Wählen Sie im Navigationsbereich Services.
3. Wählen Sie auf der Seite Services den Namen Ihres Services aus.
4. Wählen Sie auf der Seite Service-Details die Option Bearbeiten und dann Weiter aus.
5. Wählen Sie auf der Seite Benutzerdefinierte Einstellungen konfigurieren im Abschnitt Service-Instances die Option Löschen für die Service-Instance aus, die Sie im Rahmen dieses Tutorials erstellt haben, und wählen Sie dann Weiter aus.
6. Überprüfen Sie Ihre Eingaben und wählen Sie Aktualisieren aus.
7. Ein Modal fordert Sie auf, den Löschvorgang zu überprüfen. Folgen Sie den Anweisungen und wählen Sie Yes, delete aus.

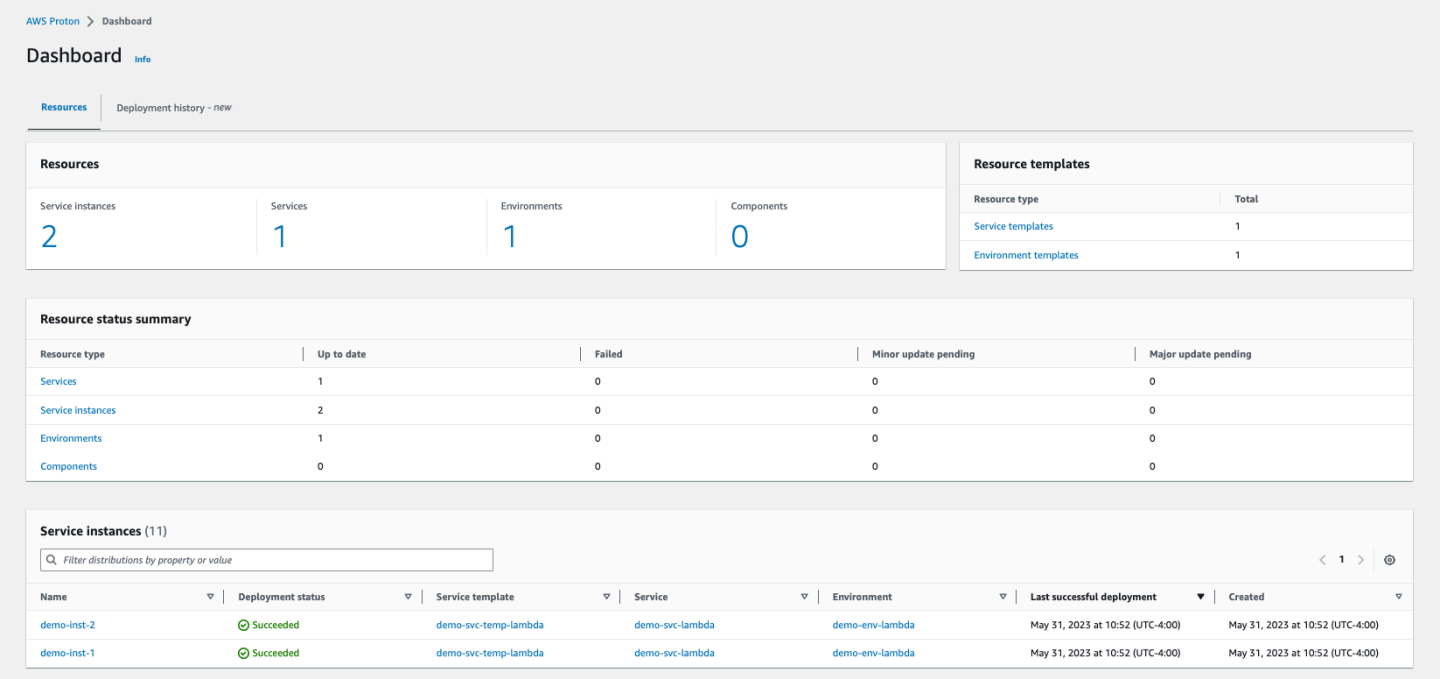
Halten Sie die Infrastruktur mit dem AWS Proton Dashboard auf dem neuesten Stand

Das AWS Proton Dashboard bietet eine Zusammenfassung der AWS Proton Ressourcen in Ihrem AWS Konto, wobei der Schwerpunkt auf Veraltung liegt – wie aktualisierte bereitgestellte Ressourcen aktualisiert wurden. Eine bereitgestellte Ressource ist aktuell, wenn sie die empfohlene Version der zugehörigen Vorlage verwendet. Eine out-of-date bereitgestellte Ressource benötigt möglicherweise ein Haupt- oder Nebenversionsupdate der Vorlage.

Anzeigen des Dashboards in der AWS Proton Konsole

Um das AWS Proton Dashboard anzuzeigen, öffnen Sie die AWS Proton Konsole und wählen Sie dann im Navigationsbereich Dashboard aus.

Ressourcen

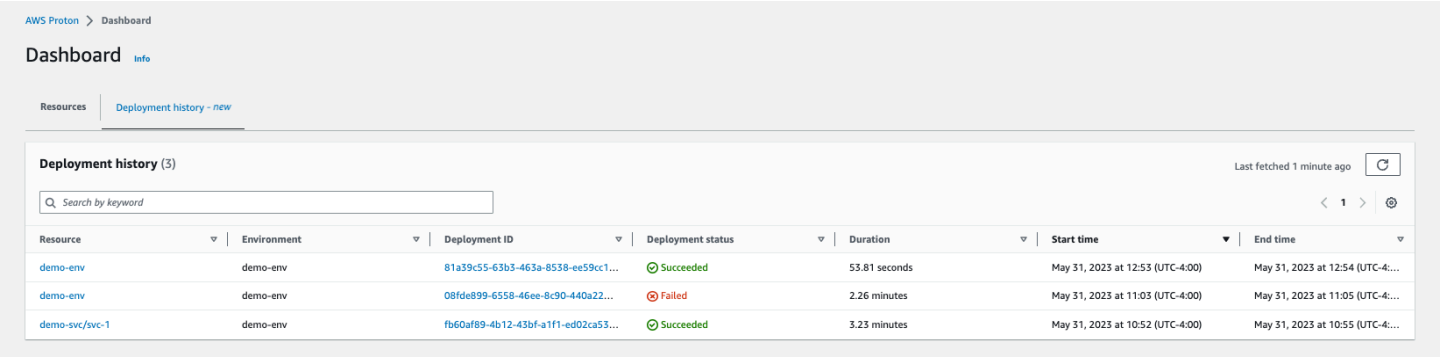


Auf der ersten Registerkarte des Dashboards wird die Anzahl aller Ressourcen in Ihrem Konto angezeigt. Auf der Registerkarte Ressourcen wird die Anzahl Ihrer Service-Instances, Services, Umgebungen und Komponenten sowie Ihre Ressourcenvorlagen angezeigt. Außerdem wird die Ressourcenanzahl für jeden bereitgestellten Ressourcentyp nach dem Status der Ressourcen dieses Typs aufgeschlüsselt. Eine Service-Instance-Tabelle zeigt Details zu jeder Service-Instance – ihren Bereitstellungsstatus, die Ressourcen, AWS Proton mit denen sie verknüpft ist, die Aktualisierungen, die für sie verfügbar sind, und einige Zeitstempel.

Sie können die Service-Instance-Liste nach einer beliebigen Tabelleneigenschaft filtern. Sie können beispielsweise filtern, um Service-Instances mit Bereitstellungen innerhalb eines bestimmten Zeitfensters oder Service-Instances anzuzeigen, die im Vergleich zu Empfehlungen für Haupt- oder Nebenversionen veraltet sind.

Wählen Sie einen Service-Instance-Namen aus, um zur Detailseite der Service-Instance zu navigieren, auf der Sie handeln können, um entsprechende Versionsaktualisierungen vorzunehmen. Wählen Sie einen anderen AWS Proton Ressourcennamen aus, um zur Detailseite zu navigieren, oder wählen Sie einen Ressourcentyp aus, um zur jeweiligen Ressourcenliste zu navigieren.

Bereitstellungsverlauf



Auf der Registerkarte Bereitstellungsverlauf können Sie Details zu Ihren Bereitstellungen anzeigen. In der Tabelle mit dem Bereitstellungsverlauf können Sie den Bereitstellungsstatus sowie Umgebung und Bereitstellungs-ID verfolgen. Sie können den Ressourcennamen oder die Bereitstellungs-ID auswählen, um noch mehr Details anzuzeigen, z. B. eine Bereitstellungsstatusmeldung und Ressourcenausgaben. Mit der Tabelle können Sie auch nach jeder Tabelleneigenschaft filtern.

Sicherheit in AWS Proton

Die Sicherheit in der Cloud hat bei AWS höchste Priorität. Als AWS-Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die eingerichtet wurden, um die Anforderungen der anspruchsvollsten Organisationen in puncto Sicherheit zu erfüllen.

Sicherheit ist eine übergreifende Verantwortlichkeit zwischen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst und Sicherheit in der Cloud:

- Sicherheit der Cloud selbst – AWS ist dafür verantwortlich, die Infrastruktur zu schützen, mit der AWS-Services in der AWS Cloud ausgeführt werden. AWS stellt Ihnen außerdem Services bereit, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS-Compliance-Programme regelmäßig. Informationen zu den Compliance-Programmen, die für AWS Proton gelten, finden Sie unter AWS-Services im Rahmen nach Compliance-Programm.
- Sicherheit in der Cloud – Ihr Verantwortungsumfang wird durch den AWS-Service bestimmt, den Sie verwenden. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der geteilten Verantwortung bei der Verwendung von AWS Proton einsetzen können. Die folgenden Themen veranschaulichen, wie Sie AWS Proton zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfigurieren können. Sie erfahren außerdem, wie Sie andere AWS-Services verwenden, um Ihre AWS Proton-Ressourcen zu überwachen und zu schützen.

Themen

- CodeBuild Bereitstellung von benutzerdefinierter Amazon VPC-Unterstützung

Identitäts- und Zugriffsverwaltung für AWS Proton

AWS Identity and Access Management (IAM) ist ein AWS-Service, mit dem Administratoren den Zugriff auf AWS-Ressourcen sicher steuern können. IAM-Administratoren steuern, wer authentifiziert (angemeldet) und autorisiert (Berechtigungen besitzt) ist, um AWS Proton Ressourcen zu nutzen. IAM ist ein AWS-Service, den Sie ohne zusätzliche Kosten verwenden können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, unterscheidet sich je nach Ihrer Arbeit in AWS Proton.

Service user (Service-Benutzer) – Wenn Sie den AWS Proton-Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen. Wenn Sie für Ihre Arbeit weitere AWS Proton-Funktionen ausführen, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Unter Fehlerbehebung für AWS Proton-Identität und -Zugriff finden Sie nützliche Informationen für den Fall, dass Sie keinen Zugriff auf eine Funktion in AWS Proton haben.

Service administrator (Service-Administrator) – Wenn Sie in Ihrem Unternehmen für AWS Proton-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf AWS Proton. Es

ist Ihre Aufgabe, zu bestimmen, auf welche AWS Proton-Funktionen und Ressourcen Ihre Service-Benutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit AWS Proton verwenden kann, finden Sie unter Featuresweise von AWS Proton mit IAM.

IAM-Administrator – Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf AWS Proton verfassen können. Beispiele für identitätsbasierte AWS Proton-Richtlinien, die Sie in IAM verwenden können, finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS Proton.

Authentifizierung mit Identitäten

Authentifizierung ist die Art, wie Sie sich mit Ihren Anmeldeinformationen bei AWS anmelden. Die Authentifizierung (Anmeldung bei AWS) muss als Root-Benutzer des AWS-Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle erfolgen.

Sie können sich bei AWS als Verbundidentität mit Anmeldeinformationen anmelden, die über eine Identitätsquelle bereitgestellt werden. Benutzer von AWS IAM Identity Center. (IAM Identity Center), die Single-Sign-on-Authentifizierung Ihres Unternehmens und Anmeldeinformationen für Google oder Facebook sind Beispiele für Verbundidentitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie auf AWS mithilfe des Verbunds zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich bei der AWS Management Console oder beim AWS-Zugriffsportal anmelden. Weitere Informationen zum Anmelden bei AWS finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch von AWS-Anmeldung.

Bei programmgesteuerten Zugriff auf AWS bietet AWS ein Software Development Kit (SDK) und eine Command Line Interface (CLI, Befehlszeilenschnittstelle) zum kryptographischen Signieren Ihrer Anforderungen mit Ihren Anmeldeinformationen. Wenn Sie keine AWS-Tools verwenden, müssen Sie Anforderungen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode zum eigenen Signieren von Anforderungen finden Sie unter Signieren von AWS-API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS empfiehlt beispielsweise die Verwendung von Multi-Faktor Authentifizierung (MFA), um die Sicherheit Ihres Kontos zu verbessern. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center-

Benutzerhandbuch und Verwenden der Multi-Faktor-Authentifizierung (MFA) in AWS im IAM-Benutzerhandbuch.

AWS-Konto-Root-Benutzer

Wenn Sie ein AWS-Konto neu erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen des Kontos hat. Diese Identität wird als AWS-Konto-Root-Benutzer bezeichnet. Für den Zugriff auf den Root-Benutzer müssen Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode empfiehlt es sich, menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, aufzufordern, den Verbund mit einem Identitätsanbieter zu verwenden, um auf AWS-Services mit temporären Anmeldeinformationen zuzugreifen.

Eine Verbundidentität ist ein Benutzer aus dem Benutzerverzeichnis Ihres Unternehmens, ein Web Identity Provider, AWS Directory Service, das Identity-Center-Verzeichnis oder jeder Benutzer, der mit Anmeldeinformationen, die über eine Identitätsquelle bereitgestellt werden, auf AWS-Services zugreift. Wenn Verbundidentitäten auf AWS-Konten zugreifen, übernehmen sie Rollen und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen im IAM Identity Center erstellen oder Sie können eine Verbindung mit einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und synchronisieren, um sie in allen AWS-Konten und Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität in Ihrem AWS-Konto mit bestimmten Berechtigungen für eine einzelne Person oder eine einzelne Anwendung. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen

Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

Eine IAM-Gruppe ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter Erstellen eines IAM-Benutzers (anstatt einer Rolle) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität in Ihrem AWS-Konto mit spezifischen Berechtigungen. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der AWS Management Console übernehmen, indem Sie Rollen wechseln. Sie können eine Rolle annehmen, indem Sie eine AWS CLI oder AWS-API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter Verwenden von IAM-Rollen im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center-Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.

- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. In einigen AWS-Services können Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff – Einige AWS-Services verwenden Features in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon EC2 aus oder speichert Objekte in Amazon S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward access sessions (FAS) – Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anforderungen werden nur dann gestellt, wenn ein Dienst eine Anforderung erhält, die Interaktionen mit anderen AWS-Services oder Ressourcen erfordert, um abgeschlossen werden zu können. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.
  - Serviceverknüpfte Rolle – Eine serviceverknüpfte Rolle ist ein Typ von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverbundene Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen in Amazon EC2 – Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und AWS CLI- oder AWS-API-Anforderungen durchführen. Das ist eher zu empfehlen,

als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Erstellen Sie ein Instance-Profil, das an die Instance angefügt ist, um eine AWS-Rolle einer EC2-Instance zuzuweisen und die Rolle für sämtliche Anwendungen der Instance bereitzustellen. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter Erstellen einer IAM-Rolle (anstatt eines Benutzers) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Für die Zugriffssteuerung in AWS erstellen Sie Richtlinien und weisen diese den AWS-Identitäten oder -Ressourcen zu. Eine Richtlinie ist ein Objekt in AWS, das, wenn es einer Identität oder Ressource zugeordnet wird, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anforderung stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Benutzerinformationen über die AWS Management Console, die AWS CLI oder die AWS -API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem AWS-Konto anfügen können. Verwaltete Richtlinien umfassen von AWS verwaltete und von Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter Auswahl zwischen verwalteten und eingebundenen Richtlinien im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services umfassen.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können verwaltete AWS-Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3, AWS WAF und Amazon VPC sind Beispiele für Dienste, die ACLs unterstützen. Weitere Informationen“ zu ACLs finden Sie unter Zugriffskontrollliste (ACL) – Übersicht (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger häufig verwendete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- Berechtigungsgrenzen – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Ein ausdrückliches Ablehnen in einer dieser Richtlinien setzt das Zulassen außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.
- Service-Kontrollrichtlinien (SCPs) – SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OE) in AWS Organizations angeben. AWS Organizations ist ein Dienst für die Gruppierung und zentrale Verwaltung mehrerer AWS-Konten Ihres Unternehmens. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. SCPs schränken Berechtigungen für Entitäten in Mitgliedskonten einschließlich des jeweiligen Root-Benutzer des AWS-Kontos ein. Weitere Informationen zu Organisationen und SCPs finden Sie unter Funktionsweise von SCPs im AWS Organizations-Benutzerhandbuch.
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen dazu, wie AWS die Zulässigkeit einer Anforderung ermittelt, wenn mehrere Richtlinientypen beteiligt sind, finden Sie unter Logik für die Richtlinienauswertung im IAM-Benutzerhandbuch.

Featuresweise von AWS Proton mit IAM

Bevor Sie IAM zum Verwalten des Zugriffs auf AWS Proton verwenden, erfahren Sie, welche IAM-Funktionen Sie mit AWS Proton verwenden können.

IAM-Funktionen, die Sie mit AWS Proton verwenden können

IAM-Feature	AWS Proton-Support
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Hauptberechtigungen	Ja
Servicerollen	Ja
Service-verknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie AWS Proton und wie die meisten IAM-Funktionen AWS-Services funktionieren AWS-Services, finden Sie im IAM-Benutzerhandbuch unter Diese Funktionen funktionieren mit IAM.

Identitätsbasierte Richtlinien für AWS Proton

Unterstützt Richtlinien auf Identitätsbasis.	Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für AWS Proton

Beispiele für identitätsbasierte AWS Proton-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS Proton.

Ressourcenbasierte Richtlinien in AWS Proton

Unterstützt ressourcenbasierte Richtlinien	Nein

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services umfassen.

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Prinzipal und die Ressource in unterschiedlichen AWS-Konten befinden, muss ein IAM-Administrator im vertrauenswürdigen Konto auch der Prinzipalentität (Benutzer oder Rolle) die Berechtigung zum Zugriff auf die Ressource

erteilen. Sie erteilen Berechtigungen, indem Sie der juristischen Stelle eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden im IAM-Benutzerhandbuch.

Richtlinienaktionen für AWS Proton

Unterstützt Richtlinienaktionen	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie die zugehörige AWS-API-Operation. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keine passende API-Operation gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der AWS Proton-Aktionen finden Sie unter Von AWS Proton definierte Aktionen in der Service-Autorisierungs-Referenz.

Richtlinienaktionen in AWS Proton verwenden das folgende Präfix vor der Aktion:

```
proton
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "proton:action1",
      "proton:action2"
         ]
```

Sie können auch Platzhalter verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `List` beginnen, einschließlich der folgenden Aktion:

```
"Action": "proton:List*"
```

Beispiele für identitätsbasierte AWS Proton-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS Proton.

Richtlinienressourcen für AWS Proton

Unterstützt Richtlinienressourcen	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein – `Resource`oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Eine Liste der AWS Proton-Ressourcentypen und ihrer ARNs finden Sie unter Von AWS Proton definierte Ressourcen in der Service-Autorisierungs-Referenz. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von AWS Proton definierte Aktionen.

Beispiele für identitätsbasierte AWS Proton-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für AWS Proton.

Richtlinien-Bedingungsschlüssel für AWS Proton

Unterstützt servicespezifische Richtlinienbedingungsschlüssel	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition` block) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren verwenden, z. B. ist gleich oder kleiner als, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen `AND`-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungsschlüssel angeben, wertet AWS die Bedingung mittels einer logischen `OR`-Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungsschlüssel und servicespezifische Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter Globale AWS-Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Eine Liste von AWS Proton-Bedingungsschlüsseln finden Sie unter Bedingungsschlüssel für AWS Proton in der Service-Autorisierungs-Referenz. Informationen dazu, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von AWS Proton definierte Aktionen.

Ein Beispiel für eine condition-key-based Richtlinie zur Beschränkung des Zugriffs auf eine Ressource finden Sie unter. Beispiele für Richtlinien auf der Grundlage von Bedingungsschlüsseln für AWS Proton

Zugriffssteuerungslisten (ACLs) in AWS Proton

Unterstützt ACLs	Nein

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Zugriffskontrolllisten (ACLs) sind Listen von Empfängern, die Sie Ressourcen anfügen können. Sie erteilen Konten Berechtigungen für den Zugriff auf die Ressource, auf die sie sich beziehen.

Attributbasierte Zugriffskontrolle (Attribute-Based Access Control, ABAC) mit AWS Proton

Unterstützt ABAC (Tags in Richtlinien)	Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und mehrere AWS-Ressourcen anfügen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie Tag-Informationen an, indem Sie die Schlüssel `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*, oder `aws:TagKeys`Bedingung verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter Was ist ABAC? im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Weitere Informationen über das Markieren von AWS Proton-Ressourcen mit Tags finden Sie unter AWS ProtonRessourcen und Tagging.

Temporäre Anmeldeinformationen verwenden mit AWS Proton

Unterstützt temporäre Anmeldeinformationen	Ja

Einige AWS-Services Featureieren nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, darunter welche AWS-Services mit temporären Anmeldeinformationen Featureieren, finden Sie unter AWS-Services, die mit IAM Featureieren im IAM-Benutzerhandbuch.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen Methode als einem Benutzernamen und einem Passwort bei der AWS Management Console anmelden. Wenn Sie beispielsweise über den Single Sign-On (SSO)-Link Ihres Unternehmens auf AWS zugreifen, erstellt dieser Prozess automatisch temporäre Anmeldeinformationen. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter Wechseln zu einer Rolle (Konsole) im IAM-Benutzerhandbuch.

Sie können mithilfe der AWS CLI- oder AWS-API manuell temporäre Anmeldeinformationen erstellen. Sie können dann diese temporären Anmeldeinformationen verwenden, um auf AWS zuzugreifen. AWS empfiehlt, dass Sie temporäre Anmeldeinformationen dynamisch generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Serviceübergreifende Prinzipal-Berechtigungen für AWS Proton

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anforderungen werden nur dann gestellt, wenn ein

Dienst eine Anforderung erhält, die Interaktionen mit anderen AWS-Services oder Ressourcen erfordert, um abgeschlossen werden zu können. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.

Servicerollen für AWS Proton

Unterstützt Servicerollen	Ja

Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

Weitere Informationen finden Sie unter AWS ProtonBeispiele für Richtlinien für IAM-Dienstrollen.

> **Warning**
>
> Die Änderung der Berechtigungen für eine Servicerolle kann die Funktionalität von AWS Proton beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn AWS Proton eine Anleitung dazu gibt.

Serviceverknüpfte Rollen für AWS Proton

Unterstützt serviceverknüpfte Rollen	Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverbundene Rollen anzeigen, aber nicht bearbeiten.

Einzelheiten zum Erstellen oder Verwalten von dienstbezogenen Rollen finden Sie unter AWS-ServicesDiese Rollen funktionieren mit IAM. Suchen Sie in der Tabelle nach einem Service mit einem

`Yes` in der Spalte Service-linked role (Serviceverknüpfte Rolle). Wählen Sie den Link Yes (Ja) aus, um die Dokumentation für die serviceverknüpfte Rolle für diesen Service anzuzeigen.

Richtlinienbeispiele für AWS Proton

In den folgenden Abschnitten finden Sie Beispiele für AWS Proton IAM-Richtlinien.

Themen

Beispiele für identitätsbasierte Richtlinien für AWS Proton

Benutzer und Rollen haben standardmäßig nicht die Berechtigung, AWS Proton-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben über die AWS Management Console, die AWS Command Line Interface (AWS CLI) oder die AWS-API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Einzelheiten zu den von AWS Proton definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Proton in der Service-Autorisierungs-Referenz.

Themen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand AWS Proton-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-

Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS-verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen – Um Ihren Benutzern und Workloads Berechtigungen zu gewähren, verwenden Sie die AWS-verwaltete Richtlinien die Berechtigungen für viele allgemeine Anwendungsfälle gewähren. Sie sind in Ihrem AWS-Konto verfügbar. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie AWS-kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS-verwaltete Richtlinien oder AWS-verwaltete Richtlinien für Auftragsfunktionen im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Service-Aktionen zu gewähren, wenn diese durch ein bestimmtes AWS-Service, wie beispielsweise AWS CloudFormation, verwendet werden. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Bedarf einer Multi-Faktor-Authentifizierung (MFA) – Wenn Sie ein Szenario haben, das IAM-Benutzer oder Root-Benutzer in Ihrem AWS-Konto erfordert, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien

MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Links zu Beispielen für identitätsbasierte Richtlinien für AWS Proton

Links zu beispielhaften Beispielen für identitätsbasierte Richtlinien für AWS Proton

- Von AWS verwaltete Richtlinien für AWS Proton
- AWS ProtonBeispiele für Richtlinien für IAM-Dienstrollen
- Beispiele für Richtlinien auf der Grundlage von Bedingungsschlüsseln für AWS Proton

AWS ProtonBeispiele für Richtlinien für IAM-Dienstrollen

Administratoren besitzen und verwalten die Ressourcen, die AWS Proton erstellt werden, wie in der Umgebung und den Dienstvorlagen definiert. Sie ordnen ihrem Konto IAM-Servicerollen zu, die es ihnen ermöglichen, Ressourcen in ihrem Namen AWS Proton zu erstellen. Administratoren stellen die IAM-Rollen und AWS Key Management Service Schlüssel für Ressourcen bereit, die später den Entwicklern gehören und von diesen verwaltet werden, wenn AWS Proton sie ihre Anwendung als AWS Proton Dienst in einer Umgebung bereitstellen. AWS Proton Weitere Informationen AWS KMS zur Datenverschlüsselung finden Sie unter. Datenschutz in AWS Proton

Eine Servicerolle ist eine Amazon Web Services (IAM) -Rolle, mit der AWS Proton Sie Ressourcen in Ihrem Namen aufrufen können. Wenn Sie eine Service-Rolle festlegen, verwendet AWS Proton die Anmeldeinformationen der Rolle. Verwenden Sie eine Servicerolle, um explizit anzugeben, welche Aktionen ausgeführt AWS Proton werden können.

Sie erstellen die Service-Rolle und die Berechtigungsrichtlinie mit dem IAM-Service. Weitere Informationen zum Erstellen einer Servicerolle finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

AWS ProtonServicerolle für die Bereitstellung mit AWS CloudFormation

Als Mitglied des Plattformteams können Sie als Administrator eine AWS Proton Servicerolle erstellen und sie bei der Erstellung einer Umgebung als CloudFormation Servicerolle der Umgebung bereitstellen (der `protonServiceRoleArn` Parameter der CreateEnvironmentAPI-Aktion). AWS Proton Mit dieser Rolle können AWS Proton Sie in Ihrem Namen API-Aufrufe an andere Dienste

tätigen, wenn die Umgebung oder eine der darin ausgeführten Dienstinstanzen AWS verwaltetes Provisioning verwenden und AWS CloudFormation die Infrastruktur bereitstellen.

Wir empfehlen Ihnen, die folgende IAM-Rollen- und Vertrauensrichtlinie für Ihre AWS Proton Servicerolle zu verwenden. Wenn Sie die AWS Proton Konsole verwenden, um eine Umgebung zu erstellen, und sich dafür entscheiden, eine neue Rolle zu erstellen, ist dies die Richtlinie, die zu der für Sie erstellten Servicerolle AWS Proton hinzugefügt wird. Wenn Sie den Umfang der Berechtigungen für diese Richtlinie einschränken, sollten Sie bedenken, dass sie bei Fehlern AWS Proton fehlschlägt. `Access Denied`

> **Important**
>
> Beachten Sie, dass die in den folgenden Beispielen gezeigten Richtlinien jedem, der eine Vorlage für Ihr Konto registrieren kann, Administratorrechte gewähren. Da wir nicht wissen, welche Ressourcen Sie in Ihren AWS Proton Vorlagen definieren werden, verfügen diese Richtlinien über umfassende Zugriffsrechte. Wir empfehlen, dass Sie die Berechtigungen auf die spezifischen Ressourcen beschränken, die in Ihren Umgebungen bereitgestellt werden.

AWS ProtonBeispiel für eine Servicerollenrichtlinie für AWS CloudFormation

Ersetzen Sie *123456789012* mit Ihrer AWS-Konto-ID.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CancelUpdateStack",
        "cloudformation:ContinueUpdateRollback",
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DescribeStacks",
        "cloudformation:DetectStackResourceDrift",
```

```
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:ListStackResources",
        "cloudformation:UpdateStack"
      ],
      "Resource": "arn:aws:cloudformation:*:123456789012:stack/AWSProton-*"
    },
    {
      "Effect": "Allow",
      "NotAction": [
        "organizations:*",
        "account:*"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "account:ListRegions"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

AWS ProtonVertrauensrichtlinie für Dienste

```
{
```

```
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ServiceTrustRelationshipWithConfusedDeputyPrevention",
    "Effect": "Allow",
    "Principal": {
      "Service": "proton.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      },
      "ArnLike": {
        "aws:SourceArn": "arn:aws::proton:*:123456789012:environment/*"
      }
    }
  }
}
```

Rollenrichtlinie für AWS verwaltete Bereitstellungsdienste mit eingeschränktem Geltungsbereich

Im Folgenden finden Sie ein Beispiel für eine AWS Proton Servicerollenrichtlinie mit eingeschränktem Geltungsbereich, die Sie verwenden können, wenn Sie Dienste nur für die Bereitstellung von S3-Ressourcen benötigenAWS Proton.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CancelUpdateStack",
        "cloudformation:ContinueUpdateRollback",
        "cloudformation:CreateChangeSet",
        "cloudformation:CreateStack",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:DescribeStackDriftDetectionStatus",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DescribeStacks",
        "cloudformation:DetectStackResourceDrift",
```

```
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:ListStackResources",
        "cloudformation:UpdateStack"
      ],
      "Resource": "arn:aws:cloudformation:*:123456789012:stack/AWSProton-*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:*"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": [
            "cloudformation.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

AWS ProtonServicerolle für die Bereitstellung CodeBuild

Als Mitglied des Plattformteams können Sie als Administrator eine AWS Proton Servicerolle erstellen und sie bei der Erstellung einer Umgebung als CodeBuild Servicerolle der Umgebung bereitstellen (der `codebuildRoleArn` Parameter der CreateEnvironmentAPI-Aktion). AWS Proton Diese Rolle ermöglicht esAWS Proton, API-Aufrufe an andere Dienste in Ihrem Namen zu tätigen, wenn die Umgebung oder eine der darin ausgeführten Dienstinstanzen CodeBuild Provisioning zur Bereitstellung der Infrastruktur verwenden.

Wenn Sie die AWS Proton Konsole verwenden, um eine Umgebung zu erstellen, und sich dafür entscheiden, eine neue Rolle zu erstellen, AWS Proton fügt der für Sie erstellten Servicerolle eine Richtlinie mit Administratorrechten hinzu. Wenn Sie Ihre eigene Rolle erstellen und den Umfang der Berechtigungen einschränken, sollten Sie bedenken, dass AWS Proton dies bei `Access Denied` Fehlern fehlschlägt.

> **Important**
>
> Beachten Sie, dass die Richtlinien, die AWS Proton an die Rollen angehängt werden, die das Programm für Sie erstellt, jedem, der eine Vorlage für Ihr Konto registrieren kann, Administratorrechte gewähren. Da wir nicht wissen, welche Ressourcen Sie in Ihren AWS Proton Vorlagen definieren werden, verfügen diese Richtlinien über umfassende Zugriffsrechte. Wir empfehlen, dass Sie die Berechtigungen auf die spezifischen Ressourcen beschränken, die in Ihren Umgebungen bereitgestellt werden.

AWS ProtonBeispiel für eine Servicerollenrichtlinie für CodeBuild

Das folgende Beispiel bietet Berechtigungen für CodeBuild die Bereitstellung von Ressourcen mithilfe vonAWS Cloud Development Kit (AWS CDK).

Ersetzen Sie *123456789012* mit Ihrer AWS-Konto-ID.

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
     "Action": [
       "logs:CreateLogStream",
       "logs:CreateLogGroup",
       "logs:PutLogEvents"
     ],
     "Resource": [
       "arn:aws:logs:us-east-1:123456789012:log-group:/aws/codebuild/AWSProton-
Shell-*",
       "arn:aws:logs:us-east-1:123456789012:log-group:/aws/codebuild/AWSProton-
Shell-*:*"
     ],
     "Effect": "Allow"
   },
   {
     "Action": "proton:NotifyResourceDeploymentStatusChange",
     "Resource": "arn:aws:proton:us-east-1:123456789012:*",
     "Effect": "Allow"
   },
   {
     "Action": "sts:AssumeRole",
     "Resource": [
```

```
        "arn:aws:iam::123456789012:role/cdk-*-deploy-role-*",
        "arn:aws:iam::123456789012:role/cdk-*-file-publishing-role-*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

AWS Proton CodeBuild Vertrauensrichtlinie

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "CodeBuildTrustRelationshipWithConfusedDeputyPrevention",
    "Effect": "Allow",
    "Principal": {
      "Service": "codebuild.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      },
      "ArnLike": {
        "aws:SourceArn": "arn:aws::proton:*:123456789012:environment/*"
      }
    }
  }
}
```

AWS ProtonRollen im Pipeline-Dienst

Für die Bereitstellung von Service-Pipelines sind AWS Proton Berechtigungen erforderlich, um API-Aufrufe an andere Dienste zu tätigen. Die erforderlichen Servicerollen ähneln den Servicerollen, die Sie beim Erstellen von Umgebungen angeben. Die Rollen zum Erstellen von Pipelines werden jedoch von allen Diensten in Ihrem AWS Konto gemeinsam genutzt, und Sie geben diese Rollen als Kontoeinstellungen in der Konsole oder über die UpdateAccountSettingsAPI-Aktion an.

Wenn Sie die AWS Proton Konsole verwenden, um die Kontoeinstellungen zu aktualisieren und sich dafür entscheiden, eine neue Rolle für die AWS CloudFormation oder die CodeBuild Dienstrollen zu erstellen, entsprechen die Richtlinien, die zu den für Sie erstellten Servicerollen AWS Proton hinzugefügt werden, den Richtlinien, die in den vorherigen Abschnitten beschrieben wurden, AWS-

verwaltete Bereitstellungsrolle undCodeBuild Rolle bei der Bereitstellung. Wenn Sie den Umfang der Berechtigungen für diese Richtlinie einschränken, sollten Sie bedenken, dass diese bei Fehlern AWS Proton fehlschlägt. `Access Denied`

> **Important**
>
> Beachten Sie, dass die Beispielrichtlinien in den vorherigen Abschnitten jedem, der eine Vorlage für Ihr Konto registrieren kann, Administratorrechte gewähren. Da wir nicht wissen, welche Ressourcen Sie in Ihren AWS Proton Vorlagen definieren werden, verfügen diese Richtlinien über umfassende Zugriffsrechte. Wir empfehlen, dass Sie die Berechtigungen auf die spezifischen Ressourcen beschränken, die in Ihren Pipelines bereitgestellt werden.

AWS ProtonRolle der Komponente

Als Mitglied des Plattformteams können Sie als Administrator eine AWS Proton Servicerolle erstellen und sie bei der Erstellung einer Umgebung als CloudFormation Komponentenrolle der Umgebung bereitstellen (der `componentRoleArn` Parameter der CreateEnvironmentAPI-Aktion). AWS Proton Diese Rolle umfasst die Infrastruktur, die direkt definierte Komponenten bereitstellen können. Weitere Informationen zu Komponenten finden Sie unterKomponenten.

Die folgende Beispielrichtlinie unterstützt die Erstellung einer direkt definierten Komponente, die einen Amazon Simple Storage Service (Amazon S3) -Bucket und eine zugehörige Zugriffsrichtlinie bereitstellt.

AWS ProtonBeispiel für eine Rollenrichtlinie für eine Komponente

Ersetzen Sie *123456789012* mit Ihrer AWS-Konto-ID.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CancelUpdateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DescribeStacks",
        "cloudformation:ContinueUpdateRollback",
        "cloudformation:DetectStackResourceDrift",
```

```
        "cloudformation:DescribeStackResourceDrifts",
        "cloudformation:DescribeStackEvents",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListChangeSets",
        "cloudformation:ListStackResources"
      ],
      "Resource": "arn:aws:cloudformation:*:123456789012:stack/AWSProton-*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:GetBucket",
        "iam:CreatePolicy",
        "iam:DeletePolicy",
        "iam:GetPolicy",
        "iam:ListPolicyVersions",
        "iam:DeletePolicyVersion"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": "cloudformation.amazonaws.com"
        }
      }
    }
  ]
}
```

AWS ProtonVertrauensrichtlinie für Komponenten

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ServiceTrustRelationshipWithConfusedDeputyPrevention",
    "Effect": "Allow",
    "Principal": {
      "Service": "proton.amazonaws.com"
```

```
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      },
      "ArnLike": {
        "aws:SourceArn": "arn:aws::proton:*:123456789012:environment/*"
      }
    }
  }
}
```

Beispiele für Richtlinien auf der Grundlage von Bedingungsschlüsseln für AWS Proton

Das folgende Beispiel für eine IAM-Richtlinie verweigert den Zugriff auf AWS Proton Aktionen, die den im Block angegebenen Vorlagen entsprechen. `Condition` Beachten Sie, dass diese Bedingungsschlüssel nur von den Aktionen unterstützt werden, die unter Aktionen, Ressourcen und Bedingungsschlüssel für aufgeführt sind. AWS Proton Um Berechtigungen für andere Aktionen zu verwalten, müssen Sie z. `DeleteEnvironmentTemplate` B. die Zugriffskontrolle auf Ressourcenebene verwenden.

Beispielrichtlinie, die AWS Proton Vorlagenaktionen für eine bestimmte Vorlage verweigert:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": ["proton:*"],
            "Resource": "*",
            "Condition": {
                "StringEqualsIfExists": {
                    "proton:EnvironmentTemplate":
 ["arn:aws:proton:region_id:123456789012:environment-template/my-environment-template"]
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": ["proton:*"],
            "Resource": "*",
```

```
            "Condition": {
                "StringEqualsIfExists": {
                    "proton:ServiceTemplate":
 ["arn:aws:proton:region_id:123456789012:service-template/my-service-template"]
                }
            }
        }
    ]
}
```

In der nächsten Beispielrichtlinie verweigert die erste Anweisung auf Ressourcenebene den Zugriff auf AWS Proton Vorlagenaktionen`ListServiceTemplates`, die nicht mit der im Block aufgeführten Dienstvorlage übereinstimmen. `Resource` Die zweite Anweisung verweigert den Zugriff auf AWS Proton Aktionen, die der im Block aufgeführten Vorlage entsprechen. `Condition`

Beispielrichtlinie, die AWS Proton Aktionen verweigert, die einer bestimmten Vorlage entsprechen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "proton:*"
            ],
            "Resource": "arn:aws:region_id:123456789012:service-template/my-service-
template"
        },
        {
            "Effect": "Deny",
            "Action": [
                "proton:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringEqualsIfExists": {
                    "proton:ServiceTemplate": [
                        "arn:aws:proton:region_id:123456789012:service-template/my-
service-template"
                    ]
                }
            }
        }
```

```
    ]
}
```

Das letzte Richtlinienbeispiel erlaubt AWS Proton Entwickleraktionen, die der spezifischen Dienstvorlage entsprechen, die im `Condition` Block aufgeführt ist.

Beispielrichtlinie, um AWS Proton Entwickleraktionen zuzulassen, die einer bestimmten Vorlage entsprechen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "proton:ListServiceTemplates",
                "proton:ListServiceTemplateVersions",
                "proton:ListServices",
                "proton:ListServiceInstances",
                "proton:ListEnvironments",
                "proton:GetServiceTemplate",
                "proton:GetServiceTemplateVersion",
                "proton:GetService",
                "proton:GetServiceInstance",
                "proton:GetEnvironment",
                "proton:CreateService",
                "proton:UpdateService",
                "proton:UpdateServiceInstance",
                "proton:UpdateServicePipeline",
                "proton:DeleteService",
                "codestar-connections:ListConnections"
            ],
            "Resource": "*",
            "Condition": {
                "StringEqualsIfExists": {
                    "proton:ServiceTemplate":
 "arn:aws:proton:region_id:123456789012:service-template/my-service-template"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "codestar-connections:PassConnection"
            ],
            "Resource": "arn:aws:codestar-connections:*:*:connection/*",
            "Condition": {
                "StringEquals": {
                    "codestar-connections:PassedToService": "proton.amazonaws.com"
                }
            }
        }

    ]
}
```

Von AWS verwaltete Richtlinien für AWS Proton

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, von AWS verwaltete Richtlinien zu verwenden, als selbst Richtlinien zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere von AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS-Konto verfügbar. Weitere Informationen zu verwalteten AWS-Richtlinien finden Sie unter Verwaltete AWS-Richtlinien im IAM-Leitfaden.

AWS-Services pflegen und aktualisieren AWS-verwaltete Richtlinien. Die Berechtigungen in von AWS verwalteten Richtlinien können nicht geändert werden. Services fügen einer von AWS verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Services entfernen keine Berechtigungen aus einer von AWS verwalteten Richtlinie, so dass Richtlinien-Aktualisierungen Ihre vorhandenen Berechtigungen nicht beeinträchtigen.

Darüber hinaus unterstützt AWS verwaltete Richtlinien für Auftragsfunktionen, die mehrere Services umfassen. So bietet die AWS-verwaltete Richtlinie ReadOnlyAccess beispielsweise einen schreibgeschützten Zugriff auf alle AWS-Services und Ressourcen. Wenn ein Service ein neues Feature startet, fügt AWS schreibgeschützte Berechtigungen für neue Vorgänge und Ressourcen hinzu. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS-Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

AWS Protonbietet verwaltete IAM-Richtlinien und Vertrauensstellungen, die Sie Benutzern, Gruppen oder Rollen zuordnen können, sodass Sie Ressourcen und API-Operationen unterschiedlich steuern können. Sie können diese Richtlinien direkt anwenden oder als Ausgangspunkt nutzen, um eigene Richtlinien zu erstellen.

Die folgende Vertrauensstellung wird für jede der AWS Proton verwalteten Richtlinien verwendet.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ExampleTrustRelationshipWithProtonConfusedDeputyPrevention",
    "Effect": "Allow",
    "Principal": {
      "Service": "proton.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      },
      "ArnLike": {
        "aws:SourceArn": "arn:aws::proton:*:123456789012:environment/*"
      }
    }
  }
}
```

AWS verwaltete Richtlinie: AWSProtonFullAccess

Sie können eine Verbindung AWSProtonFullAccess zu Ihren IAM-Entitäten herstellen. AWS Protonordnet diese Richtlinie auch einer Servicerolle zu, mit der Sie Aktionen AWS Proton in Ihrem Namen ausführen können.

Diese Richtlinie gewährt Administratorberechtigungen, die vollen Zugriff auf AWS Proton Aktionen und eingeschränkten Zugriff auf andere AWS Dienstaktionen ermöglichen, AWS Proton abhängig von.

Die Richtlinie umfasst die folgenden Namespaces für wichtige Aktionen:

- `proton`— Ermöglicht Administratoren vollen Zugriff auf APIs. AWS Proton

- `iam`— Ermöglicht Administratoren die Übergabe von Rollen anAWS Proton. Dies ist erforderlich, AWS Proton damit im Namen des Administrators API-Aufrufe an andere Dienste getätigt werden können.
- `kms`— Ermöglicht Administratoren, einem vom Kunden verwalteten Schlüssel einen Zuschuss hinzuzufügen.
- `codestar-connections`— Ermöglicht Administratoren, Codestar-Verbindungen aufzulisten und weiterzugeben, sodass sie von verwendet werden können. AWS Proton

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "proton:*",
        "kms:ListAliases",
        "kms:DescribeKey",
        "codestar-connections:ListConnections"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "proton.*.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
```

```
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "proton.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/sync.proton.amazonaws.com/
AWSServiceRoleForProtonSync",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "sync.proton.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "codestar-connections:PassConnection"
      ],
      "Resource": "arn:aws:codestar-connections:*:*:connection/*",
      "Condition": {
        "StringEquals": {
          "codestar-connections:PassedToService": "proton.amazonaws.com"
        }
      }
    }
  ]
}
```

AWS verwaltete Richtlinie: AWSProtonDeveloperAccess

Sie können sie an Ihre AWSProtonDeveloperAccess IAM-Entitäten anhängen. AWS Protonordnet diese Richtlinie auch einer Servicerolle zu, mit der Sie Aktionen AWS Proton in Ihrem Namen ausführen können.

Diese Richtlinie gewährt Berechtigungen, die eingeschränkten Zugriff auf AWS Proton Aktionen und andere AWS Aktionen ermöglichen, die AWS Proton davon abhängen. Der Umfang dieser

Berechtigungen ist darauf ausgelegt, die Rolle eines Entwicklers zu unterstützen, der AWS Proton Dienste entwickelt und bereitstellt.

Diese Richtlinie gewährt keinen Zugriff auf APIs zum Erstellen, Löschen und Aktualisieren von AWS Proton Vorlagen und Umgebungen. Wenn Entwickler noch eingeschränktere Berechtigungen benötigen, als diese Richtlinie vorsieht, empfehlen wir, eine benutzerdefinierte Richtlinie zu erstellen, die so begrenzt ist, dass sie nur die geringsten Rechte gewährt.

Die Richtlinie umfasst die folgenden Namespaces für wichtige Aktionen:

- `proton`— Ermöglicht Mitwirkenden den Zugriff auf eine begrenzte Anzahl von APIs. AWS Proton
- `codestar-connections`— Erlaubt Mitwirkenden, Codestar-Verbindungen aufzulisten und weiterzugeben, damit sie von verwendet werden können. AWS Proton

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "codecommit:ListRepositories",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineExecution",
        "codepipeline:GetPipelineState",
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codestar-connections:ListConnections",
        "codestar-connections:UseConnection",
        "proton:CancelServiceInstanceDeployment",
        "proton:CancelServicePipelineDeployment",
        "proton:CreateService",
        "proton:DeleteService",
        "proton:GetAccountRoles",
        "proton:GetAccountSettings",
        "proton:GetEnvironment",
        "proton:GetEnvironmentAccountConnection",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateMajorVersion",
```

```
        "proton:GetEnvironmentTemplateMinorVersion",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetRepository",
        "proton:GetRepositorySyncStatus",
        "proton:GetResourcesSummary",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateMajorVersion",
        "proton:GetServiceTemplateMinorVersion",
        "proton:GetServiceTemplateVersion",
        "proton:GetTemplateSyncConfig",
        "proton:GetTemplateSyncStatus",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentOutputs",
        "proton:ListEnvironmentProvisionedResources",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplateMajorVersions",
        "proton:ListEnvironmentTemplateMinorVersions",
        "proton:ListEnvironmentTemplates",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListRepositories",
        "proton:ListRepositorySyncDefinitions",
        "proton:ListServiceInstanceOutputs",
        "proton:ListServiceInstanceProvisionedResources",
        "proton:ListServiceInstances",
        "proton:ListServicePipelineOutputs",
        "proton:ListServicePipelineProvisionedResources",
        "proton:ListServices",
        "proton:ListServiceTemplateMajorVersions",
        "proton:ListServiceTemplateMinorVersions",
        "proton:ListServiceTemplates",
        "proton:ListServiceTemplateVersions",
        "proton:ListTagsForResource",
        "proton:UpdateService",
        "proton:UpdateServiceInstance",
        "proton:UpdateServicePipeline",
        "s3:ListAllMyBuckets",
        "s3:ListBucket"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
```

```
      "Action": "codestar-connections:PassConnection",
      "Resource": "arn:aws:codestar-connections:*:*:connection/*",
      "Condition": {
        "StringEquals": {
          "codestar-connections:PassedToService": "proton.amazonaws.com"
        }
      }
    }
  ]
}
```

AWS verwaltete Richtlinie: AWSProtonReadOnlyAccess

Sie können sie an Ihre AWSProtonReadOnlyAccess IAM-Entitäten anhängen. AWS Protonordnet diese Richtlinie auch einer Servicerolle zu, mit der Sie Aktionen AWS Proton in Ihrem Namen ausführen können.

Diese Richtlinie gewährt Berechtigungen, die nur Lesezugriff auf AWS Proton Aktionen und eingeschränkten Lesezugriff auf andere AWS Dienstaktionen ermöglichen, abhängig von. AWS Proton

Die Richtlinie umfasst die folgenden Namespaces für wichtige Aktionen:

- `proton`— Ermöglicht Mitwirkenden den schreibgeschützten Zugriff auf APIs. AWS Proton

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "codepipeline:ListPipelineExecutions",
        "codepipeline:ListPipelines",
        "codepipeline:GetPipeline",
        "codepipeline:GetPipelineState",
        "codepipeline:GetPipelineExecution",
        "proton:GetAccountRoles",
        "proton:GetAccountSettings",
```

```
        "proton:GetEnvironment",
        "proton:GetEnvironmentAccountConnection",
        "proton:GetEnvironmentTemplate",
        "proton:GetEnvironmentTemplateMajorVersion",
        "proton:GetEnvironmentTemplateMinorVersion",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetRepository",
        "proton:GetRepositorySyncStatus",
        "proton:GetResourcesSummary",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateMajorVersion",
        "proton:GetServiceTemplateMinorVersion",
        "proton:GetServiceTemplateVersion",
        "proton:GetTemplateSyncConfig",
        "proton:GetTemplateSyncStatus",
        "proton:ListEnvironmentAccountConnections",
        "proton:ListEnvironmentOutputs",
        "proton:ListEnvironmentProvisionedResources",
        "proton:ListEnvironments",
        "proton:ListEnvironmentTemplateMajorVersions",
        "proton:ListEnvironmentTemplateMinorVersions",
        "proton:ListEnvironmentTemplates",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListRepositories",
        "proton:ListRepositorySyncDefinitions",
        "proton:ListServiceInstanceOutputs",
        "proton:ListServiceInstanceProvisionedResources",
        "proton:ListServiceInstances",
        "proton:ListServicePipelineOutputs",
        "proton:ListServicePipelineProvisionedResources",
        "proton:ListServices",
        "proton:ListServiceTemplateMajorVersions",
        "proton:ListServiceTemplateMinorVersions",
        "proton:ListServiceTemplates",
        "proton:ListServiceTemplateVersions",
        "proton:ListTagsForResource"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS verwaltete Richtlinie: AWSProtonSyncServiceRolePolicy

AWS Protonfügt diese Richtlinie der AWSServiceRoleForProtonSync dienstbezogenen Rolle hinzu, die die Vorlagensynchronisierung AWS Proton ermöglicht.

Diese Richtlinie gewährt Berechtigungen, die eingeschränkten Zugriff auf AWS Proton Aktionen und andere AWS Dienstaktionen ermöglichen, die davon AWS Proton abhängen.

Die Richtlinie umfasst die folgenden Namespaces für wichtige Aktionen:

- `proton`— Ermöglicht den eingeschränkten AWS Proton Synchronisierungszugriff auf APIs. AWS Proton
- `codestar-connections`— Ermöglicht den eingeschränkten AWS Proton Synchronisierungszugriff auf CodeConnections APIs.

Informationen zu den Berechtigungsdetails für finden Sie AWSProtonSyncServiceRolePolicy unter Dienstbezogene Rollenberechtigungen für AWS Proton.

AWSverwaltete Richtlinie: AWSProtonCodeBuildProvisioningBasicAccess

Permissions CodeBuild muss einen Build für die AWS Proton CodeBuild Bereitstellung ausführen. Sie können es `AWSProtonCodeBuildProvisioningBasicAccess` an Ihre CodeBuild Provisioning-Rolle anhängen.

Diese Richtlinie gewährt die Mindestberechtigungen für das Funktionieren von AWS Proton CodeBuild Provisioning. Sie gewährt Berechtigungen, die das Generieren von CodeBuild Build-Logs ermöglichen. Es gewährt Proton auch die Erlaubnis, Benutzern Infrastructure as Code (IaC) - Ausgaben zur Verfügung zu AWS Proton stellen. Es bietet keine Berechtigungen, die von IaC-Tools zur Verwaltung der Infrastruktur benötigt werden.

Die Richtlinie umfasst die folgenden Namespaces für wichtige Aktionen:

- `logs`- Ermöglicht das Generieren von CodeBuild Build-Logs. Ohne diese Erlaubnis kann der Start nicht ausgeführt CodeBuild werden.
- `proton`- Ermöglicht es einem CodeBuild Provisioning-Befehl, die Aktualisierung der IaaC-Ausgaben für eine bestimmte AWS Proton Ressource aufzurufen`aws proton notify-resource-deployment-status-change`.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "logs:CreateLogStream",
    "logs:CreateLogGroup",
    "logs:PutLogEvents"
   ],
   "Resource": [
    "arn:aws:logs:*:*:log-group:/aws/codebuild/AWSProton-*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": "proton:NotifyResourceDeploymentStatusChange",
   "Resource": "arn:aws:proton:*:*:*"
  }
 ]
}
```

AWSverwaltete Richtlinie: AWSProtonCodeBuildProvisioningServiceRolePolicy

AWS Protonordnet diese Richtlinie der AWSServiceRoleForProtonCodeBuildProvisioning dienstbezogenen Rolle zu, die eine CodeBuild basierte AWS Proton Bereitstellung ermöglicht.

Diese Richtlinie gewährt Berechtigungen, die einen eingeschränkten Zugriff auf AWS Dienstaktionen ermöglichen, AWS Proton abhängig von.

Die Richtlinie umfasst die folgenden Namespaces für wichtige Aktionen:

- `cloudformation`— Ermöglicht die AWS Proton CodeBuild basierte Bereitstellung mit eingeschränktem Zugriff auf APIs. AWS CloudFormation
- `codebuild`— Ermöglicht eingeschränkten Zugriff auf APIs durch AWS Proton CodeBuild basiertes Provisioning. CodeBuild

- `iam`— Ermöglicht Administratoren die Übergabe von Rollen anAWS Proton. Dies ist erforderlich, AWS Proton damit im Namen des Administrators API-Aufrufe an andere Dienste getätigt werden können.
- `servicequotas`— Ermöglicht AWS Proton die Überprüfung des Limits für CodeBuild gleichzeitige Builds, wodurch ein ordnungsgemäßes Build-Queuing gewährleistet wird.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ListStackResources"
      ],
      "Resource": [
        "arn:aws:cloudformation:*:*:stack/AWSProton-CodeBuild-*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:UpdateProject",
        "codebuild:StartBuild",
        "codebuild:StopBuild",
        "codebuild:RetryBuild",
        "codebuild:BatchGetBuilds",
        "codebuild:BatchGetProjects"
      ],
      "Resource": "arn:aws:codebuild:*:*:project/AWSProton*"
```

```
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEqualsIfExists": {
          "iam:PassedToService": "codebuild.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
          "servicequotas:GetServiceQuota"
      ],
      "Resource": "*"
    }
  ]
}
```

AWSverwaltete Richtlinie: Richtlinie AwsProtonServiceGitSyncServiceRole

AWS Protonfügt diese Richtlinie der mit dem AwsProtonServiceGitSyncServiceRole Richtliniendienst verknüpften Rolle hinzu, mit der die Dienstsynchronisierung durchgeführt AWS Proton werden kann.

Diese Richtlinie gewährt Berechtigungen, die eingeschränkten Zugriff auf AWS Proton Aktionen und andere AWS Dienstaktionen ermöglichen, die davon AWS Proton abhängen.

Die Richtlinie umfasst die folgenden Namespaces für wichtige Aktionen:

- `proton`— Ermöglicht AWS Proton Sync eingeschränkten Zugriff auf AWS Proton Proton-APIs.

Informationen zu den Berechtigungsdetails für die AwsProtonServiceGitSyncServiceRole Richtlinie finden Sie unter Servicebezogene Rollenberechtigungen für. AWS Proton

AWS Proton-Aktualisierungen für AWS verwaltete Richtlinien

Anzeigen von Details zu Aktualisierungen für AWS-verwaltete Richtlinien für AWS Proton, seit dieser Dienst mit der Verfolgung dieser Änderungen begonnen hat. Um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Seite AWS Proton-Dokumentverlauf.

Änderung	Beschreibung	Datum
AWSProtonCodeBuildProvisioningServiceRolePolicy – Aktualisierung auf eine bestehende Richtlinie	AWS ProtonDiese Richtlinie wurde aktualisiert und um zusätzliche Berechtigungen erweitert, um sicherzustellen, dass Konten über das Limit für CodeBuild gleichzeitige Builds verfügen, um Provisioning verwenden zu können CodeBuild .	12. Mai 2023
AwsProtonServiceGitSyncServiceRoleRichtlinie — Neue Richtlinie	AWS ProtonEs wurde eine neue Richtlinie hinzugefügt, um die Synchronisierung von Diensten AWS Proton zu ermöglichen. Die Richtlinie wird in der AWSServiceRoleForProtonServiceSyncdienstbezogenen Rolle verwendet.	31. März 2023
AWSProtonDeveloperAccess – Aktualisierung auf eine bestehende Richtlinie	AWS Protonhat eine neue `GetResourcesSummary` Aktion hinzugefügt, mit der Sie eine Zusammenfassung Ihrer Vorlagen, bereitgestellten Vorlagenressourcen und veralteten Ressourcen anzeigen können.	18. November 2022
AWSProtonReadOnlyAccess – Aktualisierung auf eine bestehende Richtlinie	AWS Protonhat eine neue `GetResourcesSummary` Aktion hinzugefügt, mit der Sie eine Zusammenfassung Ihrer Vorlagen, bereitgestellten Vorlagenressourcen	18. November 2022

Änderung	Beschreibung	Datum
	und veralteten Ressourcen anzeigen können.	
AWSProtonCodeBuildProvisioningBasicAccess – Neue Richtlinie.	AWS Protonhat eine neue Richtlinie hinzugefügt, CodeBuild die die zum Ausführen eines Builds für die AWS Proton CodeBuild Bereitstellung erforderlichen Berechtigungen gewährt.	16. November 2022
AWSProtonCodeBuildProvisioningServiceRolePolicy – Neue Richtlinie.	AWS Protonhat eine neue Richtlinie hinzugefügt, die die Durchführung von Vorgängen im Zusammenhang mit der CodeBuild basierten Bereitstellung ermöglich tAWS Proton. Die Richtlini e wird in der AWSServic eRoleForProtonCode BuildProvisioningserviceve rknüpften Rolle verwendet.	02. September 2022
AWSProtonFullAccess – Aktualisierung auf eine bestehende Richtlinie	AWS Protonhat diese Richtlini e aktualisiert, um Zugriff auf neue AWS Proton API-Opera tionen zu gewähren und um Berechtigungsprobleme für einige AWS Proton Konsoleno perationen zu beheben.	30. März 2022

Änderung	Beschreibung	Datum
AWSProtonDeveloperAccess – Aktualisierung auf eine bestehende Richtlinie	AWS ProtonDiese Richtlinie wurde aktualisiert, um Zugriff auf neue AWS Proton API-Operationen zu gewähren und um Probleme mit Zugriffsb erechtigungen für einige AWS Proton Konsolenoperationen zu beheben.	30. März 2022
AWSProtonReadOnlyAccess – Aktualisierung auf eine bestehende Richtlinie	AWS Protonaktualisieren Sie diese Richtlinie, um Zugriff auf neue AWS Proton API-Operationen zu gewähren und um Berechtigungsprobl eme bei einigen AWS Proton Konsolenoperationen zu beheben.	30. März 2022
AWSProtonSyncServi ceRolePolicy – Neue Richtlini e.	AWS Protonhat eine neue Richtlinie hinzugefügt, die die Ausführung von Vorgängen im Zusammenhang mit der Vorlagensynchronisierung ermöglichtAWS Proton. Die Richtlinie wird in der AWSServiceRoleForP rotonSyncserviceverknüpften Rolle verwendet.	23. November 2021
AWSProtonFullAccess – Neue Richtlinie.	AWS Protonhat eine neue Richtlinie hinzugefügt, um Administratorrollen Zugriff auf AWS Proton API-Operationen und die AWS Proton Konsole zu gewähren.	09. Juni 2021

Änderung	Beschreibung	Datum
AWSProtonDeveloperAccess – Neue Richtlinie.	AWS ProtonEs wurde eine neue Richtlinie hinzugefügt, um Entwicklerrollen Zugriff auf AWS Proton API-Operationen und die AWS Proton Konsole zu gewähren.	09. Juni 2021
AWSProtonReadOnlyAccess – Neue Richtlinie.	AWS Protonhat eine neue Richtlinie hinzugefügt, um schreibgeschützten Zugriff auf AWS Proton API-Operationen und die AWS Proton Konsole zu gewähren.	09. Juni 2021
AWS Proton hat die Änderungsverfolgung gestartet .	AWS Proton hat mit der Verfolgung von Änderunge n für seine AWS-verwalteten Richtlinien begonnen.	09. Juni 2021

Verwenden von serviceverknüpften Rollen für AWS Proton

AWS Proton verwendet serviceverknüpfte Rollen von AWS Identity and Access Management (IAM). Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit AWS Proton verknüpft ist. Serviceverknüpfte Rollen werden von AWS Proton vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer AWS-Services in Ihrem Namen erfordert.

Themen

- Rollen für die AWS Proton Synchronisierung verwenden
- Rollen für die basierte Bereitstellung verwenden CodeBuild

Rollen für die AWS Proton Synchronisierung verwenden

AWS Proton verwendet serviceverknüpfte Rollen von AWS Identity and Access Management (IAM). Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit AWS Proton

verknüpft ist. Serviceverknüpfte Rollen werden von AWS Proton vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer AWS-Services in Ihrem Namen erfordert.

Eine serviceverknüpfte Rolle vereinfacht die Einrichtung von AWS Proton, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS Proton definiert die Berechtigungen seiner serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, kann nur AWS Proton die Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dies schützt Ihre AWS Proton-Ressourcen, da Sie nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen entfernen können.

Informationen zu anderen Services, die serviceorientierte Rollen unterstützen, finden Sie unter AWS services that work with IAM (-Services, die mit IAM funktionieren). Suchen Sie nach den Services, für die Yes (Ja) in der Spalte Service-linked roles (Serviceorientierte Rollen) angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Rollen für AWS Proton

AWS Protonverwendet zwei dienstverknüpfte Rollen mit dem Namen AWSServiceRoleForProtonSyncund AWSServiceRoleForProtonServiceSync.

Die AWSServiceRoleForProtonSync dienstverknüpfte Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `sync.proton.amazonaws.com`

Die genannte Rollenberechtigungsrichtlinie AWSProtonSyncServiceRolePolicy ermöglicht esAWS Proton, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktion: AWS ProtonVorlagen und Vorlagenversionen erstellen, verwalten und weiterlesen
- Aktion: Verbindung verwenden am CodeConnections

AWSProtonSyncServiceRolePolicy

Diese Richtlinie umfasst die folgenden Berechtigungen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SyncToProton",
      "Effect": "Allow",
      "Action": [
        "proton:UpdateServiceTemplateVersion",
        "proton:UpdateServiceTemplate",
        "proton:UpdateEnvironmentTemplateVersion",
        "proton:UpdateEnvironmentTemplate",
        "proton:GetServiceTemplateVersion",
        "proton:GetServiceTemplate",
        "proton:GetEnvironmentTemplateVersion",
        "proton:GetEnvironmentTemplate",
        "proton:DeleteServiceTemplateVersion",
        "proton:DeleteEnvironmentTemplateVersion",
        "proton:CreateServiceTemplateVersion",
        "proton:CreateServiceTemplate",
        "proton:CreateEnvironmentTemplateVersion",
        "proton:CreateEnvironmentTemplate",
        "proton:ListEnvironmentTemplateVersions",
        "proton:ListServiceTemplateVersions",
        "proton:CreateEnvironmentTemplateMajorVersion",
        "proton:CreateServiceTemplateMajorVersion"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AccessGitRepos",
      "Effect": "Allow",
      "Action": [
        "codestar-connections:UseConnection"
      ],
      "Resource": "arn:aws:codestar-connections:*:*:connection/*"
    }
  ]
}
```

Informationen zur finden Sie AWSProtonSyncServiceRolePolicy unter AWSverwaltete Richtlinie: AWSProtonSyncServiceRolePolicy.

Die AWSServiceRoleForProtonServiceSync dienstbezogene Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `service-sync.proton.amazonaws.com`

Die genannte Rollenberechtigungsrichtlinie AWSServiceRoleForProtonServiceSync ermöglicht esAWS Proton, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktion: AWS ProtonDienste und Dienstinstanzen erstellen, verwalten und darauf lesen

AwsProtonServiceGitSyncServiceRoleRichtlinie

Diese Richtlinie umfasst die folgenden Berechtigungen:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "ProtonServiceSync",
   "Effect": "Allow",
   "Action": [
    "proton:GetService",
    "proton:UpdateService",
    "proton:UpdateServicePipeline",
    "proton:CreateServiceInstance",
    "proton:GetServiceInstance",
    "proton:UpdateServiceInstance",
    "proton:ListServiceInstances",
    "proton:GetComponent",
    "proton:CreateComponent",
    "proton:ListComponents",
    "proton:UpdateComponent",
    "proton:GetEnvironment",
    "proton:CreateEnvironment",
    "proton:ListEnvironments",
    "proton:UpdateEnvironment"
   ],
   "Resource": "*"
  }
 ]
}
```

Informationen zur finden Sie AwsProtonServiceSyncServiceRolePolicy unter AWSverwaltete Richtlinie: AwsProtonServiceSyncServiceRolePolicy.

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

Erstellen einer serviceverknüpften Rolle für AWS Proton

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie ein Repository oder einen Dienst für die Synchronisierung AWS Proton in derAWS Management Console, der oder der AWS CLI AWS API konfigurieren, AWS Proton erstellt die dienstverknüpfte Rolle für Sie.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie ein Repository oder einen Dienst für die Synchronisierung konfigurierenAWS Proton, AWS Proton erstellt die dienstverknüpfte Rolle erneut für Sie.

Um die AWSServiceRoleForProtonSync dienstverknüpfte Rolle neu zu erstellen, sollten Sie ein Repository für die Synchronisierung konfigurieren, und für die AWSServiceRoleForProtonServiceSync Neuerstellung sollten Sie einen Dienst für die Synchronisierung konfigurieren.

Bearbeiten einer serviceverknüpften Rolle für AWS Proton

AWS Protonerlaubt es Ihnen nicht, die dienstverknüpfte Rolle zu bearbeiten. AWSServiceRoleForProtonSync Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach der Erstellung einer serviceverknüpften Rolle nicht bearbeitet werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für AWS Proton

Sie müssen die AWSServiceRoleForProtonSync Rolle nicht manuell löschen. Wenn Sie alle AWS Proton verknüpften Repositorys für die Repository-Synchronisierung in der AWS Management ConsoleAWS CLI, der oder der AWS API löschen, werden die Ressourcen AWS Proton bereinigt und die mit dem Dienst verknüpfte Rolle für Sie gelöscht.

Unterstützte Regionen für serviceverknüpfte AWS Proton-Rollen

AWS Proton unterstützt die Verwendung von serviceverknüpften Rollen in allen AWS-Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter AWS Proton-Endpunkte und -Kontingente in der Allgemeine AWS-Referenz.

Rollen für die basierte Bereitstellung verwenden CodeBuild

AWS Proton verwendet serviceverknüpfte Rollen von AWS Identity and Access Management (IAM). Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit AWS Proton verknüpft ist. Serviceverknüpfte Rollen werden von AWS Proton vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer AWS-Services in Ihrem Namen erfordert.

Eine serviceverknüpfte Rolle vereinfacht die Einrichtung von AWS Proton, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. AWS Proton definiert die Berechtigungen seiner serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, kann nur AWS Proton die Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dies schützt Ihre AWS Proton-Ressourcen, da Sie nicht versehentlich die Berechtigung für den Zugriff auf die Ressourcen entfernen können.

Informationen zu anderen Services, die serviceorientierte Rollen unterstützen, finden Sie unter AWS services that work with IAM (-Services, die mit IAM funktionieren). Suchen Sie nach den Services, für die Yes (Ja) in der Spalte Service-linked roles (Serviceorientierte Rollen) angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Berechtigungen von serviceverknüpften Rollen für AWS Proton

AWS Protonverwendet die serviceverknüpfte Rolle mit dem Namen AWSServiceRoleForProtonCodeBuildProvisioning— A Service Linked Role für die AWS Proton CodeBuild Bereitstellung.

Die AWSServiceRoleForProtonCodeBuildProvisioning dienstgebundene Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `codebuild.proton.amazonaws.com`

Die genannte Rollenberechtigungsrichtlinie AWSProtonCodeBuildProvisioningServiceRolePolicy ermöglicht esAWS Proton, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktion: AWS CloudFormationStacks und Transformationen erstellen, verwalten und darauf lesen
- Aktion: CodeBuild Projekte und Builds erstellen, verwalten und weiterlesen

AWSProtonCodeBuildProvisioningServiceRolePolicy

Diese Richtlinie umfasst die folgenden Berechtigungen:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation:DeleteChangeSet",
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ListStackResources"
      ],
      "Resource": [
        "arn:aws:cloudformation:*:*:stack/AWSProton-CodeBuild-*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "codebuild:CreateProject",
        "codebuild:DeleteProject",
        "codebuild:UpdateProject",
        "codebuild:StartBuild",
        "codebuild:StopBuild",
        "codebuild:RetryBuild",
        "codebuild:BatchGetBuilds",
        "codebuild:BatchGetProjects"
      ],
      "Resource": "arn:aws:codebuild:*:*:project/AWSProton*"
```

```
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEqualsIfExists": {
          "iam:PassedToService": "codebuild.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
          "servicequotas:GetServiceQuota"
      ],
      "Resource": "*"
    }
  ]
}
```

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

Erstellen einer serviceverknüpften Rolle für AWS Proton

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie eine Umgebung erstellen, die CodeBuild basiertes Provisioning AWS Proton in derAWS Management Console, der oder der AWS API verwendetAWS CLI, AWS Proton wird die serviceverknüpfte Rolle für Sie erstellt.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie eine Umgebung erstellen, in der CodeBuild basiertes Provisioning verwendet AWS Proton wirdAWS Proton, wird die serviceverknüpfte Rolle erneut für Sie erstellt.

Bearbeiten einer serviceverknüpften Rolle für AWS Proton

AWS Protonermöglicht es Ihnen nicht, die AWSServiceRoleForProtonCodeBuildProvisioning serviceverknüpfte Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr

geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für AWS Proton

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpften Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch alle Umgebungen und Dienste (Instanzen und Pipelines) löschen, in denen die CodeBuild basierte Bereitstellung verwendet wird, AWS Proton bevor Sie sie manuell löschen können.

Manuelles Löschen der -serviceverknüpften Rolle

Verwenden Sie die IAM-Konsole, AWS CLI- oder AWS-API, um die AWSServiceRoleForProtonCodeBuildProvisioning serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für serviceverknüpfte AWS Proton-Rollen

AWS Proton unterstützt die Verwendung von serviceverknüpften Rollen in allen AWS-Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter AWS Proton-Endpunkte und -Kontingente in der Allgemeine AWS-Referenz.

Fehlerbehebung für AWS Proton-Identität und -Zugriff

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die beim Arbeiten mit AWS Proton und IAM auftreten könnten.

Themen

- Ich bin nicht autorisiert, eine Aktion in AWS Proton auszuführen.
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine AWS Proton-Ressourcen gewähren

Ich bin nicht autorisiert, eine Aktion in AWS Proton auszuführen.

Wenn die AWS Management Console Ihnen mitteilt, dass Sie nicht zur Ausführung einer Aktion autorisiert sind, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson` IAM-Benutzer versucht, die Konsole zum Anzeigen von Details zu einer fiktiven *`my-example-widget`*-Ressource zu verwenden, jedoch nicht über `proton:`*`GetWidget`*-Berechtigungen verfügt.

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

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

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Durchführen der `iam:PassRole`-Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an AWS Proton übergeben zu können.

Einige AWS-Services erlauben die Übergabe einer vorhandenen Rolle an diesen Dienst, sodass keine neue Servicerolle oder serviceverknüpfte Rolle erstellt werden muss. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in AWS Proton auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

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

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung benötigen. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine AWS Proton-Ressourcen gewähren

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem

die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen dazu, ob AWS Proton diese Funktionen unterstützt, finden Sie unter Featuresweise von AWS Proton mit IAM.
- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen für alle Ihre AWS-Konten finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen Ihrer AWS-Konto im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie AWS-Konten-Drittanbieter Zugriff auf Ihre Ressourcen bereitstellen, finden Sie unter Gewähren des Zugriffs auf AWS-Konten von externen Benutzern im IAM-Benutzerhandbuch.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

Konfigurations- und Schwachstellenanalyse in AWS Proton

AWS Protonstellt keine Patches oder Updates für vom Kunden bereitgestellten Code bereit. Kunden sind dafür verantwortlich, Patches auf ihren eigenen Code zu aktualisieren und anzuwenden, einschließlich des Quellcodes für ihre Dienste und Anwendungen, auf denen ausgeführt wirdAWS Protonund den Code, der in ihren Service- und Umgebungsvorlagenpaketen bereitgestellt wird.

Kunden sind dafür verantwortlich, Infrastrukturressourcen in ihren Umgebungen und Diensten zu aktualisieren und zu patchen.AWS Protonaktualisiert oder patcht keine Ressourcen automatisch. Kunden sollten die Dokumentation zu den Ressourcen in ihrer Architektur konsultieren, um ihre jeweiligen Patch-Richtlinien zu verstehen.

Abgesehen von der Bereitstellung von Kunden angeforderten Umgebungs- und Service-Updates für kleinere Versionen von Service- und Umgebungsvorlagen,AWS Protonstellt keine Patches oder Aktualisierungen der Ressourcen bereit, die Kunden in ihren Service- und Umgebungsvorlagen und Vorlagenpaketen definieren.

Weitere Informationen finden Sie in den folgenden Ressourcen:

- Modell der übergreifenden Verantwortlichkeit
- Amazon Web Services: Übersicht über Sicherheitsprozesse

Datenschutz in AWS Proton

AWS Protonfolgt dem Modell derAWS übergreifenden Verantwortlichkeit und der , das Vorschriften und Richtlinien für den Datenschutz beinhaltet. AWSist verantwortlich für den Schutz der globalen Infrastruktur, die die gesamte ausgeführt wirdAWS-Services. AWShat die Kontrolle über die Daten, die in dieser Infrastruktur gehostet werden. Dies gilt auch für die Steuerelemente zur Sicherheitskonfiguration für den Umgang mit Kundeninhalten und persönlichen Daten. AWSKunden und APN-Partner, die entweder als Daten-Controller oder als Datenverarbeiter agieren, sind verantwortlich für alle personenbezogenen Daten, die sie inAWS Cloud

Zum Zweck des Datenschutzes empfehlen wir, dieAWS-Konto Anmeldeinformationen für das zu schützen und individuelle Benutzerkonten mitAWS Identity and Access Management (IAM) einzurichten, damit jeder Benutzer nur die Berechtigungen besitzt, die er für seine beruflichen Aufgaben benötigt. Außerdem sollten Sie die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Factor Authentication (MFA).
- Verwenden Sie SSL/TLS für die Kommunikation mit AWS-Ressourcen. Wir empfehlen TLS 1.2 oder höher.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail.
- Verwenden Sie AWS-Verschlüsselungslösungen zusammen mit allen Standardsicherheitskontrollen in AWS-Services.

Wir empfehlen dringend, in Freitextfeldern wie z. B. im Feld Name keine sensiblen, identifizierenden Informationen wie Kontonummern von Kunden einzugeben. Dies gilt auch, wenn Sie mitAWS Proton oder auf andereAWS-Services Weise mit der Konsole, der API oder denAWS SDKs arbeiten.AWS CLI Alle Daten, die Sie in Freitextfelder für Ressourcen-IDs oder ähnliche Elemente im Zusammenhang mit der Verwaltung vonAWS Ressourcen eingeben, können in Diagnoseprotokolle aufgenommen werden. Wenn Sie eine URL für einen externen Server bereitstellen, schließen Sie keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL ein.

Weitere Informationen zum Datenschutz enthält der Blog-Beitrag AWS Shared Responsibility Model and GDPR im AWS-Sicherheitsblog.

Serverseitige Verschlüsselung im Ruhezustand

Wenn Sie sich dafür entscheiden, vertrauliche Daten in Ihren Vorlagenpaketen zu verschlüsseln, die im S3-Bucket gespeichert sind, in dem Sie Ihre Vorlagenpakete speichern, müssen Sie einen SSE-S3- oder SSE-KMS-Schlüssel verwenden, um das Abrufen der VorlagenpaketeAWS Proton zu ermöglichen, damit sie an eine registrierteAWS Proton Vorlage angehängt werden können.

Verschlüsselung während der Übertragung

Die gesamte Service-zu-Service-Kommunikation wird während der Übertragung mit SSL/TLS verschlüsselt.

AWS ProtonVerwaltung von Verschlüsselungsschlüsseln

DarinAWS Proton werden alle Kundendaten standardmäßig mit einemAWS Proton eigenen Schlüssel verschlüsselt. Wenn Sie einen kundeneigenen und verwaltetenAWS KMS Schlüssel angeben, werden alle Kundendaten mit dem vom Kunden bereitgestellten Schlüssel verschlüsselt, wie in den folgenden Absätzen beschrieben.

Wenn Sie eineAWS Proton Vorlage erstellen, geben Sie Ihren Schlüssel an undAWS Proton verwenden Ihre Anmeldeinformationen, um einen Zuschuss zu erstellen, der die Verwendung Ihres Schlüssels ermöglichtAWS Proton.

Wenn Sie die Gewährung manuell zurückziehen oder Ihren angegebenen Schlüssel deaktivieren oder löschen, kann er die Daten, die mit dem angegebenen Schlüssel und den Zuschlägen verschlüsselt wurden, nicht lesen`ValidationException`.AWS Proton

AWS Proton-Verschlüsselungskontext

AWS Protonunterstützt Verschlüsselungskontext-Header. Ein Verschlüsselungskontext ist ein optionaler Satz von Schlüssel-Wert-Paaren, die zusätzliche kontextbezogene Informationen zu den Daten enthalten können. Allgemeine Informationen zum Verschlüsselungs-Kontext finden Sie unter AWS Key Management Service Concepts – Encryption Context (Konzepte – Verschlüsselungs-Kontext) im AWS Key Management Service-Entwicklerhandbuch.

Ein Verschlüsselungskontext ist ein Satz von Schlüssel-Wert-Paaren, die beliebige nicht geheime Daten enthalten können. Wenn Sie einen Verschlüsselungskontext in eine Anforderung

zur Verschlüsselung von Daten aufnehmen, bindet den VerschlüsselungskontextAWS KMS kryptografisch an die verschlüsselten Daten. Zur Entschlüsselung der Daten müssen Sie denselben Verschlüsselungskontext übergeben.

Kunden können anhand des Verschlüsselungskontexts die Verwendung ihres kundenverwalteten Schlüssels in Prüfungs-Datensätzen und -Protokollen identifizieren. Außerdem wird er als Klartext in Protokolle wieAWS CloudTrail und Amazon CloudWatch Logs aufgenommen.

AWS Protonverwendet keinen kundenspezifischen oder extern spezifizierten Verschlüsselungskontext.

AWS Protonfügt den folgenden Verschlüsselungskontext hinzu.

```
{
  "aws:proton:template": "<proton-template-arn>",
  "aws:proton:resource": "<proton-resource-arn>"
}
```

Der erste Verschlüsselungskontext identifiziert dieAWS Proton Vorlage, der die Ressource zugeordnet ist, und dient auch als Einschränkung für vom Kunden verwaltete Schlüsselberechtigungen und -ermächtigungen.

Der zweite Verschlüsselungskontext identifiziert die verschlüsselteAWS Proton Ressource.

Die folgenden Beispiele zeigen die Verwendung desAWS Proton Verschlüsselungskontextes.

Entwickler, der eine Dienstinstanz erstellt.

```
{
  "aws:proton:template": "arn:aws:proton:region_id:123456789012:service-template/my-
template",
  "aws:proton:resource": "arn:aws:proton:region_id:123456789012:service/my-service/
service-instance/my-service-instance"
}
```

Ein Administrator, der eine Vorlage erstellt.

```
{
  "aws:proton:template": "arn:aws:proton:region_id:123456789012:service-template/my-
template",
```

```
  "aws:proton:resource": "arn:aws:proton:region_id:123456789012:service-template/my-
template"
}
```

Infrastruktursicherheit in AWS Proton

Als verwalteter Service AWS Proton ist durch die AWS globale Netzwerksicherheit von geschützt. Informationen zu AWS Sicherheitsservices und wie die Infrastruktur AWS schützt, finden Sie unter AWS Cloud-Sicherheit. Informationen zum Entwerfen Ihrer AWS Umgebung mit den bewährten Methoden für die Infrastruktursicherheit finden Sie unter Infrastrukturschutz in Security Pillar AWS Well-Architected Framework.

Sie verwenden durch AWS veröffentlichte API-Aufrufe, um AWS Proton über das Netzwerk auf zuzugreifen. Kunden müssen Folgendes unterstützen:

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

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

Um die Netzwerkisolierung zu verbessern, können Sie AWS PrivateLink wie im folgenden Abschnitt beschrieben verwenden.

AWS Proton und Schnittstellen-VPC-Endpunkte (AWS PrivateLink)

Sie können eine private Verbindung zwischen Ihrer VPC und herstellen, AWS Proton indem Sie einen Schnittstellen-VPC-Endpunkt erstellen. Schnittstellenendpunkte werden von unterstütztAWS PrivateLink, einer Technologie, die es Ihnen ermöglicht, ohne Internet-Gateway, NAT-Gerät, VPN-Verbindung oder - AWS Direct Connect Verbindung privat auf AWS Proton APIs zuzugreifen. Instances in Ihrer VPC benötigen für die Kommunikation mit AWS Proton APIs keine öffentlichen IP-Adressen. Der Datenverkehr zwischen Ihrer VPC und verlässt das Amazon-Netzwerk AWS Proton nicht.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere Elastic-Network-Schnittstellen in Ihren Subnetzen dargestellt.

Weitere Informationen finden Sie unter Schnittstellen-VPC-Endpunkte (AWS PrivateLink) im Amazon-VPC-Benutzerhandbuch.

Überlegungen zu AWS Proton VPC-Endpunkten

Bevor Sie einen Schnittstellen-VPC-Endpunkt für einrichten AWS Proton, lesen Sie die Eigenschaften und Einschränkungen von Schnittstellenendpunkten im Amazon-VPC-Benutzerhandbuch.

AWS Proton unterstützt Aufrufe aller API-Aktionen von Ihrer VPC aus.

VPC-Endpunktrichtlinien werden für unterstützt AWS Proton. Standardmäßig AWS Proton ist der vollständige Zugriff auf über den Endpunkt erlaubt. Weitere Informationen finden Sie unter Steuerung des Zugriffs auf Services mit VPC-Endpunkten im Amazon-VPC-Benutzerhandbuch.

Erstellen eines Schnittstellen-VPC-Endpunkts für AWS Proton

Sie können einen VPC-Endpunkt für den AWS Proton Service entweder über die Amazon-VPC-Konsole oder die AWS Command Line Interface (AWS CLI) erstellen. Weitere Informationen finden Sie unter Erstellung eines Schnittstellenendpunkts im Benutzerhandbuch für Amazon VPC.

Erstellen Sie einen VPC-Endpunkt für AWS Proton unter Verwendung des folgenden Servicenamens:

- com.amazonaws.*region*.proton

Wenn Sie privates DNS für den Endpunkt aktivieren, können Sie API-Anforderungen an AWS Proton unter Verwendung seines standardmäßigen DNS-Namens für die Region senden, z. B. `proton.`*region*`.amazonaws.com`.

Weitere Informationen finden Sie unter Zugriff auf einen Service über einen Schnittstellenendpunkt im Benutzerhandbuch für Amazon VPC.

Erstellen einer VPC-Endpunktrichtlinie für AWS Proton

Sie können eine Endpunktrichtlinie an Ihren VPC-Endpunkt anhängen, der den Zugriff auf AWS Proton steuert. Die Richtlinie gibt die folgenden Informationen an:

- Prinzipal, der die Aktionen ausführen kann.

- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuerung des Zugriffs auf Services mit VPC-Endpunkten im Amazon-VPC-Benutzerhandbuch.

Beispiel: VPC-Endpunktrichtlinie für - AWS Proton Aktionen

Im Folgenden finden Sie ein Beispiel für eine Endpunktrichtlinie für AWS Proton. Wenn diese Richtlinie an einen Endpunkt angefügt wird, gewährt sie Zugriff auf die aufgelisteten AWS Proton Aktionen für alle Prinzipale auf allen Ressourcen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Principal": "*",
      "Action": [
        "proton:ListServiceTemplates",
        "proton:ListServiceTemplateMajorVersions",
        "proton:ListServiceTemplateMinorVersions",
        "proton:ListServices",
        "proton:ListServiceInstances",
        "proton:ListEnvironments",
        "proton:GetServiceTemplate",
        "proton:GetServiceTemplateMajorVersion",
        "proton:GetServiceTemplateMinorVersion",
        "proton:GetService",
        "proton:GetServiceInstance",
        "proton:GetEnvironment",
        "proton:CreateService",
        "proton:UpdateService",
        "proton:UpdateServiceInstance",
        "proton:UpdateServicePipeline",
        "proton:DeleteService"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Protokollieren und Überwachen in AWS Proton

Überwachung ist wichtig, um die Zuverlässigkeit, Verfügbarkeit und Performance vonAWS Protonund dein andererAWS-Lösungen.AWSbietet die folgenden Überwachungstools, um zu beobachten, wie Ihre Instanzen laufenAWS Proton, melden Sie, wenn etwas schiefgeht, und ergreifen Sie gegebenenfalls automatisch Maßnahmen.

Zu diesem ZeitpunktAWS Protonselbst ist nicht in Amazon CloudWatch Logs integriert oderAWS Trusted Advisoraus. Administratoren können CloudWatch konfigurieren und verwenden, um andere zu überwachenAWS-Serviceswie in ihren Service- und Umgebungsvorlagen definiert.AWS Protonist in integriertAWS CloudTrailaus.

- Amazon CloudWatch überwacht Ihre AWS-Ressourcen und die in AWS ausgeführten Anwendungen in Echtzeit. Sie können Metriken erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Beispielsweise können Sie mit CloudWatch die CPU-Auslastung oder andere Metriken Ihrer Amazon EC2-Instances erfassen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im Amazon CloudWatch User Guide.
- Amazon CloudWatch LogsMit Amazon können Sie Ihre Protokolldateien von Amazon EC2 EC2-Instances, CloudTrail und anderen Quellen überwachen, speichern und darauf zugreifen. CloudWatch Logs kann Informationen in den Protokolldateien überwachen und Sie benachrichtigen, wenn bestimmte Schwellenwerte erreicht werden. Sie können Ihre Protokolldaten auch in einem sehr robusten Speicher archivieren. Weitere Informationen finden Sie im Amazon CloudWatch Logs User Guide.
- AWS CloudTrail erfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS-Konto-Kontos erfolgten, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon-S3-Bucket. Sie können die Benutzer und Konten, die AWS aufgerufen haben, identifizieren, sowie die Quell-IP-Adresse, von der diese Aufrufe stammen, und den Zeitpunkt der Aufrufe ermitteln. Weitere Informationen finden Sie im AWS CloudTrail-Benutzerhandbuch.
- Amazon EventBridgeEs ist ein Serverless-Ereignisbus-Service, über den Sie Ihre Anwendungen einfach mit Daten aus verschiedenen Quellen verbinden können. EventBridge stellt einen Stream von Echtzeitdaten aus Ihren eigenen Anwendungen, Software-as-a-Service (SaaS) -Anwendungen undAWS-Servicesund leitet diese Daten an Ziele wie Lambda weiter. Auf diese Weise können Sie Ereignisse überwachen, die in Services auftreten, und ereignisgesteuerte Architekturen

erstellen. Weitere Informationen finden Sie unterAutomatisieren AWS Proton mit EventBridgeund dieEventBridge-Benutzerhandbuchaus.

Ausfallsicherheit in AWS Proton

DieAWSIm Umfeld der globalen -InfrastrukturAWS-Regionund Availability Zones.AWS-Regions stellen mehrere physisch getrennte und isolierte Availability Zones bereit, die über hoch redundante Netzwerke mit niedriger Latenz, hohem Durchsatz und hochredundanten Vernetzungen verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Zonen ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zuAWS-Regions und Availability Zones finden Sie unterAWSGlobale - Infrastrukturaus.

Neben der globalen AWS-Infrastruktur stellt AWS Proton Funktionen bereit, um Ihren Anforderungen an Ausfallsicherheit und Datensicherung gerecht zu werden.

AWS ProtonBackups

AWS Protonunterhält eine Sicherung aller Kundendaten. Im Falle eines vollständigen Ausfalls kann diese Sicherung zur Wiederherstellung verwendet werdenAWS Protonund Kundendaten aus einem früheren gültigen Status.

Bewährte Methoden für die Sicherheit für AWS Proton

AWS Protonbietet Sicherheitsfunktionen, die Sie beim Entwickeln und Implementieren Ihrer eigenen Sicherheitsrichtlinien berücksichtigen sollten. Die folgenden bewährten Methoden sind allgemeine Richtlinien und keine vollständige Sicherheitslösung. Da diese bewährten Methoden für Ihre Umgebung möglicherweise nicht angemessen oder ausreichend sind, sollten Sie sie als hilfreiche Überlegungen und nicht als bindend ansehen.

Themen

- Verwendung von IAM für die Zugriffskontrolle
- Keine Anmeldeinformationen in Vorlagen und Vorlagenpakete einbetten

- Schützen Sie sensible Daten mithilfe der Verschlüsselung
- Verwenden vonAWS CloudTrailum API-Aufrufe anzuzeigen und zu protokollieren

Verwendung von IAM für die Zugriffskontrolle

IAM ist einAWS-Servicedie Sie zum Verwalten von Benutzern und deren Berechtigungen inAWSaus. Sie können IAM mitAWS Protonum anzugeben welcheAWS ProtonAktionen, die Administratoren und Entwickler ausführen können, z. B. das Verwalten von Vorlagen, Umgebungen oder Diensten. Sie können IAM-Dienstrollen verwenden, um zuzulassenAWS Protonum in Ihrem Namen Anrufe bei anderen -Services zu tätigen.

Weitere Informationen zuAWS Protonund IAM-Rollen sieheIdentitäts- und Zugriffsverwaltung für AWS Protonaus.

Implementieren der geringstmöglichen Zugriffsrechte Weitere Informationen finden Sie unterBerechtigungen und Richtlinien in IAMimAWS Identity and Access Management-Benutzerhandbuchaus.

Keine Anmeldeinformationen in Vorlagen und Vorlagenpakete einbetten

Anstatt vertrauliche Informationen in Ihre einzubettenAWS CloudFormationVorlagen und Vorlagenpakete, empfehlen wir IhnenDynamische Referenzenin Ihrer Stack-Vorlage.

Dynamische Referenzen bieten eine kompakte und leistungsstarke Möglichkeit, externe Werte zu referenzieren, die in anderen Services wieAWS Systems ManagerParameterspeicher oderAWS Secrets Manageraus. Wenn Sie eine dynamische Referenz verwenden, ruft CloudFormation bei Bedarf den Wert der angegebenen Referenz in Stack- und Änderungssatz-Operationen ab und übergibt den Wert an die betreffende Ressource. CloudFormation speichert jedoch nie den tatsächlichen Referenzwert. Weitere Informationen finden Sie unterVerwenden von dynamischen Referenzen zum Angeben von VorlagenwertenimAWS CloudFormation-Benutzerhandbuchaus.

AWS Secrets Managerhilft Ihnen, die Anmeldeinformationen für Ihre Datenbanken und Services sicher zu verschlüsseln, zu speichern und wieder abzurufen. DieAWS Systems ManagerParameter Storebietet eine sichere, hierarchische Speicherung für die Konfigurationsdatenverwaltung.

Für weitere Informationen zum Definieren von Vorlagenparametern siehehttps://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/parameters-section-structure.htmlimAWS CloudFormation-Benutzerhandbuchaus.

Schützen Sie sensible Daten mithilfe der Verschlüsselung

WITHINAWS Protonwerden alle Kundendaten standardmäßig mit einemAWS Protonim Besitz eines Schlüssels.

Als Mitglied des Plattformteams können Sie einen vom Kunden verwalteten Schlüssel zurAWS Protonum Ihre sensiblen Daten zu verschlüsseln und zu sichern. Verschlüsseln Sie sensible Daten im Ruhezustand in Ihrem S3-Bucket. Weitere Informationen finden Sie unter Datenschutz in AWS Proton .

Verwenden vonAWS CloudTrailum API-Aufrufe anzuzeigen und zu protokollieren

AWS CloudTrailverfolgt jede Person, die -API-Aufrufe in IhremAWS-Kontoaus. API-Aufrufe werden protokolliert, wenn jemand dasAWS ProtonAPI, dieAWS Proton-Konsole oderAWS Proton AWS CLI-Befehle. Aktivieren Sie die Protokollierung, und legen Sie einen Amazon S3-Bucket zum Speichern der Protokolle fest. Auf diese Weise können bei Bedarf Sie nachvollziehen, wer welcheAWS Protonrufen Sie Ihr Konto an. Weitere Informationen finden Sie unter Protokollieren und Überwachen in AWS Proton.

Dienstübergreifende Confused-Deputy-Prävention

Das Confused-Deputy-Problem ist ein Sicherheitsproblem, bei dem eine juristische Stelle, die nicht über die Berechtigung zum Ausführen einer Aktion verfügt, eine privilegiertere juristische Stelle zwingen kann, die Aktion auszuführen. In AWS kann der dienstübergreifende Identitätswechsel zu Confused-Deputy-Problem führen. Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen Dienst). Der aufrufende Service kann manipuliert werden, um seine Berechtigungen zu verwenden, um Aktionen auf die Ressourcen eines anderen Kunden auszuführen, für die er sonst keine Zugriffsberechtigung haben sollte. Um dies zu verhindern, bietet AWS Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben.

Wir empfehlen die Verwendung der globalen Bedingungskontext-Schlüssel `aws:SourceArn` und `aws:SourceAccount` in ressourcenbasierten Richtlinien, um die Berechtigungen, die AWS Proton einem anderen Service erteilt, auf eine bestimmte Ressource zu beschränken. Wenn der `aws:SourceArn`-Wert die Konto-ID nicht enthält, z. B. einen Amazon-S3-Bucket-ARN, müssen Sie beide globale Bedingungskontextschlüssel verwenden, um Berechtigungen einzuschränken.

Wenn Sie beide globale Bedingungskontextschlüssel verwenden und der `aws:SourceArn`-Wert die Konto-ID enthält, müssen der `aws:SourceAccount`-Wert und das Konto im `aws:SourceArn`-Wert dieselbe Konto-ID verwenden, wenn sie in der gleichen Richtlinienanweisung verwendet wird. Verwenden Sie `aws:SourceArn`, wenn Sie nur eine Ressource mit dem betriebsübergreifenden Zugriff verknüpfen möchten. Verwenden Sie `aws:SourceAccount`, wenn Sie zulassen möchten, dass Ressourcen in diesem Konto mit der betriebsübergreifenden Verwendung verknüpft werden.

Der Wert von`aws:SourceArn`muss eine Ressource sein, dieAWS ProtonGeschäfte

Der effektivste Weg, um sich vor dem verwirrten Stellvertreterproblem zu schützen, ist die Verwendung des`aws:SourceArn`globaler Bedingungskontextschlüssel mit dem vollständigen ARN der Ressource Wenn Sie den vollständigen ARN der Ressource nicht kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den`aws:SourceArn`globaler Kontextbedingungsschlüssel mit Platzhaltern (*) für die unbekannten Teile des ARN. Zum Beispiel, `arn:aws::proton:*:`*`123456789012`*`:environment/*`.

Das folgende Beispiel zeigt, wie Sie den`aws:SourceArn`und`aws:SourceAccount`globale Bedingungskontext-Schlüssel in`AWS Proton`Vermeiden des Problems des verwirrten Stellvertreters

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Sid": "ExampleProtonConfusedDeputyPreventionPolicy",
        "Effect": "Allow",
        "Principal": {"Service": "proton.amazonaws.com"},
        "Action": "sts:AssumeRole",
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "123456789012"
            },
            "ArnLike": {
                "aws:SourceArn": "arn:aws::proton:*:123456789012:environment/*"
            }
        }
    }
}
```

CodeBuild Bereitstellung von benutzerdefinierter Amazon VPC-Unterstützung

AWS Proton CodeBuild Provisioning führt beliebige, vom Kunden bereitgestellte CLI-Befehle in einem CodeBuild Projekt aus, das sich imAWS Proton Umgebungskonto befindet. Diese Befehle verwalten Ressourcen in der Regel mithilfe eines Infrastructure as Code (IaC) -Tools wie CDK. Wenn Sie Ressourcen in einer Amazon VPC haben, CodeBuild können Sie möglicherweise nicht darauf zugreifen. Um dies zu ermöglichen, CodeBuild unterstützt es die Ausführung innerhalb einer bestimmten Amazon VPC. Zu den Anwendungsbeispielen gehören:

- Rufen Sie Abhängigkeiten aus selbst gehosteten, internen Artefakt-Repositorys ab, z. B.`PyPI` für Python,`Maven` für Java und`npm` für Node.js
- CodeBuild muss auf einen Jenkins-Server in einer bestimmten Amazon VPC zugreifen, um eine Pipeline zu registrieren.
- Greifen Sie auf Objekte in einem Amazon S3 S3-Bucket zu, das so konfiguriert ist, dass der Zugriff nur über einen Amazon VPC-Endpunkt möglich ist.
- Führen Sie Integrationstests von Ihrem Build aus mit Daten in einer Amazon RDS-Datenbank aus, die in einem privaten Subnetz isoliert ist.

Weitere Informationen finden SieCodeBuild in der VPC-Dokumentation für diesen.

Wenn Sie möchten, dass CodeBuild Provisioning in einer benutzerdefinierten VPC ausgeführt wird,AWS Proton bietet dies eine unkomplizierte Lösung. Zunächst müssen Sie der Umgebungsvorlage die VPC-ID, Subnetze und Sicherheitsgruppen hinzufügen. Als Nächstes geben Sie diese Werte in die Umgebungsspezifikation ein. Dies führt dazu, dass ein CodeBuild Projekt für Sie erstellt wird, das auf eine bestimmte VPC abzielt.

Aktualisierung der Umgebungsvorlage

Schema

Die VPC-ID, Subnetze und Sicherheitsgruppen müssen dem Vorlagenschema hinzugefügt werden, damit sie in der Umgebungsspezifikation existieren können.

Ein Beispiel`schema.yaml`:

```
schema:
  format:
```

```
    openapi: "3.0.0"
  environment_input_type: "EnvironmentInputType"
  types:
    EnvironmentInputType:
      type: object
      properties:
        codebuild_vpc_id:
          type: string
        codebuild_subnets:
          type: array
          items:
            type: string
        codebuild_security_groups:
          type: array
          items:
            type: string
```

Dadurch werden drei neue Eigenschaften hinzugefügt, die vom Manifest verwendet werden:

- `codebuild_vpc_id`
- `codebuild_subnets`
- `codebuild_security_groups`

Manifest

Um die Amazon VPC-Einstellungen zu konfigurieren CodeBuild,`project_properties` ist im Vorlagenmanifest eine optionale Eigenschaft namens verfügbar. Der Inhalt von`project_properties` wird demAWS CloudFormation Stapel hinzugefügt, der das CodeBuild Projekt erstellt. Dadurch ist es möglich, nicht nur AmazonAWS CloudFormation VPC-Eigenschaften, sondern auch jede unterstützte CodeBuild CloudFormation Eigenschaft hinzuzufügen, z. B. ein Build-Timeout. Dieselben Daten, die für`proton-inputs.json` bereitgestellt wurden, werden für die Werte von zur Verfügung gestellt`project_properties`.

Füge diesen Abschnitt zu deinem hinzu`manifest.yaml`:

```
project_properties:
          VpcConfig:
            VpcId: "{{ environment.inputs.codebuild_vpc_id }}"
            Subnets: "{{ environment.inputs.codebuild_subnets }}"
            SecurityGroupIds: "{{ environment.inputs.codebuild_security_groups }}"
```

Somanifest.yaml könnte das Ergebnis aussehen:

```
infrastructure:
  templates:
    - rendering_engine: codebuild
      settings:
        image: aws/codebuild/amazonlinux2-x86_64-standard:4.0
        runtimes:
          nodejs: 16
        provision:
          - npm install
          - npm run build
          - npm run cdk bootstrap
          - npm run cdk deploy -- --require-approval never
        deprovision:
          - npm install
          - npm run build
          - npm run cdk destroy -- --force
        project_properties:
          VpcConfig:
            VpcId: "{{ environment.inputs.codebuild_vpc_id }}"
            Subnets: "{{ environment.inputs.codebuild_subnets }}"
            SecurityGroupIds: "{{ environment.inputs.codebuild_security_groups }}"
```

Erstellen der Umgebung

Wenn Sie eine Umgebung mit Ihrer CodeBuild Provisioning VPC-fähigen Vorlage erstellen, müssen Sie die Amazon VPC-ID, Subnetze und Sicherheitsgruppen angeben.

Führen Sie zum Abrufen einer Liste aller Amazon VPC-IDs Ihrer Region den folgenden Befehl aus:

```
aws ec2 describe-vpcs
```

Führen Sie zum Abrufen einer Liste aller Subnetz-IDs den folgenden aus:

```
aws ec2 describe-subnets --filters "Name=vpc-id,Values=vpc-id"
```

> **Important**
>
> Schließt nur private Subnetze ein. CodeBuild schlägt fehl, wenn Sie öffentliche Subnetze bereitstellen. Öffentliche Subnetze haben eine Standardroute zu einem Internet Gateway, private Subnetze nicht.

Führen Sie zum Abrufen der Sicherheitsgruppen den folgenden Befehl aus, um die Sicherheitsgruppen-IDs abzurufen. Diese IDs können auch abgerufen werden überAWS Management Console:

```
aws ec2 describe-security-groups --filters "Name=vpc-id,Values=vpc-id"
```

Die Werte werden wie folgt aussehen:

```
vpc-id: vpc-045ch35y28dec3a05
subnets:
  - subnet-04029a82e6ae46968
  - subnet-0f500a9294fc5f26a
 security-groups:
  - sg-03bc4c4ce32d67e8d
```

Sicherstellung von CodeBuild Berechtigungen

Für die Unterstützung von Amazon VPC sind bestimmte Berechtigungen erforderlich, z. B. die Fähigkeit, ein Elastic Network Interface zu erstellen.

Wenn die Umgebung in der Konsole erstellt wird, geben Sie diese Werte während des Assistenten zur Umgebungserstellung ein. Wenn Sie die Umgebung programmgesteuert erstellen möchten,`spec.yaml` sieht Ihre wie folgt aus:

```

proton: EnvironmentSpec

spec:
  codebuild_vpc_id: vpc-045ch35y28dec3a05
  codebuild_subnets:
    - subnet-04029a82e6ae46968
    - subnet-0f500a9294fc5f26a
  codebuild_security_groups:
```

```
    - sg-03bc4c4ce32d67e8d
```

AWS ProtonRessourcen und Tagging

AWS ProtonZu den Ressourcen, denen ein Amazon-Ressourcenname (ARN) zugewiesen ist, gehören Umgebungsvorlagen und deren Haupt- und Nebenversionen, Service-Vorlagen sowie deren Haupt- und Nebenversionen, Umgebungen, Services, Service-Instances, Komponenten und Repositorys. Sie können diese Ressourcen mit Tags organisieren und kenntlich machen. Sie können Tags verwenden, um Ressourcen nach Zweck, Eigentümer, Umgebung oder anderen Kriterien zu kategorisieren. Weitere Informationen finden Sie unter Tagging-Strategien in . So verfolgen und verwalten Sie IhreAWS Proton-Ressourcen verwenden, können Sie die in den folgenden Abschnitten beschriebenen Tagging-Funktionen verwenden.

AWSmarkierend

Sie können Metadaten Ihren AWS-Ressourcen in Form von Tags zuweisen. Jedes Tag (Markierung) besteht aus einem kundendefinierten Schlüssel und einem optionalen Wert. Mit Tags können Sie Ressourcen verwalten, identifizieren, organisieren, suchen und filtern.

> **Important**
>
> Fügen Sie keine personenbezogenen Daten (Personally Identifiable Information, PII) oder andere vertrauliche Informationen in Tags hinzu. Tags sind für viele AWS-Services zugänglich, einschließlich der Abrechnung. Tags sind nicht für private oder vertrauliche Daten gedacht.

Jedes -Tag besteht aus zwei Teilen.

- einem Tag-Schlüssel (z. B. `CostCenter`, `Environment` oder `Project`). Bei Tag-Schlüsseln wird zwischen Groß- und Kleinschreibung unterschieden.
- Einem Tag-Wert (z. B.`111122223333`oder`Production`) enthalten. Wie bei Tag-Schlüsseln wird auch bei Tag-Werten zwischen Groß- und Kleinschreibung unterschieden.

Die folgenden grundlegenden Benennungs- und Verwendungsanforderungen gelten für Tags.

- Eine Ressource kann bis zu 50 Tags besitzen, die von Benutzern erstellt wurden.

> **Note**
>
> Vom System erstellte Tags, die mit dem beginnen`aws:`Präfix sind reserviert fürAWSverwenden und nicht auf dieses Limit anrechnen. Tags, die mit dem einem `aws:`-Präfix beginnen, können nicht bearbeitet oder gelöscht werden.

- Jeder Tag (Markierung) muss für jede Ressource eindeutig sein. Jeder Tag (Markierung) kann nur einen Wert haben.
- Der Tag-Schlüssel muss eine Länge zwischen 1 und 128 Unicode-Zeichen in UTF-8 aufweisen.
- Der Tag-Wert muss eine Länge zwischen 1 und 256 Unicode-Zeichen in UTF-8 aufweisen.
- Zulässige Zeichen Buchstaben, Leerzeichen, die in UTF-8 darstellbar sind, sowie die folgenden Zeichen: + - @.

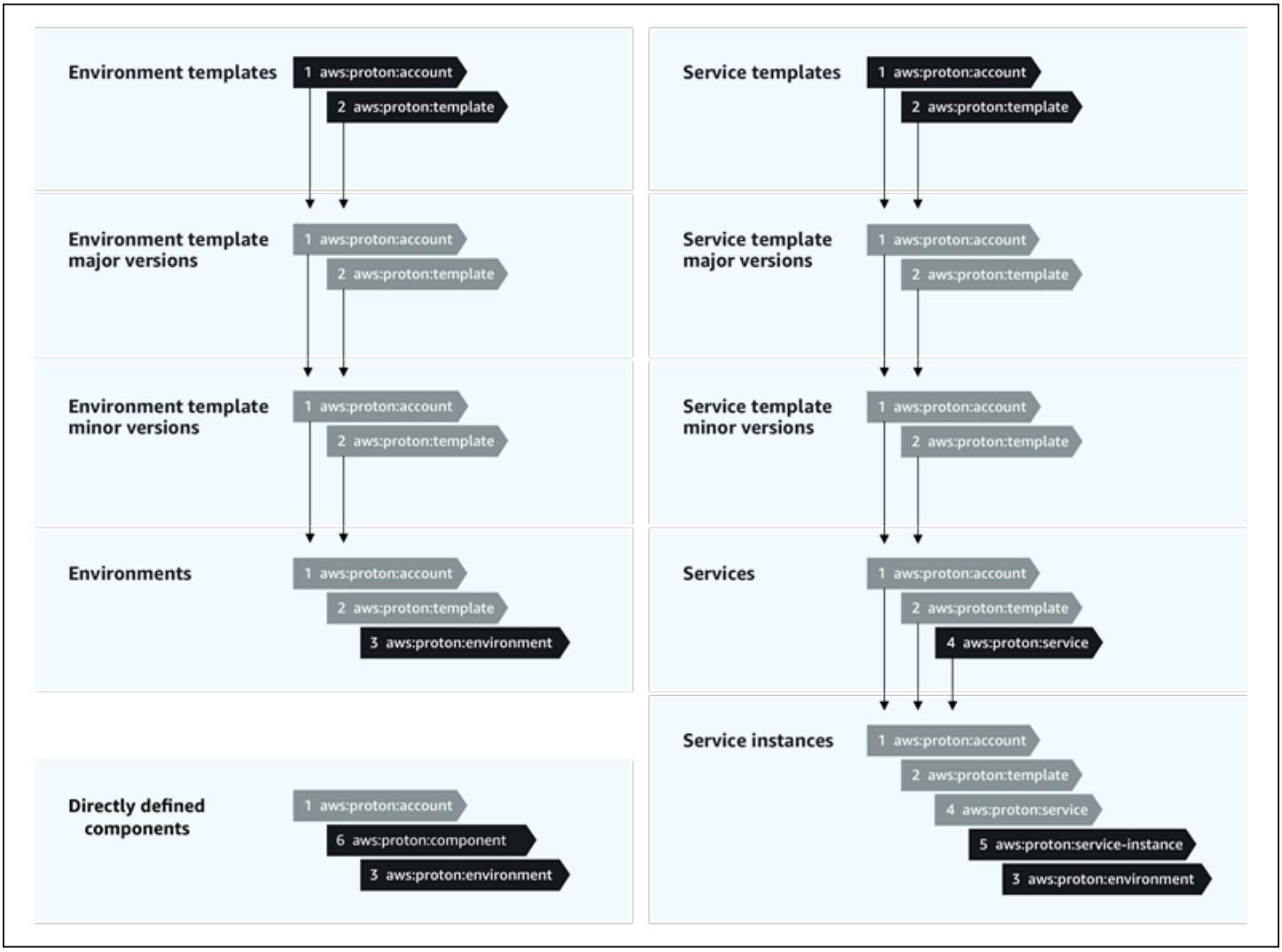
AWS Protonmarkierend

mitAWS Protonkönnen Sie sowohl die Tags, die Sie erstellen, als auch die Tags verwenden, dieAWS Protongeneriert automatisch für Sie.

AWS Proton AWSVerwaltete Tags

Wenn Sie eine erstellenAWS ProtonRessource,AWS ProtonWird automatisch generiert.AWSVerwaltete Tags für Ihre neue Ressource, wie im folgenden Diagramm dargestellt.AWSverwaltete Tags werden später an andere weitergegebenAWS ProtonRessourcen, die auf Ihrer neuen Ressource basieren. Beispielsweise werden verwaltete Tags aus einer Umgebungsvorlage an ihre Versionen weitergegeben, und verwaltete Tags aus einem Service werden an seine Dienstinstanzen weitergegeben.

> **Note**
>
> AWSVerwaltete Tagssind nichtgeneriert für Verbindungen mit Umgebungskonten. Weitere Informationen finden Sie unter the section called “Kontoverbindungen”.



Weitergabe von Tags an bereitgestellte Ressourcen

Wenn bereitgestellte Ressourcen, wie sie in Service- und Umgebungsvorlagen definiert sind, unterstützenAWStagging, dasAWSVerwaltete Tags werden als vom Kunden verwaltete Tags an bereitgestellte Ressourcen weitergegeben. Diese Tags werden nicht an eine bereitgestellte Ressource weitergegeben, die nicht unterstütztAWSTagging.

AWS Protonwendet Tags auf Ihre Ressourcen anAWS ProtonKonten, registrierte Vorlagen und bereitgestellte Umgebungen sowie Dienste und Dienstinstanzen, wie in der folgenden Tabelle beschrieben. Sie können Folgendes verwendenAWSverwaltete Tags zum Anzeigen und Verwalten IhrerAWS ProtonRessourcen, aber Sie können sie nicht ändern.

AWSVerwalteter Tag-Schlüssel	Propagiert durch kundenverwalteten Schlüssel	Beschreibung
`aws:proton:account`	`proton:account`	DieAWSKonto, das erstellt und bereitgestellt wirdAWS ProtonRessourcen schätzen.
`aws:proton:template`	`proton:template`	Der ARN einer ausgewählten Vorlage.
`aws:proton:environment`	`proton:environment`	Der ARN einer ausgewählten Umgebung.
`aws:proton:service`	`proton:service`	Der ARN eines ausgewählten Dienstes.
`aws:proton:service-instance`	`proton:service-instance`	Der ARN einer ausgewählten Dienstinstanz.
`aws:proton:component`	`proton:component`	Der ARN einer ausgewählten Komponente.

Es folgt ein Beispiel für eineAWSverwaltetes Tag für eineAWS ProtonRessource.

```
"aws:proton:template" = "arn:aws:proton:region-id:account-id:environment-template/env-template"
```

Im Folgenden finden Sie ein Beispiel für ein kundenverwaltetes Tag, das auf eine bereitgestellte Ressource angewendet wurde und von einemAWSVerwaltetes Tag.

```
"proton:environment:database" = "arn:aws:proton:region-id:account-id:rds/env-db"
```

mitAWS-verwaltete Bereitstellung,AWS Protonwendet propagierte Tags direkt auf bereitgestellte Ressourcen an.

mitSelbstverwaltetes Provisioning,AWS Protonstellt propagierte Tags zusammen mit den gerenderten IAc-Dateien zur Verfügung, die es im Provisioning Pull Request (PR) einreicht. Tags werden in der String-Map-Variablen bereitgestelltproton_tags. Wir empfehlen Ihnen, in Ihrer Terraform-

Konfiguration einen Verweis auf diese Variable zu erstellen, die Folgendes einschließtAWS ProtonStichworte in`default_tags`. Dies verbreitet sichAWS Proton-Tags für alle bereitgestellten Ressourcen.

Das folgende Beispiel zeigt diese Methode der Tag-Propagierung in einer Terraform-Umgebungsvorlage.

Hier sehen Sie den`proton_tags`Variablendefinition:

proton.environment.variables.tf:

```
variable "environment" {
  type = object({
    inputs = map(string)
    name = string
  })
}

variable "proton_tags" {
  type = map(string)
  default = null
}
```

So werden dieser Variablen Tag-Werte zugewiesen:

proton.auto.tfvars.json:

```
{
  "environment": {
    "name": "dev",
    "inputs": {
      "ssm_parameter_value": "MyNewParamValue"
    }
  }

  "proton_tags" : {
    "proton:account" : "123456789012",
    "proton:template" : "arn:aws:proton:us-east-1:123456789012:environment-template/
fargate-env",
    "proton:environment" : "arn:aws:proton:us-east-1:123456789012:environment/dev"
  }
}
```

Und so können Sie hinzufügenAWS Proton-Tags in Ihrer Terraform-Konfiguration, sodass sie zu bereitgestellten Ressourcen hinzugefügt werden:

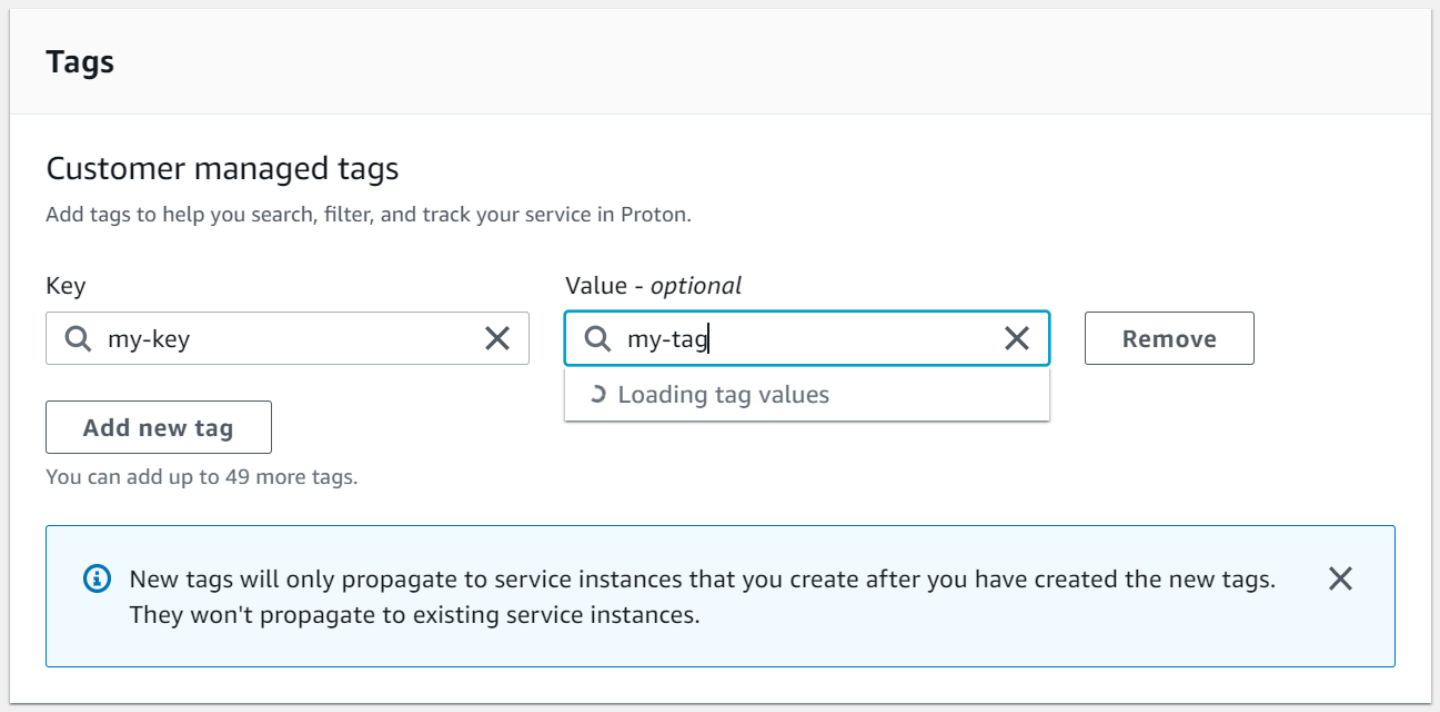
```
# Configure the AWS Provider
provider "aws" {
  region = var.aws_region
  default_tags {
    tags = var.proton_tags
  }
}
```

Kundenverwaltete Tags

EACHAWS ProtonRessource hat ein maximales Kontingent von 50 vom Kunden verwalteten Tags. Kundenverwaltete Tags werden an untergeordnete Elemente weitergegebenAWS ProtonRessourcen auf die gleiche Weise wieAWSverwaltete Tags tun dies, außer dass sie sich nicht an vorhandene weitergebenAWS ProtonRessourcen oder bereitgestellte Ressourcen. Wenn Sie ein neues Tag auf einAWS ProtonRessource mit vorhandenen untergeordneten Ressourcen und Sie möchten, dass die vorhandenen untergeordneten Ressourcen mit dem neuen Tag gekennzeichnet werden, müssen Sie jede vorhandene untergeordnete Ressource manuell über die Konsole oderAWS CLI.

Erstellen von Tags mithilfe der Konsole und der CLI

Wenn Sie eine erstellenAWS Proton-Ressource mithilfe der Konsole haben Sie die Möglichkeit, vom Kunden verwaltete Tags entweder auf der ersten oder zweiten Seite der Erstellungsprozedur zu erstellen, wie im folgenden Konsolen-Snapshot gezeigt. Klicken Sie aufNeues Tag hinzufügen, geben Sie Schlüssel und Wert ein und fahren Sie fort.



Nachdem Sie eine neue Ressource erstellt habenAWS Proton-Konsole können Sie die Liste derAWSverwaltete und vom Kunden verwaltete Tags auf der Detailseite.

Erstellen oder bearbeiten

1. In derAWS ProtonKonsole, öffne einAWS ProtonRessourcen-Detailseite, auf der Sie eine Liste von Tags sehen können.
2. Wählen Sie Manage tags (Tags (Markierungen) verwalten) aus.
3. In derVerwalten von Tagskönnen Sie Tags anzeigen, entfernen und bearbeiten. Sie können dasAWSVerwaltete Tags, die oben aufgeführt sind. Sie können jedoch vom Kunden verwaltete Tags mit Bearbeitungsfeldern hinzufügen und ändern, die nach demAWSVerwaltete Tags.

   Klicken Sie aufNeues Tag hinzufügenum ein neues Tag zu erstellen.
4. Geben Sie einen Schlüssel und Wert für den neuen Tag ein.
5. Um ein Tag zu bearbeiten, geben Sie einen Wert in das Feld Tagwert für einen ausgewählten Schlüssel ein.
6. So löschen Sie ein TagRemovefür ein ausgewähltes Tag.
7. Wenn Sie fertig sind, klicken Sie aufSpeichern Sie die Änderungen.

Erstellen Sie TagsAWS Proton AWS CLI

Sie können Tags anzeigen, erstellen, entfernen und bearbeitenAWS Proton AWS CLI.

Sie können ein Tag für eine Ressource erstellen oder bearbeiten, wie im folgenden Beispiel gezeigt.

```
$ aws proton tag-resource \
    --resource-arn "arn:aws:proton:region-id:account-id:service-template/webservice" \
    --tags '[{"key":"mykey1","value":"myval1"},{"key":"mykey2","value":"myval2"}]'
```

Sie können ein Tag für eine Ressource entfernen, wie im folgenden Beispiel gezeigt.

```
$ aws proton untag-resource \
    --resource-arn "arn:aws:proton:region-id:account-id:service-template/webservice" \
    --tag-keys '["mykey1","mykey2"]'
```

Sie können Tags für eine Ressource auflisten, wie im letzten Beispiel gezeigt.

```
$ aws proton list-tags-for-resource \
    --resource-arn "arn:aws:proton:region-id:account-id:service-template/webservice"
```

Fehlerbehebung für AWS Proton

Erfahren Sie, wie Sie in eine Fehlersuche fürAWS Proton.

Themen

Bereitstellungsfehler, die aufAWS CloudFormation dynamische Parameter verweisen

Wenn Sie Bereitstellungsfehler sehen, die auf Ihre CloudFormation dynamischen Variablen verweisen, stellen Sie sicher, dass es sich um Jinja-Escape-Variablen handelt. Diese Fehler können durch eine Fehlinterpretation Ihrer dynamischen Variablen durch Jinja verursacht werden. Die CloudFormation dynamische Parametersyntax ist der Jinja-Syntax, die Sie für IhreAWS Proton Parameter verwenden, sehr ähnlich.

Beispiel für eine CloudFormation dynamische Variablensyntax:

`'{{resolve:secretsmanager:MySecret:SecretString:password:EXAMPLE1-90ab-cdef-fedc-ba987EXAMPLE}}'`.

Beispiel für die Jinja-Syntax einesAWS Proton Parameters:

`'{{ service_instance.environment.outputs.env-outputs }}'`.

Um diese Fehlinterpretationsfehler zu vermeiden, maskiert Jinja Ihre CloudFormation dynamischen Parameter, wie in den folgenden Beispielen gezeigt.

Dieses Beispiel stammt aus demAWS CloudFormation Benutzerhandbuch. Die SegmenteAWS Secrets Manager Secret-Name und JSON-Key können verwendet werden, um die im Secret gespeicherten Anmeldeinformationen abzurufen.

```
MyRDSInstance:
  Type: AWS::RDS::DBInstance
  Properties:
    DBName: 'MyRDSInstance'
      AllocatedStorage: '20'
      DBInstanceClass: db.t2.micro
```

```
      Engine: mysql
      MasterUsername: '{{resolve:secretsmanager:MyRDSSecret:SecretString:username}}'
      MasterUserPassword:
 '{{resolve:secretsmanager:MyRDSSecret:SecretString:password}}'
```

Um den CloudFormation dynamischen Parametern zu entkommen, können Sie zwei verschiedene Methoden verwenden:

- Einen Block einschließen zwischen`{% raw %}` and `{% endraw %}`:

```
'{% raw %}'
MyRDSInstance:
  Type: AWS::RDS::DBInstance
  Properties:
    DBName: 'MyRDSInstance'
      AllocatedStorage: '20'
      DBInstanceClass: db.t2.micro
      Engine: mysql
      MasterUsername: '{{resolve:secretsmanager:MyRDSSecret:SecretString:username}}'
      MasterUserPassword:
 '{{resolve:secretsmanager:MyRDSSecret:SecretString:password}}'
'{% endraw %}'
```

- Füge einen Parameter ein zwischen`"{{ }}"`:

```
MyRDSInstance:
  Type: AWS::RDS::DBInstance
  Properties:
    DBName: 'MyRDSInstance'
      AllocatedStorage: '20'
      DBInstanceClass: db.t2.micro
      Engine: mysql
      MasterUsername:
 "{{ '{{resolve:secretsmanager:MyRDSSecret:SecretString:username}}' }}"
      MasterUserPassword:
 "{{ '{{resolve:secretsmanager:MyRDSSecret:SecretString:password}}' }}"
```

Weitere Informationen finden Sie unter Jinja auf der Flucht.

AWS Proton-Kontingente

In der folgenden Tabelle sind aufgeführtAWS ProtonKontingente. Alle Werte verstehen sich proAWSKonto, pro unterstütztemAWSRegion.

Ressourcenkontingent	Standardlimit	Anpassbar?
Maximale Größe des Vorlagenpakets	10 MB	✗ Nein
Maximale Größe der Vorlagenmanifestdatei	2 MB	✗ Nein
Maximale Größe der Vorlagenschemadatei	2 MB	✗ Nein
Maximale Größe jeder Vorlagendatei	2 MB	✗ Nein
Maximale Länge jedes Vorlagennamens	100 Zeichen	✗ Nein
Maximale Anzahl vonCloudFormationVorlagendateien pro Paket	1	✗ Nein
Maximale Anzahl registrierter Vorlagen pro Konto-, Service- und Umgebungsvorlagen zusammen	1000	✓ Ja
Maximale Anzahl registrierter Vorlageversionen pro Vorlage	1000	✓ Ja
Maximale Anzahl von Dateien proCodeBuildBereitstellungspaket	500	✗ Nein
Die maximale Anzahl an Umgebungen pro Konto	1000	✓ Ja
Maximale Anzahl der Services pro Konto	1000	✓ Ja
Maximale Anzahl von Service-Instances pro Service	20	✓ Ja
Maximale Anzahl der Komponenten pro Konto	1000	✓ Ja
Maximale Anzahl von Umgebungskontoverbindungen pro Umgebungskonto	1000	✓ Ja

Dokumentverlauf

In der folgenden Tabelle werden die wichtigen Änderungen in der Dokumentation in Bezug auf die neueste Version von AWS Proton und das Feedback von Kunden beschrieben. Um Benachrichtigungen über Aktualisierungen dieser Dokumentation zu erhalten, können Sie einen RSS-Feed abonnieren.

- API-Version: 2020-07-20

Änderung	Beschreibung	Datum
Aktualisierung der verwalteten Richtlinien	`AWSProtonCodeBuildProvisioningServiceRolePolicy` Die Richtlinie wurde aktualisiert.	12. Mai 2023
Service-Synchronisationskonfigurationen.	AWS Protonfügt Unterstützung für Service Sync-Konfigurationen hinzu.	31. März 2023
CodeBuild	AWS Protonfügt Unterstützung für die CodeBuildBereitstellung hinzu.	16. November 2022
Aktualisierung der verwalteten Richtlinien	Es wurde eine `AWSProtonCodeBuildProvisioningBasicAccess` Richtlinie hinzugefügt, CodeBuild die die Berechtigungen erteilt, die für die Ausführung eines Builds für die AWS Proton CodeBuild Bereitstellung erforderlich sind.	11. November 2022

Verbreitung von Terraform-Tags	Terraform-Tag-Propagation wurde dem Kapitel Tagging hinzugefügt.	16. September 2022
Leitfaden zur API-Migration	Der API-Migrationsleitfaden vor GA wurde entfernt.	12. August 2022
AWS Protonobjekte	Es wurde ein Thema über AWS Proton Objekte und ihre Beziehung zu anderen Objekten AWS und Objekten von Drittanbietern hinzugefügt. Siehe AWS ProtonObjekte.	29. Juli 2022
Erläuterungen zum verlinkten Repositorium	Der Zweck verknüpfter (registrierter) Repositorys und ihre Verwendung im gesamten Leitfaden wurden geklärt.	18. Juli 2022
Leitfaden zusammenführen	Die beiden separaten Administrator- und Benutzerhandbücher wurden in einem einzigen Handbuch, dem AWS ProtonBenutzerhandbuch, zusammengefasst.	30. Juni 2022
Aktualisierung der verwalteten Richtlinien	Die verwalteten Richtlinien wurden aktualisiert, um Zugriff auf neue AWS Proton API-Operationen zu gewähren und Berechtigungsprobleme für einige AWS Proton Konsolenoperationen zu beheben. Siehe AWSverwaltete Richtlinien für AWS Proton.	20. Juni 2022

Erste Schritte Schritte Schritte Schritte Schritte Schritte Schritte Schritte Schritte Schritte Schritte Schritte	Aktualisiert Erste Schritte mit dem AWS CLI mit einem neuen Tutorial, das die neue Vorlagenbibliothek verwendet.	14. Juni 2022
Direkt definierte Komponenten	Das Kapitel „Komponenten“ wurde hinzugefügt und im gesamten Handbuch wurden entsprechende Änderungen vorgenommen.	1. Juni 2022
AWS ProtonVorlagenbibliothek	Das Thema Die AWS Proton Vorlagenbibliothek wurde hinzugefügt.	6. Mai 2022
Allgemeine Verfügbarkeit von Terraform (GA)	Pull-Request-Bereitstellung wurde in Self-Managed Provisioning umbenannt. Das Thema Bereitstellungsmethoden wurde hinzugefügt.	23. März 2022
Tagging im Repositorium	Unterstützung für das Taggen von Repository-Ressourcen hinzugefügt. Siehe Einen Link zu deinem Repository erstellen .	23. März 2022
Aktualisierung der Dokumentation	Das Tagging von Umgebungskontoverbindungen wurde hinzugefügt.	26. November 2021

Vorlagensynchronisierung und Terraform-Vorschau	Automatisierte Vorlagenversionierung mit der Funktion zur Vorlagensynchronisierung für allgemeine Verfügbarkeit und Pull-Request-Bereitstellung mit Terraform in der Vorschau hinzugefügt. API-Migrationsleitfaden wieder da.	24. November 2021
Aktualisierungen der Dokumentation	Verbesserungen in den Abschnitten EventBridgeTutorial, Arbeitsablauf Erste Schritte, AWS ProtonFunktionsweise und Vorlagenpaket hinzugefügt.	17. September 2021
AWS ProtonVeröffentlichung der Konsolen-Hilfetafeln	Der Konsole wurden hinzugefügt. Durch das Löschen der Konsolenvorlagenversion werden keine niedrigeren Versionen mehr gelöscht. Der -Entwicklerhandbuch wurde entfernt.	8. September 2021
AWS ProtonVersion für allgemeine Verfügbarkeit (GA)	Es wurden kontoübergreifende Umgebungen, EventBridgeÜberwachung, IAM-Bedingungsschlüssel, IDEMpotenzunterstützung und erhöhte Kontingente hinzugefügt.	9. Juni 2021

Fügen Sie Dienstinstanzen für einen Dienst hinzu und löschen Sie sie und verwenden Sie die vorhandene externe Infrastruktur für Umgebungen mit AWS Proton	Diese öffentliche Vorschauversion enthält Updates, die es Ihnen ermöglichen, Service-Instances zu einem Service hinzuzufügen und zu löschen, Ihre bestehende externe Infrastruktur in einer AWS Proton Umgebung zu verwenden und Umgebungen, Dienstinstanzen und Pipeline-Bereitstellungen zu stornieren. AWS Protonunterstützt jetzt PrivateLink. Eine zusätzliche Löschvalidierung wurde hinzugefügt, um zu verhindern, dass eine Nebenversion versehentlich gelöscht wird, während eine Ressource sie verwendet.	27. April 2021
Taggen mit AWS Proton	Die öffentliche Vorschauversion 2 beinhaltet AWS Proton Tagging und die Möglichkeit, Dienste ohne eine Service-Pipeline zu starten.	5. März 2021
Erstversion	Die öffentliche Vorschauversion ist jetzt in ausgewählten Regionen verfügbar.	1. Dezember 2020

AWS-Glossar

Die neueste AWS-Terminologie finden Sie im AWS-Glossar in der AWS-Glossar-Referenz.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.