Benutzerhandbuch

AWS Deadline Cloud

Version latest

AWS Deadline Cloud: Benutzerhandbuch

Table of Contents

Was ist AWS Deadline Cloud?

Mit Deadline Cloud können AWS-Service Sie Rendering-Projekte und -Jobs auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances direkt von Pipelines und Workstations aus zur Erstellung digitaler Inhalte erstellen und verwalten.

Deadline Cloud bietet Konsolenschnittstellen, lokale Anwendungen, Befehlszeilentools und eine API. Mit Deadline Cloud können Sie Farmen, Flotten, Jobs, Benutzergruppen und Speicher erstellen, verwalten und überwachen. Sie können auch Hardwarefunktionen spezifizieren, Umgebungen für bestimmte Workloads erstellen und die Tools zur Inhaltserstellung, die für Ihre Produktion erforderlich sind, in Ihre Deadline Cloud-Pipeline integrieren.

Deadline Cloud bietet eine einheitliche Oberfläche, über die Sie all Ihre Rendering-Projekte an einem Ort verwalten können. Sie können Benutzer verwalten, ihnen Projekte zuweisen und Berechtigungen für Jobrollen erteilen.

Themen

Funktionen von Deadline Cloud

Hier sind einige der wichtigsten Möglichkeiten, wie Deadline Cloud Ihnen bei der Ausführung und Verwaltung von Visual Computing-Workloads helfen kann:

- Erstellen Sie schnell Ihre Farmen, Warteschlangen und Flotten. Überwachen Sie ihren Status und gewinnen Sie Einblicke in den Betrieb Ihrer Farm und Ihre Jobs.
- Verwalten Sie Deadline Cloud-Benutzer und -Gruppen zentral und weisen Sie Berechtigungen zu.
- Verwalten Sie die Anmeldesicherheit für Projektbenutzer und externe Identitätsanbieter mit AWS IAM Identity Center.

- Verwalten Sie den Zugriff auf Projektressourcen sicher mit AWS Identity and Access Management (IAM-) Richtlinien und Rollen.
- Verwenden Sie Tags, um Projektressourcen zu organisieren und schnell zu finden.
- Verwalten Sie die Nutzung der Projektressourcen und die geschätzten Kosten für Ihr Projekt.
- Stellen Sie eine breite Palette von Rechenverwaltungsoptionen bereit, um das Rendern in der Cloud oder persönlich zu unterstützen.

Konzepte und Terminologie für Deadline Cloud

Um Ihnen den Einstieg in AWS Deadline Cloud zu erleichtern, werden in diesem Thema einige der wichtigsten Konzepte und Begrifflichkeiten erläutert.

Budgetmanager

: Der Budgetmanager ist Teil des Deadline Cloud-Monitors. Verwenden Sie den Budgetmanager, um Budgets zu erstellen und zu verwalten. Sie können ihn auch verwenden, um Aktivitäten einzuschränken, um das Budget einzuhalten.

Deadline Cloud-Kundenbibliothek

: Die Client Library umfasst eine Befehlszeilenschnittstelle und eine Bibliothek zur Verwaltung von Deadline Cloud. Zu den Funktionen gehören das Senden von Jobpaketen auf der Grundlage der Open Job Description-Spezifikation an Deadline Cloud, das Herunterladen von Ausgaben für Jobanhänge und die Überwachung Ihrer Farm über die Befehlszeilenschnittstelle.

Anwendung zur Erstellung digitaler Inhalte (DCC)

: Anwendungen zur Erstellung digitaler Inhalte (DCCs) sind Produkte von Drittanbietern, mit denen Sie digitale Inhalte erstellen. Beispiele für DCCs sind Maya, Nuke, und Houdini. Deadline Cloud bietet integrierte Plugins für Stellenabsender für bestimmte Bereiche. DCCs

Farm

: Eine Farm ist ein Ort, an dem sich Ihre Projektressourcen befinden. Sie besteht aus Warteschlangen und Flotten.

Flotte

: Eine Flotte ist eine Gruppe von Worker-Knoten, die das Rendern durchführen. Worker-Knoten verarbeiten Jobs. Eine Flotte kann mehreren Warteschlangen zugeordnet werden, und eine Warteschlange kann mehreren Flotten zugeordnet werden.

Aufgabe

Ein Job ist eine Rendering-Anfrage. Benutzer reichen Jobs ein. Jobs enthalten spezifische Jobeigenschaften, die als Schritte und Aufgaben beschrieben werden.

Arbeitsanhänge

Ein Jobanhang ist eine Deadline Cloud-Funktion, mit der Sie Eingaben und Ausgaben für Jobs verwalten können. Auftragsdateien werden während des Rendervorgangs als Auftragsanhänge hochgeladen. Bei diesen Dateien kann es sich um Texturen, 3D-Modelle, Lichtanlagen und ähnliche Objekte handeln.

Priorität der Job

Die Auftragspriorität ist die ungefähre Reihenfolge, in der Deadline Cloud einen Job in einer Warteschlange verarbeitet. Sie können die Job-Priorität zwischen 1 und 100 festlegen. Jobs mit einer höheren Priorität werden in der Regel zuerst verarbeitet. Jobs mit derselben Priorität werden in der Reihenfolge bearbeitet, in der sie eingegangen sind.

Auftragseigenschaften

Auftragseigenschaften sind Einstellungen, die Sie beim Absenden eines Renderjobs definieren. Einige Beispiele umfassen den Bildbereich, den Ausgabepfad, Auftragsanhänge, renderfähige Kamera und mehr. Die Eigenschaften variieren je nach dem DCC, von dem das Rendering eingereicht wurde.

Auftragsvorlage

Eine Jobvorlage definiert die Laufzeitumgebung und alle Prozesse, die als Teil eines Deadline Cloud-Jobs ausgeführt werden.

Warteschlange

In einer Warteschlange befinden sich eingereichte Jobs und deren Rendern ist geplant.
Eine Warteschlange muss einer Flotte zugeordnet werden, um ein erfolgreiches Rendern zu ermöglichen. Eine Warteschlange kann mehreren Flotten zugeordnet werden.

Zuordnung zwischen Warteschlange und Flotte

Wenn eine Warteschlange einer Flotte zugeordnet ist, liegt eine Zuordnung zwischen Warteschlange und Flotte vor. Verwenden Sie eine Zuordnung, um Mitarbeitern aus einer Flotte Aufträge in dieser Warteschlange zuzuordnen. Sie können Zuordnungen starten und beenden, um die Arbeitsplanung zu steuern.

Schritt

Ein Schritt ist ein bestimmter Prozess, der im Job ausgeführt werden soll.

Frist für den Cloud-Einreicher

Ein Deadline Cloud-Einreicher ist ein DCC-Plugin (Digital Content Creation). Künstler verwenden es, um Jobs über eine DCC-Schnittstelle eines Drittanbieters einzureichen, mit der sie vertraut sind.

Tags

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen können. Jedes Tag besteht aus einem Schlüssel und einem optionalen Wert, den Sie definieren.

Mit Tags können Sie Ihre AWS Ressourcen auf unterschiedliche Weise kategorisieren. Sie könnten beispielsweise eine Reihe von Tags für die EC2 Amazon-Instances Ihres Kontos definieren, mit deren Hilfe Sie den Besitzer und die Stack-Ebene jeder Instance verfolgen können.

Sie können Ihre AWS Ressourcen auch nach Zweck, Eigentümer oder Umgebung kategorisieren. Dieser Ansatz ist nützlich, wenn Sie über viele Ressourcen desselben Typs verfügen. Anhand der Tags, die Sie ihr zugewiesen haben, können Sie eine bestimmte Ressource schnell identifizieren.

Aufgabe

Eine Aufgabe ist eine einzelne Komponente eines Renderschritts.

Nutzungsbasierte Lizenzierung (UBL)

Die nutzungsbasierte Lizenzierung (UBL) ist ein On-Demand-Lizenzmodell, das für ausgewählte Produkte von Drittanbietern verfügbar ist. Bei diesem Modell handelt es sich um eine nutzungsabhängige Bezahlung, bei der Ihnen die Anzahl der Stunden und Minuten in Rechnung gestellt wird, die Sie nutzen.

Nutzungsexplorer

Der Usage Explorer ist eine Funktion von Deadline Cloud Monitor. Er bietet eine ungefähre Schätzung Ihrer Kosten und Nutzung.

Worker

Mitarbeiter gehören zu Flotten und führen die von Deadline Cloud zugewiesenen Aufgaben aus, um Schritte und Aufträge zu erledigen. Mitarbeiter speichern die Protokolle von Aufgabenvorgängen in Amazon CloudWatch Logs. Mitarbeiter können auch die Funktion für

Jobanhänge verwenden, um Eingaben und Ausgaben mit einem Amazon Simple Storage Service (Amazon S3) -Bucket zu synchronisieren.

Erste Schritte mit Deadline Cloud

Verwenden Sie Deadline Cloud, um schnell eine Renderfarm mit Standardeinstellungen und Ressourcen wie der EC2 Amazon-Instanzkonfiguration und Amazon Simple Storage Service (Amazon S3) -Buckets zu erstellen.

Sie können die Einstellungen und Ressourcen auch definieren, wenn Sie eine Renderfarm erstellen. Diese Methode nimmt mehr Zeit in Anspruch als die Verwendung der Standardeinstellungen und Ressourcen, bietet Ihnen jedoch mehr Kontrolle.

Nachdem Sie sich mit den Konzepten und der Terminologie von Deadline Cloud vertraut gemacht haben, finden Sie unter Erste Schritte step-by-step Anweisungen zum Erstellen Ihrer Farm, zum Hinzufügen von Benutzern und Links zu hilfreichen Informationen.

Zugreifen auf Deadline Cloud

Sie können auf eine der folgenden Arten auf Deadline Cloud zugreifen:

- Deadline Cloud-Konsole — Greifen Sie in einem Browser auf die Konsole zu, um eine Farm und ihre Ressourcen zu erstellen und den Benutzerzugriff zu verwalten. Weitere Informationen finden Sie unter Erste Schritte.
- Deadline Cloud Monitor — Verwalten Sie Ihre Renderjobs, einschließlich der Aktualisierung von Prioritäten und Jobstatus. Überwachen Sie Ihre Farm und sehen Sie sich Protokolle und den Auftragsstatus an. Für Benutzer mit Inhaberberechtigungen bietet der Deadline Cloud-Monitor auch Zugriff darauf, die Nutzung zu untersuchen und Budgets zu erstellen. Der Deadline Cloud-Monitor ist sowohl als Webbrowser als auch als Desktop-Anwendung verfügbar.
- AWS SDK und AWS CLI — Verwenden Sie AWS Command Line Interface (AWS CLI), um die Deadline Cloud-API-Operationen von der Befehlszeile auf Ihrem lokalen System aus aufzurufen. Weitere Informationen finden Sie unter Eine Entwickler-Workstation einrichten.

Zugehörige Services

Deadline Cloud funktioniert mit den folgenden Komponenten AWS-Services:

- Amazon CloudWatch — Mit CloudWatch können Sie Ihre Projekte und die zugehörigen AWS Ressourcen überwachen. Weitere Informationen finden Sie unter Monitoring with CloudWatch im Deadline Cloud Developer Guide.
- Amazon EC2 — Dies AWS-Service bietet virtuelle Server, auf denen Ihre Anwendungen in der Cloud ausgeführt werden. Sie können Ihre Projekte so konfigurieren, dass EC2 Amazon-Instances für Ihre Workloads verwendet werden. Weitere Informationen finden Sie unter EC2 Amazon-Instances.
- Amazon EC2 Auto Scaling — Mit Auto Scaling können Sie die Anzahl der Instances automatisch erhöhen oder verringern, wenn sich die Nachfrage nach Ihren Instances ändert. Auto Scaling hilft sicherzustellen, dass Sie die gewünschte Anzahl von Instances ausführen, auch wenn eine Instance ausfällt. Wenn Sie Auto Scaling mit Deadline Cloud aktivieren, werden Instances, die von Auto Scaling gestartet werden, automatisch beim Workload registriert. Ebenso werden Instances, die durch Auto Scaling beendet wurden, automatisch vom Workload abgemeldet. Weitere Informationen finden Sie im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.
- AWS PrivateLink— AWS PrivateLink bietet private Konnektivität zwischen virtuellen privaten Clouds (VPCs) und Ihren lokalen Netzwerken, ohne dass Ihr Datenverkehr dem öffentlichen Internet ausgesetzt wird. AWS-Services AWS PrivateLink macht es einfach, Dienste über verschiedene Konten hinweg zu verbinden und. VPCs Weitere Informationen finden Sie unter AWS PrivateLink.
- Amazon S3 — Amazon S3 ist ein Objektspeicherservice. Deadline Cloud verwendet Amazon S3 S3-Buckets zum Speichern von Job-Anhängen. Weitere Informationen finden Sie im Amazon S3 S3-Benutzerhandbuch.
- IAM Identity Center — Im IAM Identity Center können Sie Benutzern von einem zentralen AWS-Service Ort aus Single-Sign-On-Zugriff auf alle ihnen zugewiesenen Konten und Anwendungen gewähren. Sie können den Zugriff mehrerer Konten und die Benutzerberechtigungen für alle Ihre Konten auch zentral verwalten. AWS Organizations Weitere Informationen finden Sie unter AWS IAM Identity Center FAQs.

So funktioniert Deadline Cloud

Mit Deadline Cloud können Sie Rendering-Projekte und -Jobs direkt über Pipelines und Workstations zur Erstellung digitaler Inhalte (DCC) erstellen und verwalten.

Sie reichen Jobs mit dem AWS SDK, AWS Command Line Interface (AWS CLI) oder den Deadline Cloud-Job-Einreichern an Deadline Cloud ein. Deadline Cloud unterstützt die Open Job

Description (OpenJD) für die Spezifikation von Jobvorlagen. Weitere Informationen finden Sie unter Stellenbeschreibung öffnen auf der GitHub Webseite.

Deadline Cloud bietet Stelleneinreicher. Ein Job Submitter ist ein DCC-Plugin zum Senden von Renderjobs über eine DCC-Schnittstelle eines Drittanbieters, wie z. B. Maya or Nuke. Mit einem Einreicher können Künstler Renderaufträge über eine Schnittstelle eines Drittanbieters an Deadline Cloud einreichen, wo Projektressourcen verwaltet und Jobs überwacht werden — alles von einem Ort aus.

Mit einer Deadline Cloud-Farm können Sie Warteschlangen und Flotten erstellen, Benutzer verwalten und die Nutzung und Kosten von Projektressourcen verwalten. Eine Farm besteht aus Warteschlangen und Flotten. In einer Warteschlange befinden sich eingereichte Jobs, deren Rendern geplant ist. Eine Flotte ist eine Gruppe von Worker-Knoten, die Aufgaben ausführen, um Jobs abzuschließen. Eine Warteschlange muss einer Flotte zugeordnet werden, damit die Jobs gerendert werden können. Eine einzelne Flotte kann mehrere Warteschlangen unterstützen, und eine Warteschlange kann von mehreren Flotten unterstützt werden.

Jobs bestehen aus Schritten, und jeder Schritt besteht aus bestimmten Aufgaben. Mit dem Deadline Cloud-Monitor können Sie auf Status, Protokolle und andere Kennzahlen zur Fehlerbehebung für Jobs, Schritte und Aufgaben zugreifen.

Berechtigungen in Deadline Cloud

Deadline Cloud unterstützt Folgendes:

- Verwaltung des Zugriffs auf seine API-Operationen mithilfe von AWS Identity and Access Management (IAM)
- Verwaltung des Zugriffs von Workforce-Benutzern mithilfe einer Integration mit AWS IAM Identity Center

Bevor jemand an einem Projekt arbeiten kann, muss er Zugriff auf dieses Projekt und die zugehörige Farm haben. Deadline Cloud ist in IAM Identity Center integriert, um die Authentifizierung und Autorisierung von Mitarbeitern zu verwalten. Benutzer können direkt zu IAM Identity Center hinzugefügt werden, oder die Berechtigungen können mit Ihrem vorhandenen Identitätsanbieter (IdP) verknüpft werden, z. B. Okta or Active Directory. IT-Administratoren können Benutzern und Gruppen auf verschiedenen Ebenen Zugriffsberechtigungen gewähren. Jede nachfolgende Ebene umfasst die Berechtigungen für die vorherigen Ebenen. In der folgenden Liste werden die vier Zugriffsebenen von der niedrigsten bis zur höchsten Ebene beschrieben:

- Zuschauer — Berechtigung zum Anzeigen von Ressourcen in den Farmen, Warteschlangen, Flotten und Aufträgen, auf die sie Zugriff haben. Ein Zuschauer kann keine Jobs einreichen oder Änderungen daran vornehmen.
- Mitwirkender — Identisch mit einem Betrachter, aber mit der Erlaubnis, Jobs an eine Warteschlange oder Farm zu senden.
- Manager — Identisch mit dem Mitwirkenden, aber mit der Berechtigung, Jobs in Warteschlangen zu bearbeiten, auf die er Zugriff hat, und Berechtigungen für Ressourcen zu erteilen, auf die er Zugriff hat.
- Besitzer — Identisch mit dem Manager, kann jedoch Budgets anzeigen und erstellen und deren Nutzung einsehen.

> **Note**
>
> Diese Berechtigungen gewähren Benutzern keinen Zugriff auf die Deadline Cloud-Infrastruktur AWS Management Console oder die Erlaubnis, sie zu ändern.

Benutzer müssen Zugriff auf eine Farm haben, bevor sie auf die zugehörigen Warteschlangen und Flotten zugreifen können. Der Benutzerzugriff wird Warteschlangen und Flotten innerhalb einer Farm separat zugewiesen.

Sie können Benutzer als Einzelpersonen oder als Teil einer Gruppe hinzufügen. Das Hinzufügen von Gruppen zu einer Farm, Flotte oder Warteschlange kann die Verwaltung von Zugriffsberechtigungen für große Personengruppen vereinfachen. Wenn Sie beispielsweise ein Team haben, das an einem bestimmten Projekt arbeitet, können Sie jedes Teammitglied zu einer Gruppe hinzufügen. Anschließend können Sie der gesamten Gruppe Zugriffsberechtigungen für die entsprechende Farm, Flotte oder Warteschlange gewähren.

Softwareunterstützung mit Deadline Cloud

Deadline Cloud funktioniert mit jeder Softwareanwendung, die über eine Befehlszeilenschnittstelle ausgeführt und mithilfe von Parameterwerten gesteuert werden kann. Deadline Cloud unterstützt die OpenJD Spezifikation zur Beschreibung von Arbeit als Jobs mit Softwareskriptschritten, die zu Aufgaben parametrisiert sind (z. B. über einen Frame-Bereich). Zusammenbauen OpenJD Auftragsanweisungen zu Auftragspaketen mit Tools und Funktionen von Deadline Cloud zum Erstellen, Ausführen und Lizenzieren der Schritte aus einer Softwareanwendung eines Drittanbieters.

Zum Rendern von Jobs ist eine Lizenz erforderlich. Deadline Cloud bietet usage-based-licensing (UBL) eine Auswahl von Lizenzen für Softwareanwendungen an, die je nach Nutzung stundenweise in Minutenschritten abgerechnet werden. Mit Deadline Cloud können Sie auch Ihre eigenen Softwarelizenzen verwenden, wenn Sie möchten. Wenn ein Job nicht auf eine Lizenz zugreifen kann, wird er nicht gerendert und es wird ein Fehler ausgegeben, der im Aufgabenprotokoll im Deadline Cloud-Monitor angezeigt wird.

Erste Schritte mit Deadline Cloud

Um eine Farm in AWS Deadline Cloud zu erstellen, können Sie entweder die Deadline Cloud-Konsole oder die AWS Command Line Interface (AWS CLI) verwenden. Verwenden Sie die Konsole für eine geführte Erfahrung bei der Erstellung der Farm, einschließlich Warteschlangen und Flotten. Verwenden Sie den AWS CLI , um direkt mit dem Service zu arbeiten oder um Ihre eigenen Tools zu entwickeln, die mit Deadline Cloud funktionieren.

Um eine Farm zu erstellen und den Deadline Cloud-Monitor zu verwenden, richten Sie Ihr Konto für Deadline Cloud ein. Sie müssen die Deadline Cloud-Monitor-Infrastruktur nur einmal pro Konto einrichten. Von Ihrer Farm aus können Sie Ihr Projekt verwalten, einschließlich des Benutzerzugriffs auf Ihre Farm und ihre Ressourcen.

Um eine Farm zu erstellen, ohne die Deadline Cloud-Monitorinfrastruktur einzurichten, richten Sie eine Entwickler-Workstation für Deadline Cloud ein.

Um eine Farm mit minimalen Ressourcen für die Annahme von Jobs zu erstellen, wählen Sie auf der Startseite der Konsole Schnellstart aus. Richten Sie den Deadline Cloud-Monitor einführt Sie durch diese Schritte. Diese Farmen beginnen mit einer Warteschlange und einer Flotte, die automatisch zugeordnet werden. Dieser Ansatz ist eine bequeme Möglichkeit, Farmen im Sandbox-Stil zum Experimentieren zu erstellen.

Themen

Richten Sie Ihre ein AWS-Konto

Richten Sie Ihre AWS-Konto AWS Deadline Cloud ein.

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

Um sich für eine anzumelden AWS-Konto

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

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

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

Wenn Sie zum ersten Mal eine erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben.

Important

Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, 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.

Richten Sie den Deadline Cloud-Monitor ein

Um zu beginnen, müssen Sie Ihre Deadline Cloud-Monitor-Infrastruktur erstellen und Ihre Farm definieren. Sie können auch zusätzliche, optionale Schritte ausführen, darunter das Hinzufügen von Gruppen und Benutzern, die Auswahl einer Servicerolle und das Hinzufügen von Tags zu Ihren Ressourcen.

Schritt 1: Erstellen Sie Ihren Monitor

Der Deadline Cloud-Monitor wird verwendet AWS IAM Identity Center , um Benutzer zu autorisieren. Die IAM Identity Center-Instanz, die Sie für Deadline Cloud verwenden, muss sich in derselben Konfiguration AWS-Region wie der Monitor befinden. Wenn Ihre Konsole bei der Erstellung des Monitors eine andere Region verwendet, werden Sie daran erinnert, zur IAM Identity Center-Region zu wechseln.

Die Infrastruktur Ihres Monitors besteht aus den folgenden Komponenten:

- Monitor-Anzeigename: Anhand des Monitor-Anzeigenamens können Sie Ihren Monitor identifizieren, z. B. AnyCompany Monitor. Der Name Ihres Monitors bestimmt auch Ihre Monitor-URL.

  > **Important**
  >
  > Sie können den Anzeigenamen des Monitors nicht mehr ändern, nachdem Sie die Einrichtung abgeschlossen haben.

- Monitor-URL: Sie können über die Monitor-URL auf Ihren Monitor zugreifen. Die URL basiert auf dem Anzeigenamen des Monitors — zum Beispiel https://anycompanymonitor.awsapps.com.

  > **Important**
  >
  > Sie können die Monitor-URL nicht ändern, nachdem Sie die Einrichtung abgeschlossen haben.

- AWS-Region: Das AWS-Regionist der physische Standort für eine Sammlung von AWS Rechenzentren. Wenn Sie Ihren Monitor einrichten, wird als Region standardmäßig der Standort ausgewählt, der Ihnen am nächsten liegt. Wir empfehlen, die Region so zu ändern, dass sie Ihren Benutzern am nächsten ist. Dies reduziert die Verzögerung und verbessert die Datenübertragungsgeschwindigkeit. AWS IAM Identity Center muss genauso AWS-Region wie Deadline Cloud aktiviert sein.

  > **Important**
  >
  > Sie können Ihre Region nicht ändern, nachdem Sie die Einrichtung von Deadline Cloud abgeschlossen haben.

Führen Sie die Aufgaben in diesem Abschnitt aus, um die Infrastruktur Ihres Monitors zu konfigurieren.

Um die Infrastruktur Ihres Monitors zu konfigurieren

1. Melden Sie sich bei der an AWS Management Console, um das Welcome to Deadline Cloud-Setup zu starten, und wählen Sie dann Weiter.

2. Geben Sie zum Beispiel den Anzeigenamen des Monitors ein**`AnyCompany Monitor`**.
3. (Optional) Um den Monitornamen zu ändern, wählen Sie „URL bearbeiten“.
4. (Optional) Um den AWS-Regionso zu ändern, dass er Ihren Benutzern am nächsten kommt, wählen Sie „Region ändern“.

   a. Wählen Sie die Region aus, die Ihren Benutzern am nächsten ist.

   b. Wählen Sie „Region anwenden“.

   - (Optional) Um Gruppen und Benutzer hinzuzufügen, wählen Sie (Optional) Fügen Sie Gruppen und Benutzer hinzu.
   - (Optional) Um Ihre Monitoreinstellung weiter anzupassen, wählen Sie Zusätzliche Einstellungen.
5. Wenn Sie dazu bereit sind Schritt 2: Definieren Sie die Farmdetails, wählen Sie Weiter.

(Optional) Fügen Sie Gruppen und Benutzer hinzu

Bevor Sie die Einrichtung des Deadline Cloud-Monitors abschließen, können Sie Monitor-Benutzer hinzufügen und sie einer Gruppe hinzufügen.

Nach Abschluss der Einrichtung können Sie neue Benutzer und Gruppen erstellen und Benutzer verwalten, um ihnen beispielsweise Gruppen, Berechtigungen und Anwendungen zuzuweisen oder Benutzer von Ihrem Monitor zu löschen.

Zusätzliche Einstellungen

Die Einrichtung von Deadline Cloud umfasst zusätzliche Einstellungen. Mit diesen Einstellungen können Sie alle Änderungen einsehen, die das Deadline Cloud-Setup an Ihnen vornimmt AWS-Konto, Ihre Monitor-Benutzerrolle konfigurieren und den Typ Ihres Verschlüsselungsschlüssels ändern.

AWS IAM Identity Center

AWS IAM Identity Center ist ein cloudbasierter Single-Sign-On-Service zur Verwaltung von Benutzern und Gruppen. IAM Identity Center kann auch in den Single Sign-On (SSO) -Anbieter Ihres Unternehmens integriert werden, sodass sich Benutzer mit ihrem Unternehmenskonto anmelden können.

Deadline Cloud aktiviert IAM Identity Center standardmäßig und ist für die Einrichtung und Verwendung von Deadline Cloud erforderlich. Die IAM Identity Center-Instanz, die Sie für Deadline Cloud verwenden, muss sich in derselben Umgebung AWS-Region wie der Monitor befinden. Weitere Informationen finden Sie unter Was ist AWS IAM Identity Center.

Konfigurieren Sie die Dienstzugriffsrolle

Ein AWS Dienst kann eine Servicerolle übernehmen, um Aktionen in Ihrem Namen auszuführen. Deadline Cloud benötigt eine Monitor-Benutzerrolle, damit Benutzer auf Ressourcen in Ihrem Monitor zugreifen können.

Sie können verwaltete AWS Identity and Access Management (IAM) -Richtlinien an die Benutzerrolle „Monitor“ anhängen. Die Richtlinien gewähren Benutzern die Erlaubnis, bestimmte Aktionen auszuführen, z. B. das Erstellen von Jobs in einer bestimmten Deadline Cloud-Anwendung. Da Anwendungen von bestimmten Bedingungen in der verwalteten Richtlinie abhängen, funktioniert die Anwendung möglicherweise nicht wie erwartet, wenn Sie die verwalteten Richtlinien nicht verwenden.

Sie können die Rolle des Monitor-Benutzers nach Abschluss der Installation jederzeit ändern. Weitere Informationen zu Benutzerrollen finden Sie unter IAM-Rollen.

Die folgenden Registerkarten enthalten Anweisungen für zwei verschiedene Anwendungsfälle. Um eine neue Servicerolle zu erstellen und zu verwenden, wählen Sie die Registerkarte Neue Servicerolle. Um eine bestehende Servicerolle zu verwenden, wählen Sie die Registerkarte Bestehende Servicerolle.

New service role

Um eine neue Servicerolle zu erstellen und zu verwenden

1. Wählen Sie Neue Servicerolle erstellen und verwenden aus.
2. (Optional) Geben Sie einen Namen für die Dienstbenutzerrolle ein.
3. Wählen Sie Berechtigungsdetails anzeigen aus, um weitere Informationen zur Rolle zu erhalten.

Existing service role

Um eine bestehende Servicerolle zu verwenden

1. Wählen Sie Bestehende Servicerolle verwenden aus.

2. Öffnen Sie die Dropdownliste, um eine bestehende Servicerolle auszuwählen.
3. (Optional) Wählen Sie In der IAM-Konsole anzeigen aus, um weitere Informationen zur Rolle zu erhalten.

Schritt 2: Definieren Sie die Farmdetails

Gehen Sie zurück zur Deadline Cloud-Konsole und führen Sie die folgenden Schritte aus, um die Farmdetails zu definieren.

1. Fügen Sie in den Farmdetails einen Namen für die Farm hinzu.
2. Geben Sie unter Beschreibung die Farmbeschreibung ein. Eine klare Beschreibung kann Ihnen helfen, den Zweck Ihrer Farm schnell zu ermitteln.
3. (Optional) Standardmäßig werden Ihre Daten mit einem Schlüssel verschlüsselt, der zu Ihrer eigenen Sicherheit AWS gehört und verwaltet wird. Sie können Verschlüsselungseinstellungen anpassen (erweitert) wählen, um einen vorhandenen Schlüssel zu verwenden oder einen neuen, von Ihnen verwalteten Schlüssel zu erstellen.

   Wenn Sie die Verschlüsselungseinstellungen über das Kontrollkästchen anpassen möchten, geben Sie einen AWS KMS ARN ein oder erstellen Sie einen neuen, AWS KMS indem Sie Neuen KMS-Schlüssel erstellen wählen.
4. (Optional) Wählen Sie Neues Tag hinzufügen aus, um Ihrer Farm ein oder mehrere Tags hinzuzufügen.
5. Wählen Sie eine der folgenden Optionen:

   - Wählen Sie „Zur Überprüfung springen“ und „Erstellen“, um Ihre Farm zu überprüfen und zu erstellen.
   - Wählen Sie Weiter aus, um mit weiteren optionalen Schritten fortzufahren.

(Optional) Schritt 3: Definieren Sie die Warteschlangendetails

Die Warteschlange ist dafür verantwortlich, den Fortschritt zu verfolgen und die Arbeit für Ihre Jobs zu planen.

1. Geben Sie zunächst in den Warteschlangendetails einen Namen für die Warteschlange ein.
2. Geben Sie unter Beschreibung die Beschreibung der Warteschlange ein. Eine klare Beschreibung kann Ihnen helfen, den Zweck Ihrer Warteschlange schnell zu identifizieren.

3. Für Job-Anhänge können Sie entweder einen neuen Amazon S3 S3-Bucket erstellen oder einen vorhandenen Amazon S3 S3-Bucket auswählen. Wenn Sie noch keinen Amazon S3 S3-Bucket haben, müssen Sie einen erstellen.

    a. Um einen neuen Amazon S3 S3-Bucket zu erstellen, wählen Sie Neuen Job-Bucket erstellen. Sie können den Namen des Job-Buckets im Feld Root-Präfix definieren. Wir empfehlen, den Bucket aufzurufen**`deadlinecloud-job-attachments-[MONITORNAME]`**.

        Sie können nur Kleinbuchstaben und Bindestriche verwenden. Keine Leerzeichen oder Sonderzeichen.

    b. Um nach einem vorhandenen Amazon S3 S3-Bucket zu suchen und diesen auszuwählen, wählen Sie Aus vorhandenem Amazon S3 S3-Bucket auswählen. Suchen Sie anschließend nach einem vorhandenen Bucket, indem Sie „S3 durchsuchen“ wählen. Wenn die Liste Ihrer verfügbaren Amazon S3 S3-Buckets angezeigt wird, wählen Sie den Amazon S3 S3-Bucket aus, den Sie für Ihre Warteschlange verwenden möchten.

4. Wenn Sie vom Kunden verwaltete Flotten verwenden, wählen Sie Zuordnung zu kundenverwalteten Flotten aktivieren aus.

    - Fügen Sie für vom Kunden verwaltete Flotten einen für die Warteschlange konfigurierten Benutzer hinzu und legen Sie dann die POSIX- und/oder Windows-Anmeldeinformationen fest. Alternativ können Sie die Run-As-Funktionalität umgehen, indem Sie das Kontrollkästchen aktivieren.

5. Ihre Warteschlange benötigt die Erlaubnis, in Ihrem Namen auf Amazon S3 zuzugreifen. Wir empfehlen Ihnen, für jede Warteschlange eine neue Servicerolle zu erstellen.

    a. Führen Sie für eine neue Rolle die folgenden Schritte aus.

        i. Wählen Sie Neue Servicerolle erstellen und verwenden aus.

        ii. Geben Sie einen Rollennamen für Ihre Warteschlangenrolle ein oder verwenden Sie den angegebenen Rollennamen.

        iii. (Optional) Fügen Sie eine Beschreibung der Warteschlangenrolle hinzu.

        iv. Sie können die IAM-Berechtigungen für die Warteschlangenrolle anzeigen, indem Sie Berechtigungsdetails anzeigen wählen.

    b. Alternativ können Sie eine vorhandene Servicerolle auswählen.

6. (Optional) Fügen Sie mithilfe von Namens- und Wertepaaren Umgebungsvariablen für die Warteschlangenumgebung hinzu.

7. (Optional) Fügen Sie mithilfe von Schlüssel- und Wertepaaren Tags für die Warteschlange hinzu.

Nachdem Sie alle Warteschlangendetails eingegeben haben, wählen Sie Weiter.

(Optional) Schritt 4: Definieren Sie Flottendetails

Eine Flotte weist Mitarbeiter zu, die Ihre Rendering-Aufgaben ausführen. Wenn Sie eine Flotte für Ihre Renderaufgaben benötigen, aktivieren Sie das Kontrollkästchen Flotte erstellen.

1. Einzelheiten zur Flotte

   a. Geben Sie sowohl einen Namen als auch eine optionale Beschreibung für Ihre Flotte an.

   b. Wählen Sie aus, wie Ihre Rechenressourcen skaliert werden sollen. Mit der Option Service-Managed kann Deadline Cloud Ihre Rechenressourcen auto skalieren. Bei der vom Kunden verwalteten Option haben Sie die Kontrolle über Ihre eigene Rechenskalierung.

2. Wählen Sie im Abschnitt Instanzoption entweder Spot oder On-Demand aus. Amazon EC2 On-Demand-Instances bieten eine schnellere Verfügbarkeit und Amazon EC2 Spot-Instances eignen sich besser zur Kosteneinsparung.

3. Wählen Sie für die automatische Skalierung der Anzahl der Instances in Ihrer Flotte sowohl eine Mindestanzahl von Instances als auch eine Maximale Anzahl von Instances.

   Wir empfehlen dringend, immer die Mindestanzahl an Instanzen festzulegen, **`0`** um zusätzliche Kosten zu vermeiden.

4. Ihre Flotte benötigt die Erlaubnis, in Ihrem Namen CloudWatch an Sie zu schreiben. Wir empfehlen Ihnen, für jede Flotte eine neue Servicerolle zu erstellen.

   a. Führen Sie für eine neue Rolle die folgenden Schritte aus.

      i. Wählen Sie Neue Servicerolle erstellen und verwenden aus.

      ii. Geben Sie einen Rollennamen für Ihre Flottenrolle ein oder verwenden Sie den angegebenen Rollennamen.

      iii. (Optional) Fügen Sie eine Beschreibung der Flottenrolle hinzu.

      iv. Um die IAM-Berechtigungen für die Flottenrolle anzuzeigen, wählen Sie Berechtigungsdetails anzeigen aus.

   b. Alternativ können Sie eine vorhandene Servicerolle verwenden.

5. (Optional) Fügen Sie mithilfe von Schlüssel- und Wertepaaren Tags für die Flotte hinzu.

Nachdem Sie alle Flottendetails eingegeben haben, wählen Sie Weiter.

(Optional) Schritt 5: Konfigurieren Sie die Fähigkeiten Ihrer Mitarbeiter

Definieren Sie die Funktionen für Ihre Worker-Instanzen.

1. Wählen Sie das Betriebssystem für die Mitarbeiter in Ihrer Flotte. Behalten Sie für dieses Tutorial die Standardeinstellung bei Linux.
2. Prüfen Sie die Einstellung für die CPU-Architektur auf Informationen.
3. Aktualisieren Sie die Mindest- und Höchstzahl von v CPUs für Ihre Hardwarefunktionen.
4. Aktualisieren Sie die minimale und maximale Speicheranzahl (GiB) für Ihre Hardwarefunktionen.
5. Sie können Instance-Typen filtern, indem Sie Typen von Worker-Instances entweder zulassen oder ausschließen. In beiden Filteroptionen können Sie bis zu 10 EC2 Amazon-Instance-Typen filtern.
6. Unter Zusätzliche Funktionen (optional) können Sie das EBS-Stammvolume nach Größe (GiB), IOPS und Durchsatz (MIB/s) definieren.
7. Nachdem alle Worker-Funktionen eingerichtet wurden, wählen Sie Weiter, um die Zugriffsebene Ihrer Gruppen zu definieren.

(Optional) Schritt 6: Definieren Sie Zugriffsebenen

Wenn Sie Gruppen mit Ihrem Monitor verbunden haben, können Sie deren Zugriffsebene definieren. Die Erlaubnis zur Nutzung der Funktionen von Deadline Cloud wird nach Zugriffsebenen verwaltet. Sie können Benutzergruppen unterschiedliche Zugriffsebenen zuweisen.

1. Verwenden Sie das Menü mit den Zugriffsebenen der Deadline Cloud-Farm, um die Berechtigungsstufe für die Gruppe auszuwählen.
2. Wählen Sie Weiter, um fortzufahren und alle eingegebenen Farmdetails zu überprüfen.

Schritt 7: Überprüfen und erstellen

Überprüfen Sie alle Informationen, die Sie zur Erstellung Ihrer Farm eingegeben haben. Wenn Sie bereit sind, wählen Sie Create Farm aus.

Der Fortschritt der Erstellung Ihrer Farm wird auf der Seite Farmen angezeigt. Eine Erfolgsmeldung wird angezeigt, wenn Ihre Farm betriebsbereit ist.

Deadline Cloud-Einreicher einrichten

Dieser Prozess richtet sich an Administratoren und Künstler, die den AWS Deadline Cloud Submitter installieren, einrichten und starten möchten. Ein Deadline Cloud-Einreicher ist ein DCC-Plugin (Digital Content Creation). Künstler verwenden es, um Jobs über eine DCC-Schnittstelle eines Drittanbieters einzureichen, mit der sie vertraut sind.

> **Note**
>
> Dieser Vorgang muss auf allen Workstations abgeschlossen sein, die Künstler für das Einreichen von Renderings verwenden werden.

Auf jeder Workstation muss das DCC installiert sein, bevor der entsprechende Submitter installiert werden kann. Wenn Sie beispielsweise den Deadline Cloud Submitter für Blender herunterladen möchten, muss Blender bereits auf Ihrer Workstation installiert sein.

Themen

Schritt 1: Installieren Sie den Deadline Cloud Submitter

Die folgenden Abschnitte führen Sie durch die Schritte zur Installation des Deadline Cloud-Einreichers.

Laden Sie das Installationsprogramm für den Submitter herunter

Bevor Sie den Deadline Cloud Submitter installieren können, müssen Sie den Installer für den Submitter herunterladen. Derzeit unterstützt das Deadline Cloud-Installationsprogramm für Submitter nur Windows and Linux.

1. Melden Sie sich bei der Deadline Cloud-Konsole an AWS Management Console und öffnen Sie sie.
2. Wählen Sie im seitlichen Navigationsbereich die Option Downloads aus.

3. Suchen Sie den Installationsbereich Deadline Cloud Submitter.
4. Wählen Sie das Installationsprogramm für das Betriebssystem Ihres Computers aus und wählen Sie dann Herunterladen.

(Optional) Überprüfen Sie die Echtheit der heruntergeladenen Software

Gehen Sie wie folgt vor, um zu überprüfen, ob die heruntergeladene Software authentisch ist Windows or Linux. Möglicherweise möchten Sie dies tun, um sicherzustellen, dass niemand die Dateien während oder nach dem Download-Vorgang manipuliert hat.

Sie können diese Anweisungen verwenden, um zuerst das Installationsprogramm und dann den Deadline Cloud-Monitor zu überprüfen, nachdem Sie ihn heruntergeladen haben. Schritt 2: Installieren und richten Sie den Deadline Cloud Monitor ein

Windows

Gehen Sie wie folgt vor, um die Echtheit Ihrer heruntergeladenen Dateien zu überprüfen.

1. Ersetzen Sie den Befehl im folgenden Befehl *file* durch die Datei, die Sie überprüfen möchten. Beispiel, ***C:\PATH\TO\MY*DeadlineCloudSubmitter-windows-x64-installer.exe** . Ersetzen Sie es außerdem *signtool-sdk-version* durch die Version von SignTool SDK installiert. Beispiel, **10.0.22000.0**.

   ```
   "C:\Program Files (x86)\Windows Kits\10\bin\signtool-sdk-version\x86\signtool.exe" verify /vfile
   ```

2. Sie können beispielsweise die Installationsdatei für den Deadline Cloud-Absender überprüfen, indem Sie den folgenden Befehl ausführen:

   ```
   "C:\Program Files (x86)\Windows Kits\10\bin
   \10.0.22000.0\x86\signtool.exe" verify /v DeadlineCloudSubmitter-windows-x64-installer.exe
   ```

Linux

Verwenden Sie das gpg Befehlszeilentool, um die Echtheit Ihrer heruntergeladenen Dateien zu überprüfen.

1. Importieren Sie den OpenPGP Schlüssel, indem Sie den folgenden Befehl ausführen:

```
 gpg --import --armor <<EOF
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGX6GQsBEADduUtJgqSXI+q76O6fsFwEYKmbnlyL0xKvlq32EZuyv0otZo5L
le4m5Gg52AzrvPvDiUTLooAlvYeozaYyirIGsK08Ydz0Ftdjroiuh/mw9JSJDJRI
rnRn5yKet1JFezkjopA3pjsTBP6lW/mb1bDBDEwwwtH0x9lV7A03FJ9T7Uzu/qSh
qO/UYdkafro3cPASvkqgDt2tCvURfBcUCAjZVFcLZcVD5iwXacxvKsxxS/e7kuVV
I1+VGT8Hj8XzWYhjCZxOLZk/fvpYPMyEEujN0fYUp6RtMIXve0C9awwMCy5nBG2J
eE2Ol5DsCpTaBd4Fdr3LWcSs8JFA/YfP9auL3NczOozPoVJt+fw8CBlVIXO0J7l5
hvHDjcC+5v0wxqAlMG6+f/SX7CT8FXK+L3iOJ5gBYUNXqHSxUdv8kt76/KVmQa1B
Akl+MPKpMq+lhw++S3G/lXqwWaDNQbRRw7dSZHymQVXvPp1nsqc3hV7KlOM+6s6g
1g4mvFY4lf6DhptwZLWyQXU8rBQpojvQfiSmDFrFPWFi5BexesuVnkGIolQoklKx
AVUSdJPVEJCteyy7td4FPhBaSqT5vW3+ANbr9b/uoRYWJvn17dN0cc9HuRh/Ai+I
nkfECo2WUDLZ0fEKGjGyFX+todWvJXjvc5kmE9Ty5vJp+M9Vvb8jd6t+mwARAQAB
tCxBV1MgRGVhZGxpbmUgQ2xvdWQgPGF3cy1kZWFkbGluZUBhbWF6b24uY29tPokC
VwQTAQgAQRYhBLhAwIwpqQeWoHH6pfbNPOa3bzzvBQJl+hkLAxsvBAUJA8JnAAUL
CQgHAgIiAgYVCgkICwIDFgIBAh4HAheAAAoJEPbNPOa3bzzvKswQAJXzKSAY8sY8
F6Eas2oYwIDDdDurs8FiEnFghjUEO6MTt9AykF/jw+CQg2UzFtEyObHBymhgmhXE
3buVeom96tgM3ZDfZu+sxi5pGX6oAQnZ6riztN+VpkpQmLgwtMGpSMLl3KLwnv2k
WK8mrR/fPMkfdaewB7A6RIUYiW33GAL4KfMIs8/vIwIJw99NxHpZQVoU6dFpuDtE
1OuxGcCqGJ7mAmo6H/YawSNp2Ns80gyqIKYo7o3LJ+WRroIRlQyctq8gnR9JvYXX
42ASqLq5+OXKo4qh81blXKYqtc176BbbSNFjWnzIQgKDgNiHFZCdcOVgqDhwO15r
NICbqqwwNLj/Fr2kecYx180Ktpl0jOOw5IOyh3bf3MVGWnYRdjvA1v+/CO+55N4g
z0kf50Lcdu5RtqV10XBCifn28pecqPaSdYcssYSRl5DLiFktGbNzTGcZZwITTKQc
af8PPdTGtnnb6P+cdbW3bt9MVtN5/dgSHLThnS8MPEuNCtkTnpXshuVuBGgwBMdb
qUC+HjqvhZzbwns8dr5WI+6HWNBFgGANn6ageYl58vVp0UkuNP8wcWjRARciHXZx
ku6W2jPTHDWGNrBQO2Fx7fd2QYJheIPPAShHcfJO+xgWCof45D0vAxAJ8gGg9Eq+
gFWhsx4NSHn2gh1gDZ41Ou/4exJ1lwPM
=uVaX
-----END PGP PUBLIC KEY BLOCK-----
EOF
```

2. Stellen Sie fest, ob Sie dem OpenPGP Schlüssel vertrauen möchten. Bei der Entscheidung, ob dem oben genannten Schlüssel vertraut werden soll, sollten Sie unter anderem die folgenden Faktoren berücksichtigen:

   - Die Internetverbindung, mit der Sie den GPG-Schlüssel von dieser Website abgerufen haben, ist sicher.
   - Das Gerät, mit dem Sie auf diese Website zugreifen, ist sicher.
   - AWS hat Maßnahmen ergriffen, um das Hosting des OpenPGP öffentlichen Schlüssels auf dieser Website zu sichern.

3. Wenn Sie sich entscheiden, dem zu vertrauen OpenPGP Schlüssel, bearbeiten Sie den Schlüssel, dem Sie vertrauen möchten, gpg ähnlich wie im folgenden Beispiel:

```
$ gpg --edit-key 0xB840C08C29A90796A071FAA5F6CD3CE6B76F3CEF

    gpg (GnuPG) 2.0.22; Copyright (C) 2013 Free Software Foundation, Inc.
    This is free software: you are free to change and redistribute it.
    There is NO WARRANTY, to the extent permitted by law.


    pub  4096R/4BF0B8D2  created: 2023-06-23  expires: 2025-06-22  usage: SCEA
                         trust: unknown       validity: unknown
    [ unknown] (1). AWS Deadline Cloud example@example.com

    gpg> trust
    pub  4096R/4BF0B8D2  created: 2023-06-23  expires: 2025-06-22  usage: SCEA
                         trust: unknown       validity: unknown
    [ unknown] (1). AWS Deadline Cloud aws-deadline@amazon.com

    Please decide how far you trust this user to correctly verify other users'
 keys
    (by looking at passports, checking fingerprints from different sources,
 etc.)

      1 = I don't know or won't say
      2 = I do NOT trust
      3 = I trust marginally
      4 = I trust fully
      5 = I trust ultimately
      m = back to the main menu

    Your decision? 5
    Do you really want to set this key to ultimate trust? (y/N) y

    pub  4096R/4BF0B8D2  created: 2023-06-23  expires: 2025-06-22  usage: SCEA
                         trust: ultimate      validity: unknown
    [ unknown] (1). AWS Deadline Cloud aws-deadline@amazon.com
    Please note that the shown key validity is not necessarily correct
    unless you restart the program.

    gpg> quit
```

4. Überprüfen Sie das Installationsprogramm für Deadline Cloud Submitter

   Gehen Sie wie folgt vor, um das Installationsprogramm für den Deadline Cloud-Absender zu verifizieren:

   a. Kehren Sie zur Download-Seite der Deadline Cloud-Konsole zurück und laden Sie die Signaturdatei für das Deadline Cloud-Installationsprogramm für Submitter herunter.

   b. Überprüfen Sie die Signatur des Deadline Cloud-Installationsprogramms für Submitter, indem Sie Folgendes ausführen:

   ```
   gpg --verify ./DeadlineCloudSubmitter-linux-x64-installer.run.sig ./
   DeadlineCloudSubmitter-linux-x64-installer.run
   ```

5. Überprüfen Sie den Deadline Cloud-Monitor

   > **Note**
   >
   > Sie können den Download des Deadline Cloud-Monitors mithilfe von Signaturdateien oder plattformspezifischen Methoden überprüfen. Plattformspezifische Methoden finden Sie im Linux (Debian) Registerkarte, die Linux Registerkarte (RPM) oder Linux (AppImage) Tab, der auf Ihrem heruntergeladenen Dateityp basiert.

   Gehen Sie wie folgt vor, um die Desktop-Anwendung Deadline Cloud Monitor anhand von Signaturdateien zu verifizieren:

   a. Kehren Sie zur Downloadseite der Deadline Cloud-Konsole zurück, laden Sie die entsprechende SIG-Datei herunter und führen Sie sie dann aus

      Für .deb:

      ```
      gpg --verify ./deadline-cloud-monitor_<APP_VERSION>_amd64.deb.sig ./
      deadline-cloud-monitor_<APP_VERSION>_amd64.deb
      ```

      Für .rpm:

      ```
      gpg --verify ./deadline-cloud-monitor_<APP_VERSION>_x86_64.deb.sig ./
      deadline-cloud-monitor_<APP_VERSION>_x86_64.rpm
      ```

Für. AppImage:

```
gpg --verify ./deadline-cloud-monitor_<APP_VERSION>_amd64.AppImage.sig ./
deadline-cloud-monitor_<APP_VERSION>_amd64.AppImage
```

b. Vergewissern Sie sich, dass die Ausgabe wie folgt aussieht:

```
gpg: Signature made Mon Apr 1 21:10:14 2024 UTC

gpg: using RSA key B840C08C29A90796A071FAA5F6CD3CE6B7
```

Wenn die Ausgabe den Ausdruck enthält, bedeutet dies`Good signature from "AWS Deadline Cloud"`, dass die Signatur erfolgreich verifiziert wurde und Sie das Installationsskript für den Deadline Cloud-Monitor ausführen können.

Linux (AppImage)

Um Pakete zu verifizieren, die eine verwenden Linux . AppImage binär, führe zuerst die Schritte 1—3 in der Linux klicken Sie auf die Registerkarte und führen Sie dann die folgenden Schritte aus.

1. Laden Sie GitHub validate-x86_64 von der AppImageUpdate Seite in herunter. AppImageDatei.
2. Führen Sie nach dem Herunterladen der Datei den folgenden Befehl aus, um Ausführungsberechtigungen hinzuzufügen.

```
chmod a+x ./validate-x86_64.AppImage
```

3. Führen Sie den folgenden Befehl aus, um Ausführungsberechtigungen hinzuzufügen.

```
chmod a+x ./deadline-cloud-monitor_<APP_VERSION>_amd64.AppImage
```

4. Führen Sie den folgenden Befehl aus, um die Signatur des Deadline Cloud-Monitors zu überprüfen.

```
./validate-x86_64.AppImage ./deadline-cloud-monitor_<APP_VERSION>_amd64.AppImage
```

Wenn die Ausgabe den Ausdruck enthält`Validation successful`, bedeutet dies, dass die Signatur erfolgreich verifiziert wurde und Sie das Installationsskript für den Deadline Cloud-Monitor problemlos ausführen können.

Linux (Debian)

Um Pakete zu verifizieren, die eine verwenden Linux .deb-Binärdatei, führe zuerst die Schritte 1—3 im Linux Registerkarte.

dpkg ist in den meisten Fällen das zentrale Paketverwaltungstool debian basiert Linux Verteilungen. Sie können die .deb-Datei mit dem Tool überprüfen.

1. Laden Sie von der Downloadseite der Deadline Cloud-Konsole die .deb-Datei für den Deadline Cloud-Monitor herunter.
2. *<APP_VERSION>*Ersetzen Sie sie durch die Version der .deb-Datei, die Sie verifizieren möchten.

```
dpkg-sig --verify deadline-cloud-monitor_<APP_VERSION>_amd64.deb
```

3. Die Ausgabe wird wie folgt aussehen:

```
ProcessingLinux deadline-cloud-monitor_<APP_VERSION>_amd64.deb...
GOODSIG _gpgbuilder B840C08C29A90796A071FAA5F6CD3C 171200
```

4. Um die .deb-Datei zu überprüfen, vergewissern Sie sich, dass sie in der Ausgabe vorhanden `GOODSIG` ist.

Linux (RPM)

Um Pakete zu verifizieren, die eine verwenden Linux .rpm-Binärdatei, führen Sie zunächst die Schritte 1—3 in der Linux Registerkarte.

1. Laden Sie von der Downloadseite der Deadline Cloud-Konsole die .rpm-Datei für den Deadline Cloud-Monitor herunter.
2. *<APP_VERSION>*Ersetzen Sie sie durch die Version der .rpm-Datei, um sie zu überprüfen.

```
gpg --export --armor "Deadline Cloud" > key.pub
sudo rpm --import key.pub
rpm -K deadline-cloud-monitor-<APP_VERSION>-1.x86_64.rpm
```

3. Die Ausgabe wird wie folgt aussehen:

```
deadline-cloud-monitor-deadline-cloud-
monitor-<APP_VERSION>-1.x86_64.rpm-1.x86_64.rpm: digests signatures OK
```

4. Um die .rpm-Datei zu überprüfen, vergewissern Sie sich, dass sie in der Ausgabe enthalten `digests signatures OK` ist.

Installieren Sie den Deadline Cloud Submitter

Sie können einen Deadline Cloud-Einreicher mit installieren Windows or Linux. Mit dem Installer können Sie die folgenden Submitter installieren:

Software	Unterstützte Versionen	Windows-Installationsprogramm	Linux-Installationsprogramm
Adobe After Effects	2024, 2025	Enthalten	Nicht enthalten
Autodesk Arnold für Maya	7.1, 7.2	Enthalten	Enthalten
Autodesk Maya	2023, 2024, 2025	Inbegriffen	Inbegriffen
Mixer	3.6, 4.2	Inbegriffen	Inbegriffen
KeyShot Studio	2023, 2024	Inbegriffen	Nicht enthalten
Maxon Cinema 4D	2024, 2025	Inbegriffen	Nicht enthalten
Atombombe	15	Inbegriffen	Inbegriffen
SideFX Houdini	19,5, 20, 20,5	Inbegriffen	Inbegriffen
Unreal Engine	5.2, 5.3, 5.4	Inbegriffen	Nicht enthalten

Sie können andere Einreicher installieren, die hier nicht aufgeführt sind. Wir verwenden Deadline Cloud-Bibliotheken, um Einreicher zu erstellen. Zu den Einreichern gehören 3ds Max und Rhino. Den Quellcode für diese Bibliotheken und Einreicher finden Sie in der AWS-Deadline-Organisation. GitHub

Windows

1. Navigieren Sie in einem Dateibrowser zu dem Ordner, in den das Installationsprogramm heruntergeladen wurde, und wählen Sie dann aus. `DeadlineCloudSubmitter-windows-x64-installer.exe`

   a. Wenn ein Popup-Fenster mit Windows-Schutz für Ihren PC angezeigt wird, wählen Sie Weitere Informationen aus.

   b. Wählen Sie „Trotzdem ausführen“.

2. Nachdem der AWS Deadline Cloud Submitter Setup Wizard geöffnet wurde, wählen Sie Weiter.

3. Wählen Sie den Umfang der Installation aus, indem Sie einen der folgenden Schritte ausführen:

   - Um nur für den aktuellen Benutzer zu installieren, wählen Sie Benutzer.
   - Um für alle Benutzer zu installieren, wählen Sie System.

     Wenn Sie System wählen, müssen Sie das Installationsprogramm beenden und es als Administrator erneut ausführen, indem Sie die folgenden Schritte ausführen:

     a. Klicken Sie mit der rechten Maustaste auf **`DeadlineCloudSubmitter-windows-x64-installer.exe`** und wählen Sie dann Als Administrator ausführen.

     b. Geben Sie Ihre Administratoranmeldedaten ein und wählen Sie dann Ja.

     c. Wählen Sie System als Installationsbereich aus.

4. Nachdem Sie den Installationsbereich ausgewählt haben, wählen Sie Weiter.

5. Wählen Sie erneut Weiter, um das Installationsverzeichnis zu akzeptieren.

6. Wählen Sie Integrierter Absender für Nuke, oder den Submitter, den Sie installieren möchten.

7. Wählen Sie Weiter.

8. Überprüfen Sie die Installation und wählen Sie Weiter.

9. Wählen Sie erneut Weiter und dann Fertig stellen.

Linux

> **Note**
>
> Die Deadline Cloud ist integriert Nuke Installer für Linux und Deadline Cloud Monitor kann nur auf installiert werden Linux Distributionen mit mindestens GLIBC 2.31.

1. Öffnen Sie ein Terminal-Fenster.
2. Um eine Systeminstallation des Installers durchzuführen, geben Sie den Befehl ein **`sudo -i`** und drücken Sie die Eingabetaste, um root zu werden.
3. Navigieren Sie zu dem Verzeichnis, in das Sie das Installationsprogramm heruntergeladen haben.

   Beispiel, **`cd /home/USER/Downloads`**.
4. Geben Sie ein, um das Installationsprogramm ausführbar zu machen**`chmod +x DeadlineCloudSubmitter-linux-x64-installer.run`**.
5. Geben Sie ein, um das Deadline Cloud Submitter-Installationsprogramm auszuführen. **`./DeadlineCloudSubmitter-linux-x64-installer.run`**
6. Wenn das Installationsprogramm geöffnet wird, folgen Sie den Anweisungen auf Ihrem Bildschirm, um den Einrichtungsassistenten abzuschließen.

Schritt 2: Installieren und richten Sie den Deadline Cloud Monitor ein

Sie können die Desktop-Anwendung Deadline Cloud Monitor mit installieren Windows or Linux.

Windows

1. Falls Sie es noch nicht getan haben, melden Sie sich bei der Deadline Cloud-Konsole an AWS Management Console und öffnen Sie sie.
2. Wählen Sie im linken Navigationsbereich die Option Downloads überwachen aus.
3. Wählen Sie im Bereich Deadline Cloud Monitor die Datei für das Betriebssystem Ihres Computers aus.
4. Um den Deadline Cloud-Monitor herunterzuladen, wählen Sie Herunterladen.

Verwenden Sie den folgenden Befehl, um eine unbeaufsichtigte Installation durchzuführen:

```
DeadlineCloudMonitor_VERSION_x64-setup.exe /S
```

Standardmäßig ist der Monitor in installiert`C:\Users{username}\AppData\Local\DeadlineCloudMonitor`. Verwenden Sie stattdessen diesen Befehl, um das Installationsverzeichnis zu ändern:

```
DeadlineCloudMonitor_VERSION_x64-setup.exe /S /D={InstallDirectory}
```

Linux (AppImage)

Um Deadline Cloud Monitor AppImage auf Debian-Distributionen zu installieren

1. Laden Sie den neuesten Deadline Cloud-Monitor AppImage herunter.
2. > **Note**
   >
   > Dieser Schritt gilt für Ubuntu 22 und höher. Für andere Versionen von Ubuntu überspringen Sie diesen Schritt.

   Geben Sie Folgendes ein, um libfuse2 zu installieren:

   ```
   sudo apt udpate
   sudo apt install libfuse2
   ```
3. Um die AppImage ausführbare Datei zu erstellen, geben Sie Folgendes ein:

   ```
   chmod a+x deadline-cloud-monitor_<APP_VERSION>_amd64.AppImage
   ```

Linux (Debian)

Um Deadline Cloud zu installieren, überwachen Sie das Debian-Paket auf Debian-Distributionen

1. Laden Sie das neueste Debian-Paket für den Deadline Cloud Monitor herunter.
2. > **Note**
   >
   > Dieser Schritt gilt für Ubuntu 22 und höher. Für andere Versionen von Ubuntu überspringen Sie diesen Schritt.

Um libssl1.1 zu installieren, geben Sie Folgendes ein:

```
wget http://archive.ubuntu.com/ubuntu/pool/main/o/openssl/
libssl1.1_1.1.1f-1ubuntu2_amd64.deb
sudo apt install ./libssl1.1_1.1.1f-1ubuntu2_amd64.deb
```

3. Um das Debian-Paket Deadline Cloud Monitor zu installieren, geben Sie Folgendes ein:

```
sudo apt update
sudo apt install ./deadline-cloud-monitor_<APP_VERSION>_amd64.deb
```

4. Falls die Installation bei Paketen fehlschlägt, deren Abhängigkeiten noch nicht erfüllt sind, reparieren Sie die defekten Pakete und führen Sie dann die folgenden Befehle aus.

```
sudo apt --fix-missing update
sudo apt update
sudo apt install -f
```

Linux (RPM)

Um Deadline Cloud Monitor RPM zu installieren Rocky Linux 9 or Alma Linux 9

1. Laden Sie das neueste RPM für den Deadline Cloud-Monitor herunter.
2. Fügen Sie die zusätzlichen Pakete für Enterprise Linux 9 Repository:

```
sudo dnf install epel-release
```

3. Installieren Sie compat-openssl11 für die libssl.so.1.1-Abhängigkeit:

```
sudo dnf install compat-openssl11 deadline-cloud-monitor-<VERSION>-1.x86_64.rpm
```

Um Deadline Cloud Monitor RPM zu installieren Red Hat Linux 9

1. Laden Sie das neueste RPM für den Deadline Cloud-Monitor herunter.
2. Aktivieren Sie den CodeReady Linux Builder Repositorium:

```
subscription-manager repos --enable codeready-builder-for-rhel-9-x86_64-rpms
```

3. Installieren Sie die zusätzlichen Pakete für Enterprise RPM:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-
latest-9.noarch.rpm
```

4. Installieren Sie compat-openssl11 für die libssl.so.1.1-Abhängigkeit:

```
sudo dnf install compat-openssl11 deadline-cloud-monitor-<VERSION>-1.x86_64.rpm
```

Um Deadline Cloud Monitor RPM zu installieren Rocky Linux 8, Alma Linux 8, oder Red Hat Linux 8

1. Laden Sie die neueste Version von Deadline Cloud Monitor RPM herunter.
2. Installieren Sie den Deadline Cloud-Monitor:

```
sudo dnf install deadline-cloud-monitor-<VERSION>-1.x86_64.rpm
```

Nachdem Sie den Download abgeschlossen haben, können Sie die Echtheit der heruntergeladenen Software überprüfen. Möglicherweise möchten Sie auf diese Weise sicherstellen, dass niemand die Dateien während oder nach dem Download-Vorgang manipuliert hat. Weitere Informationen finden Sie unter Überprüfen der Authentizität der heruntergeladenen Software in Schritt 1.

Nachdem Sie den Deadline Cloud-Monitor heruntergeladen und die Authentizität überprüft haben, richten Sie den Deadline Cloud-Monitor wie folgt ein.

So richten Sie den Deadline Cloud-Monitor ein

1. Öffnen Sie den Deadline Cloud-Monitor.
2. Wenn Sie aufgefordert werden, ein neues Profil zu erstellen, führen Sie die folgenden Schritte aus.

   a. Geben Sie Ihre Monitor-URL in die URL-Eingabe ein, die wie folgt aussieht **`https://MY-MONITOR.deadlinecloud.amazonaws.com/`**

   b. Geben Sie einen Profilnamen ein.

c. Wählen Sie Profil erstellen.

   Ihr Profil wurde erstellt und Ihre Anmeldeinformationen werden nun mit jeder Software geteilt, die den von Ihnen erstellten Profilnamen verwendet.

3. Nachdem Sie das Deadline Cloud-Monitorprofil erstellt haben, können Sie den Profilnamen oder die Studio-URL nicht mehr ändern. Wenn Sie Änderungen vornehmen müssen, gehen Sie stattdessen wie folgt vor:

   a. Lösche das Profil. Wählen Sie im linken Navigationsbereich Deadline Cloud Monitor > Einstellungen > Löschen.

   b. Erstellen Sie ein neues Profil mit den gewünschten Änderungen.

4. Verwenden Sie im linken Navigationsbereich die Option >Deadline Cloud Monitor, um Folgendes zu tun:

   - Ändern Sie das Deadline Cloud-Monitorprofil, um sich bei einem anderen Monitor anzumelden.
   - Aktivieren Sie Autologin, damit Sie Ihre Monitor-URL bei nachfolgenden Öffnungen des Deadline Cloud-Monitors nicht eingeben müssen.

5. Schließen Sie das Fenster des Deadline Cloud-Monitors. Es läuft weiterhin im Hintergrund und synchronisiert Ihre Anmeldeinformationen alle 15 Minuten.

6. Führen Sie für jede DCC-Anwendung (Digital Content Creation), die Sie für Ihre Renderprojekte verwenden möchten, die folgenden Schritte aus:

   a. Öffnen Sie in Ihrem Deadline Cloud-Absender die Konfiguration der Deadline Cloud-Workstation.

   b. Wählen Sie in der Workstation-Konfiguration das Profil aus, das Sie im Deadline Cloud-Monitor erstellt haben. Ihre Deadline Cloud-Anmeldeinformationen werden jetzt mit diesem DCC geteilt und Ihre Tools sollten wie erwartet funktionieren.

Schritt 3: Starten Sie den Deadline Cloud Submitter

Das folgende Beispiel zeigt, wie Sie das installieren Blender Einreicher. Sie können andere Absender installieren, indem Sie die Anweisungen unter verwenden. Unterstützte Einsender

So starten Sie den Deadline Cloud-Absender in Blender

> **Note**
>
> Unterstützung für Blender wird bereitgestellt mit dem Conda Umgebung für servicemanagierte Flotten. Weitere Informationen finden Sie unter Standard Conda Warteschlangenumgebung.

1. Öffnen Sie .Blender.
2. Wählen Sie „Bearbeiten“ und dann „Einstellungen“. Wählen Sie unter Dateipfade die Option Skriptverzeichnisse und anschließend Hinzufügen aus. Fügen Sie ein Skriptverzeichnis für den Python-Ordner hinzu, in dem Blender Submitter wurde installiert:

   ```
   Windows:
      %USERPROFILE%\DeadlineCloudSubmitter\Submitters\Blender\python\
   Linux:
      ~/DeadlineCloudSubmitter/Submitters/Blender/python/
   ```

3. Neustart Blender.
4. Wählen Sie „Bearbeiten“ und dann „Einstellungen“. Wählen Sie als Nächstes Add-Ons und suchen Sie dann nach Deadline Cloud für Blender. Markieren Sie das Kontrollkästchen, um das Add-on zu aktivieren.
5. Öffnen Sie ein Blender Szene mit Abhängigkeiten, die innerhalb des Asset-Stammverzeichnisses existieren.
6. Wählen Sie im Menü „Rendern“ das Dialogfeld „Deadline Cloud“ aus.
   a. Wenn Sie im Deadline Cloud-Absender noch nicht authentifiziert sind, wird der Anmeldestatus als NEEDS_LOGIN angezeigt.
   b. Wählen Sie Login (Anmelden) aus.
   c. Ein Anmeldefenster im Browser wird angezeigt. Melden Sie sich mit Ihren Benutzeranmeldedaten an.
   d. Wählen Sie Zulassen. Sie sind jetzt angemeldet und der Status der Anmeldeinformationen wird als AUTHENTIFIZIERT angezeigt.
7. Wählen Sie Absenden aus.

Unterstützte Einsender

Die folgenden Abschnitte führen Sie durch die Schritte zum Starten der verfügbaren Deadline Cloud-Einreicher-Plugins.

Sie können andere Einreicher installieren, die hier nicht aufgeführt sind. Wir verwenden Deadline Cloud-Bibliotheken, um Einreicher zu erstellen. Zu den Einreichern gehören 3ds Max und Rhino. Den Quellcode für diese Bibliotheken und Einreicher finden Sie in der AWS-Deadline-Organisation. GitHub

Software	Unterstützte Versionen	Windows-Installationsprogramm	Linux-Installationsprogramm
Adobe After Effects	2024, 2025	Enthalten	Nicht enthalten
Autodesk Arnold für Maya	7.1, 7.2	Enthalten	Enthalten
Autodesk Maya	2023, 2024, 2025	Inbegriffen	Inbegriffen
Mixer	3.6, 4.2	Inbegriffen	Inbegriffen
KeyShot Studio	2023, 2024	Inbegriffen	Nicht enthalten
Maxon Cinema 4D	2024, 2025	Inbegriffen	Nicht enthalten
Atombombe	15	Inbegriffen	Inbegriffen
SideFX Houdini	19,5, 20, 20,5	Inbegriffen	Inbegriffen
Unreal Engine	5.2, 5.3, 5.4	Inbegriffen	Nicht enthalten

After Effects

Um den Deadline Cloud-Einreicher zu starten in After Effects

1. Öffnen Sie .After Effects.
2. Wählen Sie „Bearbeiten“, dann „Einstellungen“ und dann „Scripting & Expressions“.
3. Wählen Sie „Skripten erlauben, Dateien zu schreiben und auf Netzwerke zuzugreifen“.

4. Starten Sie After Effects neu
5. Wählen Sie „Fenster“ und anschließend „DeadlineCloudSubmitter.jsx“.

Um den After Effects-Submitter zu verwenden

1. Wählen Sie im Bereich „Absender“ die Option „Renderliste öffnen“.
2. Fügen Sie Ihrer Renderliste eine Komposition hinzu und richten Sie die Rendereinstellungen, das Ausgabemodul und den Ausgabepfad ein.
3. Wählen Sie im Bereich des Absenders die Option „Aktualisieren“.
4. Wählen Sie Ihre Komposition aus der Liste aus und klicken Sie dann auf Absenden. Sie können erneut „Aktualisieren“ wählen, wenn Sie Kompositionen zu Ihrer Renderliste hinzufügen oder daraus entfernen.

Sie können den Absender an die Seitenbereiche andocken, indem Sie die obere rechte Ecke des Absenders auswählen und ihn in einem der markierten Bereiche von ablegen After Effects.

Blender

So starten Sie den Deadline Cloud-Absender in Blender

> **Note**
>
> Unterstützung für Blender wird bereitgestellt mit dem Conda Umgebung für servicemanagierte Flotten. Weitere Informationen finden Sie unter Standard Conda Warteschlangenumgebung.

1. Öffnen Sie .Blender.
2. Wählen Sie „Bearbeiten“ und dann „Einstellungen“. Wählen Sie unter Dateipfade die Option Skriptverzeichnisse und anschließend Hinzufügen aus. Fügen Sie ein Skriptverzeichnis für den Python-Ordner hinzu, in dem Blender Submitter wurde installiert:

```
Windows:
   %USERPROFILE%\DeadlineCloudSubmitter\Submitters\Blender\python\
Linux:
   ~/DeadlineCloudSubmitter/Submitters/Blender/python/
```

3. Neustart Blender.
4. Wählen Sie „Bearbeiten“ und dann „Einstellungen“. Wählen Sie als Nächstes Add-Ons und suchen Sie dann nach Deadline Cloud für Blender. Markieren Sie das Kontrollkästchen, um das Add-on zu aktivieren.
5. Öffnen Sie ein Blender Szene mit Abhängigkeiten, die innerhalb des Asset-Stammverzeichnisses existieren.
6. Wählen Sie im Menü „Rendern“ das Dialogfeld „Deadline Cloud“ aus.
    a. Wenn Sie im Deadline Cloud-Absender noch nicht authentifiziert sind, wird der Anmeldestatus als NEEDS_LOGIN angezeigt.
    b. Wählen Sie Login (Anmelden) aus.
    c. Ein Anmeldefenster im Browser wird angezeigt. Melden Sie sich mit Ihren Benutzeranmeldedaten an.
    d. Wählen Sie Zulassen. Sie sind jetzt angemeldet und der Status der Anmeldeinformationen wird als AUTHENTIFIZIERT angezeigt.
7. Wählen Sie Absenden aus.

Cinema 4D

Um den Deadline Cloud Submitter in zu starten Cinema 4D

> **Note**
>
> Unterstützung für Cinema 4D wird bereitgestellt mit dem Conda Umgebung für servicemanagierte Flotten. Weitere Informationen finden Sie unter Standard Conda Warteschlangenumgebung.

1. Öffnen Sie Cinema 4D.
2. Wenn Sie aufgefordert werden, GUI-Komponenten für AWS Deadline Cloud zu installieren, gehen Sie wie folgt vor:
    a. Wenn die Aufforderung angezeigt wird, wählen Sie Ja und warten Sie, bis die Abhängigkeiten installiert sind.
    b. Neustart Cinema 4D um sicherzustellen, dass die Änderungen übernommen werden.
3. Wählen Sie Erweiterungen > AWS Deadline Cloud Submitter.

Houdini

So starten Sie den Deadline Cloud Submitter in Houdini

> **Note**
>
> Unterstützung für Houdini wird bereitgestellt mit dem Conda Umgebung für servicemanagierte Flotten. Weitere Informationen finden Sie unter Standard Conda Warteschlangenumgebung.

1. Öffnen Sie .Houdini.
2. Wählen Sie im Netzwerk-Editor das /out-Netzwerk aus.
3. Drücken Sie die Tabulatortaste und drücken Sie die Eingabetaste**`deadline`**.
4. Wählen Sie die Option Deadline Cloud und verbinden Sie sie mit Ihrem vorhandenen Netzwerk.
5. Doppelklicken Sie auf den Deadline Cloud-Knoten.

KeyShot

Um den Deadline Cloud-Absender in zu starten KeyShot

1. Öffnen KeyShot.
2. Wählen Sie aus.Windows> Scripting-Konsole > An AWS Deadline Cloud senden und ausführen.

Es gibt zwei Einreichungsmodi für den KeyShot Einreicher. Wählen Sie den Einreichungsmodus aus, um den Einreicher zu öffnen.

- Hängen Sie die BIP-Datei der Szene und alle externen Dateiverweise an — Die geöffnete Szenendatei und alle externen Dateien, auf die in der BIP verwiesen wird, sind als Jobanhänge enthalten.
- Nur die BIP-Datei der Szene anhängen — Nur die geöffnete Szenendatei wird an die Einreichung angehängt. Alle externen Dateien, auf die in der Szene verwiesen wird, müssen den Mitarbeitern über Netzwerkspeicher oder eine andere Methode zur Verfügung stehen.

Maya and Arnold for Maya

Um den Deadline Cloud-Absender in zu starten Maya

> **Note**
>
> Unterstützung für Maya and Arnold for Maya (MtoA) wird bereitgestellt mit dem Conda Umgebung für servicemanagierte Flotten. Weitere Informationen finden Sie unter Standard Conda Warteschlangenumgebung.

1. Öffnen Sie .Maya.
2. Legen Sie Ihr Projekt fest und öffnen Sie eine Datei, die sich im Stammverzeichnis der Ressource befindet.
3. Wählen Sie Windows → Einstellungen/Einstellungen → Plugin-Manager.
4. Suchen Sie nach DeadlineCloudSubmitter.
5. Um das Deadline Cloud-Einreicher-Plugin zu laden, wählen Sie Geladen aus.
    a. Wenn Sie noch nicht im Deadline Cloud-Absender authentifiziert sind, wird der Anmeldestatus als NEEDS_LOGIN angezeigt.
    b. Wählen Sie Login (Anmelden) aus.
    c. Ein Anmeldefenster im Browser wird angezeigt. Melden Sie sich mit Ihren Benutzeranmeldedaten an.
    d. Wählen Sie Zulassen. Sie sind jetzt angemeldet und der Status der Anmeldeinformationen wird als AUTHENTIFIZIERT angezeigt.
6. (Optional) Um das Deadline Cloud Submitter-Plugin bei jedem Öffnen zu laden Maya, wählen Sie Automatisch laden.
7. Wählen Sie das Deadline Cloud-Regal aus und klicken Sie dann auf die grüne Schaltfläche, um den Submitter zu starten.

Nuke

So starten Sie den Deadline Cloud-Absender in Nuke

> **Note**
>
> Unterstützung für Nuke wird bereitgestellt mit dem Conda Umgebung für servicemanagierte Flotten. Weitere Informationen finden Sie unter Standard Conda Warteschlangenumgebung.

1. Öffnen Sie .Nuke.
2. Öffnen Sie ein Nuke Skript mit Abhängigkeiten, die im Asset-Stammverzeichnis existieren.
3. Wählen Sie aus.AWS Deadline, und wählen Sie dann Submit to Deadline Cloud, um den Submitter zu starten.
   a. Wenn Sie noch nicht im Deadline Cloud-Absender authentifiziert sind, wird der Anmeldeinformationsstatus als NEEDS_LOGIN angezeigt.
   b. Wählen Sie Login (Anmelden) aus.
   c. Melden Sie sich im Anmeldefenster des Browsers mit Ihren Benutzeranmeldedaten an.
   d. Wählen Sie Zulassen. Sie sind jetzt angemeldet und der Status der Anmeldeinformationen wird als AUTHENTIFIZIERT angezeigt.
4. Wählen Sie Absenden aus.

Unreal Engine

Um den Deadline Cloud Submitter in zu starten Unreal Engine

1. Erstellen oder öffnen Sie den Ordner, den Sie für Unreal Engine projekte.
2. Öffnen Sie die Befehlszeile und führen Sie die folgenden Befehle aus:
   - **`git clone https://github.com/aws-deadline/deadline-cloud-for-unreal-engine`**
   - **`cd deadline-cloud-for-unreal/test_projects`**
   - **`git lfs fetch –all`**
3. Um das Plugin herunterzuladen für Unreal Engine, öffne das Unreal Engine Projektordner und starten Sie deadline-cloud-forunreal/test_projects/pull_ue_plugin.bat.

Dadurch werden die Plugin-Dateien eingefügt C:/LocalProjects/UnrealDeadlineCloudTest/Plugins/UnrealDeadlineCloudService.

4. Um den Absender herunterzuladen, öffnen Sie den UnrealDeadlineCloudService Ordner und führen Sie ihn aus. **`deadline-cloud-forunreal/ test_projects/Plugins/UnrealDeadlineCloudService/install_unreal_submitter.bat`**
5. Um den Absender zu starten von Unreal Engine, führen Sie die folgenden Schritte aus:

   a. Wählen Sie „Bearbeiten“ **>** „Projekteinstellungen“.

   b. Geben Sie im Suchfeld **`movie render pipeline`** ein.

   c. Passen Sie die folgenden Einstellungen für die Movie Render-Pipeline an:

      i. Geben Sie für Default Remote Executor ein. **`MoviePipelineDeadlineCloudRemoteExecutor`**

      ii. Geben Sie für Default Executor Job ein. **`MoviePipelineDeadlineCloudExecutorJob`**

      iii. Wählen Sie für Standardklassen für Jobeinstellungen das Pluszeichen aus, und geben Sie dann die Eingabetaste ein**`DeadlineCloudRenderStepSetting`**.

   Mit diesen Einstellungen können Sie das Deadline Cloud-Plug-in auswählen Unreal Engine.

Den Deadline Cloud-Monitor verwenden

Der AWS Deadline Cloud-Monitor bietet Ihnen einen Gesamtüberblick über Ihre visuellen Rechenjobs. Sie können ihn verwenden, um Jobs zu überwachen und zu verwalten, die Mitarbeiteraktivitäten in Flotten einzusehen, Budgets und Nutzung zu verfolgen und die Ergebnisse eines Jobs herunterzuladen.

Jede Warteschlange verfügt über einen Jobmonitor, der Ihnen den Status von Aufträgen, Schritten und Aufgaben anzeigt. Der Monitor bietet Möglichkeiten, Jobs direkt vom Monitor aus zu verwalten. Sie können Änderungen an der Priorisierung vornehmen, Jobs stornieren, Jobs in eine Warteschlange stellen und Jobs erneut einreichen.

Der Deadline Cloud-Monitor verfügt über eine Tabelle, in der der Übersichtsstatus für einen Job angezeigt wird. Sie können auch einen Job auswählen, um detaillierte Aufgabenprotokolle anzuzeigen, die bei der Behebung von Problemen mit einem Job helfen.

Sie können den Deadline Cloud-Monitor verwenden, um die Ergebnisse an den Speicherort auf Ihrer Workstation herunterzuladen, der bei der Erstellung des Jobs angegeben wurde.

Der Deadline Cloud-Monitor hilft Ihnen auch dabei, die Nutzung zu überwachen und die Kosten zu verwalten. Weitere Informationen finden Sie unter Ausgaben und Nutzung für Deadline Cloud-Farmen verfolgen.

Themen

Teilen Sie die URL des Deadline Cloud-Monitors

Wenn Sie den Deadline Cloud-Dienst einrichten, erstellen Sie standardmäßig eine URL, die den Deadline Cloud-Monitor für Ihr Konto öffnet. Verwenden Sie diese URL, um den Monitor in Ihrem Browser oder auf Ihrem Desktop zu öffnen. Teilen Sie die URL mit anderen Benutzern, damit diese auf den Deadline Cloud-Monitor zugreifen können.

Bevor ein Benutzer den Deadline Cloud-Monitor öffnen kann, müssen Sie dem Benutzer Zugriff gewähren. Um Zugriff zu gewähren, fügen Sie den Benutzer entweder der Liste der autorisierten Benutzer für den Monitor hinzu oder fügen Sie ihn einer Gruppe mit Zugriff auf den Monitor hinzu. Weitere Informationen finden Sie unter Benutzer in Deadline Cloud verwalten.

Um die Monitor-URL zu teilen

1. Öffnen Sie die Deadline Cloud-Konsole.
2. Wählen Sie unter Erste Schritte die Option Gehe zum Deadline Cloud-Dashboard.
3. Wählen Sie im Navigationsbereich Dashboard aus.
4. Wählen Sie im Abschnitt Kontoübersicht die Option Kontodetails aus.
5. Kopieren Sie die URL und senden Sie sie dann sicher an alle Personen, die auf den Deadline Cloud-Monitor zugreifen müssen.

Öffnen Sie den Deadline Cloud-Monitor

Sie können den Deadline Cloud-Monitor auf eine der folgenden Arten öffnen:

- Konsole — Melden Sie sich bei der Deadline Cloud-Konsole an AWS Management Console und öffnen Sie sie.
- Web — Rufen Sie die Monitor-URL auf, die Sie bei der Einrichtung von Deadline Cloud erstellt haben.
- Monitor — Verwenden Sie den Desktop-Monitor von Deadline Cloud.

Wenn Sie die Konsole verwenden, müssen Sie in der Lage sein, sich AWS mit einer AWS Identity and Access Management Identität anzumelden und sich dann mit AWS IAM Identity Center Anmeldeinformationen am Monitor anzumelden. Wenn Sie nur über IAM Identity Center-Anmeldeinformationen verfügen, müssen Sie sich mit der Monitor-URL oder der Desktop-Anwendung anmelden.

Um den Deadline Cloud-Monitor (Web) zu öffnen

1. Öffnen Sie mit einem Browser die Monitor-URL, die Sie bei der Einrichtung von Deadline Cloud erstellt haben.
2. Melden Sie sich mit Ihren Benutzeranmeldedaten an.

Um den Deadline Cloud-Monitor (Konsole) zu öffnen

1. Öffnen Sie die Deadline Cloud-Konsole.
2. Wählen Sie im Navigationsbereich Farmen aus.
3. Wählen Sie eine Farm aus und wählen Sie dann Jobs verwalten, um die Deadline Cloud-Monitorseite zu öffnen.
4. Melden Sie sich mit Ihren Benutzeranmeldedaten an.

Um den Deadline Cloud-Monitor (Desktop) zu öffnen

1. Öffnen Sie die Deadline Cloud-Konsole.

   –oder–

   Öffnen Sie den Deadline Cloud-Monitor — Web über die Monitor-URL.
2. - Gehen Sie in der Deadline Cloud-Konsole wie folgt vor:
     1. Wählen Sie im Monitor Gehe zum Deadline Cloud-Dashboard und dann im linken Menü die Option Downloads aus.
     2. Wählen Sie im Deadline Cloud-Monitor die Monitorversion für Ihren Desktop aus.
     3. Wählen Sie Herunterladen aus.
   - Gehen Sie auf dem Deadline Cloud-Monitor — Web wie folgt vor:
     - Wählen Sie im linken Menü die Option Workstation-Setup. Wenn das Workstation-Setup-Element nicht sichtbar ist, verwenden Sie den Pfeil, um das linke Menü zu öffnen.
     - Wählen Sie Herunterladen aus.
     - Wählen Sie unter Betriebssystem auswählen Ihr Betriebssystem aus.
3. Laden Sie den Deadline Cloud-Monitor für den Desktop herunter.
4. Nachdem Sie den Monitor heruntergeladen und installiert haben, öffnen Sie ihn auf Ihrem Computer.

- Wenn Sie den Deadline Cloud-Monitor zum ersten Mal öffnen, müssen Sie die Monitor-URL angeben und einen Profilnamen erstellen. Als Nächstes melden Sie sich mit Ihren Deadline Cloud-Anmeldeinformationen beim Monitor an.
- Nachdem Sie ein Profil erstellt haben, öffnen Sie den Monitor, indem Sie ein Profil auswählen. Möglicherweise müssen Sie Ihre Deadline Cloud-Anmeldeinformationen eingeben.

Warteschlangen- und Flottendetails in Deadline Cloud anzeigen

Sie können den Deadline Cloud-Monitor verwenden, um die Konfiguration der Warteschlangen und Flotten in Ihrer Farm einzusehen. Sie können den Monitor auch verwenden, um eine Liste der Jobs in einer Warteschlange oder der Arbeiter in einer Flotte anzuzeigen.

Sie müssen `VIEWING` berechtigt sein, Warteschlangen- und Flottendetails einzusehen. Wenn die Details nicht angezeigt werden, wenden Sie sich an Ihren Administrator, um die richtigen Berechtigungen zu erhalten.

Um die Details der Warteschlange einzusehen

1. Öffnen Sie den Deadline Cloud-Monitor.
2. Wählen Sie aus der Liste der Farmen die Farm aus, die die Warteschlange enthält, an der Sie interessiert sind.
3. Wählen Sie in der Liste der Warteschlangen eine Warteschlange aus, um deren Details anzuzeigen. Um die Konfiguration von zwei oder mehr Warteschlangen zu vergleichen, aktivieren Sie mehr als ein Kontrollkästchen.
4. Um eine Liste der Jobs in der Warteschlange anzuzeigen, wählen Sie den Namen der Warteschlange aus der Liste der Warteschlangen oder aus dem Detailbereich aus.

Wenn der Monitor bereits geöffnet ist, können Sie die Warteschlange aus der Warteschlangenliste im linken Navigationsbereich auswählen.

So zeigen Sie Flottendetails an:

1. Öffnen Sie den Deadline Cloud-Monitor.
2. Wählen Sie aus der Liste der Farmen die Farm aus, die die Flotte enthält, an der Sie interessiert sind.
3. Wählen Sie unter Farmressourcen die Option Flotten aus.

4. Wählen Sie in der Liste der Flotten eine Flotte aus, um deren Details anzuzeigen. Um die Konfiguration von zwei oder mehr Flotten zu vergleichen, aktivieren Sie mehr als ein Kontrollkästchen.
5. Um eine Liste der Mitarbeiter in der Flotte anzuzeigen, wählen Sie den Flottennamen aus der Flottenliste oder aus dem Detailbereich aus.

Wenn der Monitor bereits geöffnet ist, können Sie die Flotte aus der Flottenliste im linken Navigationsbereich auswählen.

Verwalten Sie Jobs, Schritte und Aufgaben in Deadline Cloud

Wenn Sie eine Warteschlange auswählen, werden Ihnen im Bereich Job Monitor des Deadline Cloud-Monitors die Jobs in dieser Warteschlange, die Schritte im Job und die Aufgaben in jedem Schritt angezeigt. Wenn Sie einen Job, einen Schritt oder eine Aufgabe auswählen, können Sie die einzelnen Jobs, Schritte oder Aufgaben über das Aktionsmenü verwalten.

Um den Auftragsmonitor zu öffnen, folgen Sie den Schritten zum Anzeigen einer WarteschlangeWarteschlangen- und Flottendetails in Deadline Cloud anzeigen, und wählen Sie dann den Job, Schritt oder die Aufgabe aus, mit dem Sie arbeiten möchten.

Für Jobs, Schritte und Aufgaben können Sie wie folgt vorgehen:

- Ändern Sie den Status in „In Warteschlange“, „Erfolgreich“, „Fehlgeschlagen“ oder „Storniert“.
- Laden Sie die verarbeitete Ausgabe des Jobs, Schritts oder der Aufgabe herunter.
- Kopieren Sie die ID des Jobs, Schritts oder der Aufgabe.

Für den ausgewählten Job können Sie:

- Archivieren Sie den Job.
- Ändern Sie die Auftragseigenschaften, z. B. indem Sie die Priorisierung ändern oder die Abhängigkeiten von Schritt zu Schritt anzeigen.
- Mithilfe der Jobparameter können Sie zusätzliche Details anzeigen.
- Reichen Sie den Job erneut ein.

Weitere Informationen finden Sie unter Jobdetails in Deadline Cloud anzeigen und verwalten.

Für jeden Schritt können Sie:

- Die Abhängigkeiten für den Schritt anzeigen. Die Abhängigkeiten für einen Schritt müssen abgeschlossen sein, bevor der Schritt ausgeführt wird.

Details hierzu finden Sie unter Einen Schritt in Deadline Cloud anzeigen.

Für jede Aufgabe können Sie:

- Protokolle für die Aufgabe anzeigen.
- Aufgabenparameter anzeigen.

Weitere Informationen finden Sie unter Eine Aufgabe in Deadline Cloud anzeigen.

Jobdetails in Deadline Cloud anzeigen und verwalten

Die Job-Monitor-Seite im Deadline Cloud-Monitor bietet Ihnen Folgendes:

- Ein Gesamtüberblick über den Fortschritt eines Jobs.
- Ein Überblick über die Schritte und Aufgaben, aus denen sich der Job zusammensetzt.

Wählen Sie einen Job aus der Liste aus, um eine Liste der Schritte für den Job anzuzeigen, und wählen Sie dann einen Schritt aus der Liste der Schritte aus, um die Aufgaben für den Job anzuzeigen. Nachdem Sie ein Element ausgewählt haben, können Sie das Aktionsmenü für dieses Element verwenden, um Details anzuzeigen.

Um Jobdetails anzuzeigen

1. Folgen Sie den Schritten, um eine Warteschlange in anzuzeigenWarteschlangen- und Flottendetails in Deadline Cloud anzeigen.
2. Wählen Sie im Navigationsbereich die Warteschlange aus, in der Sie Ihren Job eingereicht haben.
3. Wählen Sie einen Job mit einer der folgenden Methoden aus:

    a. Wählen Sie aus der Jobliste einen Job aus, um dessen Details anzuzeigen.

    b. Geben Sie im Suchfeld den Text ein, der mit dem Job verknüpft ist, z. B. den Jobnamen oder den Benutzer, der den Job erstellt hat. Wählen Sie aus den angezeigten Ergebnissen den Job aus, den Sie anzeigen möchten.

Zu den Details eines Jobs gehören die Schritte im Job und die Aufgaben in jedem Schritt. Sie können das Menü Aktionen verwenden, um Folgendes zu tun:

- Ändern Sie den Status des Jobs.
- Die Eigenschaften eines Jobs anzeigen und ändern.
  - Sie können die Abhängigkeiten zwischen den Schritten im Job anzeigen.
  - Sie können die Priorität des Jobs in einer Warteschlange ändern. Jobs mit höherer Nummernpriorität werden vor Aufträgen mit niedrigerer Nummernpriorität verarbeitet. Jobs können eine Priorität zwischen 1 und 100 haben. Wenn zwei Jobs dieselbe Priorität haben, wird der älteste Job zuerst geplant.
- Sehen Sie sich die Parameter für den Job an, die beim Absenden des Jobs festgelegt wurden.
- Laden Sie die Ausgabe eines Jobs herunter. Wenn Sie die Ausgabe eines Jobs herunterladen, enthält sie die gesamte Ausgabe, die durch die Schritte und Aufgaben im Job generiert wurde.

Archivieren Sie einen Job

Um einen Job zu archivieren, muss er sich im Terminalstatus,`FAILED`, `SUCCEEDEDSUSPENDED`, oder befinden`CANCELED`. Der `ARCHIVED` Status ist endgültig. Nachdem ein Job archiviert wurde, kann er nicht erneut in die Warteschlange gestellt oder geändert werden.

Die Daten des Jobs sind von der Archivierung des Jobs nicht betroffen. Die Daten werden gelöscht, wenn das Inaktivitäts-Timeout erreicht ist oder wenn die Warteschlange, die den Job enthält, gelöscht wird.

Andere Dinge, die mit archivierten Jobs passieren:

- Archivierte Jobs sind im Deadline Cloud-Monitor ausgeblendet.
- Archivierte Jobs sind in der Deadline Cloud-CLI 120 Tage lang schreibgeschützt sichtbar, bevor sie gelöscht werden.

Einen Job erneut in die Warteschlange stellen

Wenn Sie einen Job in die Warteschlange stellen, wechseln alle Aufgaben ohne Schrittabhängigkeiten zu. `READY` Der Status von Schritten mit Abhängigkeiten wechselt zu `READY` oder`PENDING`, wenn sie wiederhergestellt werden.

- Alle Jobs, Schritte und Aufgaben wechseln zu`PENDING`.

- Wenn ein Schritt keine Abhängigkeit hat, wechselt er zu`READY`.

Einen Job erneut einreichen

Es kann vorkommen, dass Sie einen Job erneut ausführen möchten, jedoch mit anderen Eigenschaften und Einstellungen. Sie könnten beispielsweise einen Auftrag zum Rendern einer Teilmenge von Test-Frames einreichen, die Ausgabe überprüfen und den Job dann erneut mit dem gesamten Frame-Bereich ausführen. Reichen Sie dazu den Job erneut ein.

Wenn Sie einen Job erneut einreichen, werden neue Aufgaben ohne Abhängigkeiten angezeigt. `READY` Neue Aufgaben mit Abhängigkeiten werden`PENDING`.

- Alle neuen Jobs, Schritte und Aufgaben werden`PENDING`.
- Wenn ein neuer Schritt keine Abhängigkeit hat, wird er`READY`.

Wenn Sie einen Job erneut einreichen, können Sie nur Eigenschaften ändern, die bei der ersten Erstellung des Jobs als konfigurierbar definiert wurden. Wenn beispielsweise der Name eines Jobs bei der ersten Einreichung nicht als konfigurierbare Eigenschaft des Jobs definiert wurde, kann der Name bei der erneuten Einreichung nicht bearbeitet werden.

Einen Schritt in Deadline Cloud anzeigen

Verwenden Sie den AWS Deadline Cloud-Monitor, um sich die Schritte in Ihren Verarbeitungsjobs anzusehen. Im Job-Monitor zeigt die Liste der Schritte die Liste der Schritte, aus denen sich der ausgewählte Job zusammensetzt. Wenn Sie einen Schritt auswählen, werden in der Aufgabenliste die Aufgaben des Schritts angezeigt.

Um einen Schritt anzuzeigen

1. Folgen Sie den Schritten unterJobdetails in Deadline Cloud anzeigen und verwalten, um eine Liste der Jobs anzuzeigen.
2. Wählen Sie einen Auftrag aus der Liste Jobs (Aufträge).
3. Wählen Sie einen Schritt aus der Schrittliste aus.

Sie können das Aktionsmenü verwenden, um Folgendes zu tun:

- Ändern Sie den Status des Schritts.

- Laden Sie die Ausgabe des Schritts herunter. Wenn Sie die Ausgabe eines Schritts herunterladen, enthält sie die gesamte Ausgabe, die von den Aufgaben in diesem Schritt generiert wurde.
- Sehen Sie sich die Abhängigkeiten eines Schritts an. Die Tabelle mit den Abhängigkeiten enthält eine Liste der Schritte, die abgeschlossen sein müssen, bevor der ausgewählte Schritt gestartet wird, sowie eine Liste der Schritte, die noch auf den Abschluss dieses Schritts warten.

Eine Aufgabe in Deadline Cloud anzeigen

Verwenden Sie den AWS Deadline Cloud-Monitor, um sich die Aufgaben in Ihren Verarbeitungsjobs anzusehen. Im Job-Monitor werden in der Aufgabenliste die Aufgaben angezeigt, aus denen der in der Schrittliste ausgewählte Schritt besteht.

Um eine Aufgabe anzusehen

1. Folgen Sie den Schritten unterJobdetails in Deadline Cloud anzeigen und verwalten, um eine Liste von Jobs anzuzeigen.
2. Wählen Sie einen Auftrag aus der Liste Jobs (Aufträge).
3. Wählen Sie einen Schritt aus der Schrittliste aus.
4. Wählen Sie eine Aufgabe aus der Aufgabenliste aus.

Sie können das Aktionsmenü verwenden, um Folgendes zu tun:

- Ändern Sie den Status der Aufgabe.
- Aufgabenprotokolle anzeigen. Weitere Informationen finden Sie unter Logs in Deadline Cloud anzeigen.
- Zeigt die Parameter an, die bei der Erstellung der Aufgabe festgelegt wurden.
- Laden Sie die Ausgabe der Aufgabe herunter. Wenn Sie die Ausgabe einer Aufgabe herunterladen, enthält sie nur die Ausgabe, die von der ausgewählten Aufgabe generiert wurde.

Logs in Deadline Cloud anzeigen

Logs liefern Ihnen detaillierte Informationen über den Status und die Bearbeitung von Aufgaben. Im AWS Deadline Cloud-Monitor können Sie die folgenden zwei Arten von Protokollen sehen:

- Sitzungsprotokolle beschreiben detailliert den Zeitplan der Aktionen, darunter:

  - Einrichtungsaktionen, z. B. das Synchronisieren von Anhängen und das Laden der Softwareumgebung
  - Ausführen einer Aufgabe oder einer Reihe von Aufgaben
  - Aktionen zum Schließen, z. B. das Herunterfahren der Umgebung eines Mitarbeiters

  Eine Sitzung umfasst die Bearbeitung von mindestens einer Aufgabe und kann mehrere Aufgaben umfassen. Sitzungsprotokolle enthalten auch Informationen über den Instanztyp, die vCPU und den Arbeitsspeicher von Amazon Elastic Compute Cloud (Amazon EC2). Sitzungsprotokolle enthalten auch einen Link zum Protokoll für den in der Sitzung verwendeten Worker.
- Arbeitsprotokolle enthalten Details zum Zeitplan der Aktionen, die ein Mitarbeiter während seines Lebenszyklus ausführt. Arbeitsprotokolle können Informationen über mehrere Sitzungen enthalten.

Sie können Sitzungs- und Worker-Protokolle herunterladen, um sie offline zu überprüfen.

Um Sitzungsprotokolle einzusehen

1. Folgen Sie den Schritten unterJobdetails in Deadline Cloud anzeigen und verwalten, um eine Liste der Jobs anzuzeigen.
2. Wählen Sie einen Auftrag aus der Liste Jobs (Aufträge).
3. Wählen Sie einen Schritt aus der Schrittliste aus.
4. Wählen Sie eine Aufgabe aus der Aufgabenliste aus.
5. Wählen Sie im Menü Aktionen die Option Protokolle anzeigen.

Im Abschnitt Zeitpläne wird eine Zusammenfassung der Aktionen für die Aufgabe angezeigt. Wenn Sie mehr in der Sitzung ausgeführte Aufgaben und die Aktionen zum Herunterfahren der Sitzung anzeigen möchten, wählen Sie Protokolle für alle Aufgaben anzeigen.

Um die Worker-Logs einer Aufgabe einzusehen

1. Folgen Sie den Anweisungen unterJobdetails in Deadline Cloud anzeigen und verwalten, um eine Liste der Jobs anzuzeigen.
2. Wählen Sie einen Auftrag aus der Liste Jobs (Aufträge).
3. Wählen Sie einen Schritt aus der Schrittliste aus.
4. Wählen Sie eine Aufgabe aus der Aufgabenliste aus.
5. Wählen Sie im Menü Aktionen die Option Protokolle anzeigen.

6. Wählen Sie Sitzungsinformationen aus.
7. Wählen Sie „Mitarbeiterprotokoll anzeigen“.

Um Mitarbeiterprotokolle anhand der Flottendetails anzuzeigen

1. Folgen Sie den Anweisungen unterWarteschlangen- und Flottendetails in Deadline Cloud anzeigen, um eine Flotte anzuzeigen.
2. Wählen Sie eine Mitarbeiter-ID aus der Mitarbeiterliste aus.
3. Wählen Sie im Menü „Aktionen“ die Option „Mitarbeiterprotokolle anzeigen“.

Laden Sie die fertige Ausgabe in Deadline Cloud herunter

Nach Abschluss eines Jobs können Sie den AWS Deadline Cloud-Monitor verwenden, um die Ergebnisse auf Ihre Workstation herunterzuladen. Die Ausgabedatei wird mit dem Namen und dem Speicherort gespeichert, den Sie bei der Erstellung des Jobs angegeben haben.

Ausgabedateien werden unbegrenzt gespeichert. Um die Speicherkosten zu senken, sollten Sie erwägen, eine S3-Lifecycle-Konfiguration für den Amazon S3 S3-Bucket Ihrer Warteschlange zu erstellen. Weitere Informationen finden Sie unter Verwaltung Ihres Speicherlebenszyklus im Amazon Simple Storage Service-Benutzerhandbuch.

Um die fertige Ausgabe eines Jobs, Schritts oder einer Aufgabe herunterzuladen

1. Folgen Sie den Schritten unterJobdetails in Deadline Cloud anzeigen und verwalten, um eine Liste der Jobs anzuzeigen.
2. Wählen Sie den Job, Schritt oder die Aufgabe aus, für den Sie die Ausgabe herunterladen möchten.
   - Wenn Sie einen Job auswählen, können Sie die gesamte Ausgabe für alle Aufgaben in allen Schritten für diesen Job herunterladen.
   - Wenn Sie einen Schritt auswählen, können Sie die gesamte Ausgabe für alle Aufgaben in diesem Schritt herunterladen.
   - Wenn Sie eine Aufgabe auswählen, können Sie die Ausgabe für diese einzelne Aufgabe herunterladen.
3. Wählen Sie im Menü Aktionen die Option Ausgabe herunterladen.

4. Die Ausgabe wird an den Speicherort heruntergeladen, der beim Absenden des Jobs festgelegt wurde.

> **Note**
>
> Das Herunterladen der Ausgabe über das Menü wird derzeit nur unterstützt für Windows and Linux. Wenn du eine hast Mac und wenn Sie den Menüpunkt Ausgabe herunterladen wählen, zeigt ein Fenster den AWS CLI Befehl, mit dem Sie die gerenderte Ausgabe herunterladen können.

Deadline Cloud-Farmen

Mit einer Deadline Cloud-Farm können Sie Benutzer und Projektressourcen verwalten. Eine Farm ist ein Ort, an dem sich Ihre Projektressourcen befinden. Ihre Farm besteht aus Warteschlangen und Flotten. In einer Warteschlange befinden sich eingereichte Jobs, deren Rendern geplant ist. Eine Flotte ist eine Gruppe von Worker-Knoten, die Aufgaben ausführen, um Jobs abzuschließen. Nachdem Sie eine Farm erstellt haben, können Sie Warteschlangen und Flotten erstellen, um den Anforderungen Ihres Projekts gerecht zu werden.

Erstellen Sie eine Farm

1. Wählen Sie in der Deadline Cloud-Konsole die Option Gehe zum Dashboard aus.
2. Wählen Sie im Bereich Farmen des Deadline Cloud-Dashboards Aktionen → Farm erstellen aus.
   - Alternativ können Sie in der linken Seitenleiste Farmen und andere Ressourcen und dann Create Farm auswählen.
3. Füge einen Namen für deine Farm hinzu.
4. Geben Sie unter Beschreibung die Farmbeschreibung ein. Eine klare Beschreibung kann Ihnen helfen, den Zweck Ihrer Farm schnell zu ermitteln.
5. (Optional) Standardmäßig werden Ihre Daten mit einem Schlüssel verschlüsselt, der zu Ihrer eigenen Sicherheit AWS gehört und verwaltet wird. Sie können Verschlüsselungseinstellungen anpassen (erweitert) wählen, um einen vorhandenen Schlüssel zu verwenden oder einen neuen, von Ihnen verwalteten Schlüssel zu erstellen.

   Wenn Sie die Verschlüsselungseinstellungen über das Kontrollkästchen anpassen möchten, geben Sie einen AWS KMS ARN ein oder erstellen Sie einen neuen, AWS KMS indem Sie Neuen KMS-Schlüssel erstellen wählen.
6. (Optional) Wählen Sie Neues Tag hinzufügen aus, um Ihrer Farm ein oder mehrere Tags hinzuzufügen.
7. Wählen Sie „Farm erstellen“. Nach der Erstellung wird Ihre Farm angezeigt.

Deadline Cloud-Warteschlangen

Eine Warteschlange ist eine Farmressource, die Jobs verwaltet und verarbeitet.

Um mit Warteschlangen arbeiten zu können, sollten Sie bereits einen Monitor und eine Farm eingerichtet haben.

Themen

Erstellen einer Warteschlange

1. Wählen Sie im Dashboard der Deadline Cloud-Konsole die Farm aus, für die Sie eine Warteschlange erstellen möchten.
   - Sie können auch auf der linken Seite Farmen und andere Ressourcen auswählen und dann die Farm auswählen, für die Sie eine Warteschlange erstellen möchten.
2. Wählen Sie auf der Registerkarte Warteschlangen die Option Warteschlange erstellen aus.
3. Geben Sie einen Namen für Ihre Warteschlange ein.
4. Geben Sie unter Beschreibung die Beschreibung der Warteschlange ein. Eine Beschreibung hilft Ihnen dabei, den Zweck Ihrer Warteschlange zu identifizieren.
5. Für Job-Anhänge können Sie entweder einen neuen Amazon S3 S3-Bucket erstellen oder einen vorhandenen Amazon S3 S3-Bucket auswählen.
   a. Um einen neuen Amazon S3 S3-Bucket zu erstellen
      i. Wählen Sie Neuen Job-Bucket erstellen aus.
      ii. Geben Sie einen Namen für den Bucket ein. Wir empfehlen, dem Bucket einen Namen zu gebendeadlinecloud-job-attachments-[MONITORNAME].
      iii. Geben Sie ein Root-Präfix ein, um den Stammspeicherort Ihrer Warteschlange zu definieren oder zu ändern.
   b. Um einen vorhandenen Amazon S3 S3-Bucket auszuwählen

i. Wählen Sie „Bestehenden S3-Bucket auswählen“ > „S3 durchsuchen“.

ii. Wählen Sie den S3-Bucket für Ihre Warteschlange aus der Liste der verfügbaren Buckets aus.

6. (Optional) Um Ihre Warteschlange einer vom Kunden verwalteten Flotte zuzuordnen, wählen Sie Zuordnung zu kundenverwalteten Flotten aktivieren aus.

7. Wenn Sie die Zuordnung zu kundenverwalteten Flotten aktivieren, müssen Sie die folgenden Schritte ausführen.

> **Important**
>
> Es wird dringend empfohlen, Benutzer und Gruppen für die Run-as-Funktionalität anzugeben. Wenn Sie dies nicht tun, wird die Sicherheitslage Ihrer Farm beeinträchtigt, da die Jobs dann alles tun können, was der Agent des Arbeiters tun kann. Weitere Informationen zu den potenziellen Sicherheitsrisiken finden Sie unter Jobs als Benutzer und Gruppen ausführen.

a. Für Als Benutzer ausführen:

Um Anmeldeinformationen für die Jobs der Warteschlange anzugeben, wählen Sie „In Warteschlange konfigurierter Benutzer“ aus.

Oder wählen Sie Worker Agent-Benutzer aus, wenn Sie nicht möchten, dass Sie Ihre eigenen Anmeldeinformationen festlegen und Jobs als Worker Agent-Benutzer ausführen.

b. (Optional) Geben Sie für Als Benutzeranmeldedaten ausführen einen Benutzernamen und einen Gruppennamen ein, um die Anmeldeinformationen für die Jobs der Warteschlange bereitzustellen.

Wenn Sie eine verwenden Windows Fleet, Sie müssen ein AWS Secrets Manager Geheimnis erstellen, das das Passwort für „Als Benutzer ausführen“ enthält. Wenn Sie kein vorhandenes Geheimnis mit dem Passwort haben, wählen Sie Create Secret aus, um die Secrets Manager-Konsole zu öffnen und ein Geheimnis zu erstellen.

8. Wenn Sie ein Budget angeben, können Sie die Kosten für Ihre Warteschlange besser verwalten. Wählen Sie entweder Kein Budget erforderlich oder Budget erforderlich aus.

9. Ihre Warteschlange benötigt die Erlaubnis, in Ihrem Namen auf Amazon S3 zuzugreifen. Sie können eine neue Servicerolle erstellen oder eine bestehende Servicerolle verwenden. Wenn Sie noch keine Servicerolle haben, erstellen und verwenden Sie eine neue Servicerolle.

    a. Um eine bestehende Servicerolle zu verwenden, wählen Sie eine Servicerolle auswählen und wählen Sie dann eine Rolle aus der Dropdownliste aus.

    b. Um eine neue Servicerolle zu erstellen, wählen Sie Neue Servicerolle erstellen und verwenden aus und geben Sie dann einen Rollennamen und eine Beschreibung ein.

10. (Optional) Um Umgebungsvariablen für die Warteschlangenumgebung hinzuzufügen, wählen Sie Neue Umgebungsvariable hinzufügen und geben Sie dann einen Namen und einen Wert für jede hinzugefügte Variable ein.

11. (Optional) Wählen Sie Neues Tag hinzufügen aus, um Ihrer Warteschlange ein oder mehrere Tags hinzuzufügen.

12. Um einen Standard zu erstellen Conda Warteschlangenumgebung: Lassen Sie das Kontrollkästchen aktiviert. Weitere Informationen zu Warteschlangenumgebungen finden Sie unter Eine Warteschlangenumgebung erstellen. Wenn Sie eine Warteschlange für eine vom Kunden verwaltete Flotte erstellen, deaktivieren Sie das Kontrollkästchen.

13. Wählen Sie Create queue (Warteschlange erstellen) aus.

Erstellen Sie eine Warteschlangenumgebung

Eine Warteschlangenumgebung besteht aus einer Reihe von Umgebungsvariablen und Befehlen, mit denen Flottenarbeiter eingerichtet werden. Sie können Warteschlangenumgebungen verwenden, um Softwareanwendungen, Umgebungsvariablen und andere Ressourcen für Jobs in der Warteschlange bereitzustellen.

Wenn Sie eine Warteschlange erstellen, haben Sie die Möglichkeit, eine Standardwarteschlange zu erstellen Conda Warteschlangenumgebung. Diese Umgebung bietet vom Service verwalteten Flotten Zugriff auf Pakete für DCC-Anwendungen und Renderer von Partnern. Die Standardumgebung Weitere Informationen finden Sie unter. Standard Conda Warteschlangenumgebung

Sie können Warteschlangenumgebungen mithilfe der Konsole hinzufügen oder indem Sie die JSON- oder YAML-Vorlage direkt bearbeiten. In diesem Verfahren wird beschrieben, wie Sie mit der Konsole eine Umgebung erstellen.

1. Um einer Warteschlange eine Warteschlangenumgebung hinzuzufügen, navigieren Sie zu der Warteschlange und wählen Sie die Registerkarte Warteschlangenumgebungen aus.
2. Wählen Sie „Aktionen“ und dann „Neues mit Formular erstellen“.
3. Geben Sie einen Namen und eine Beschreibung für die Warteschlangenumgebung ein.
4. Wählen Sie Neue Umgebungsvariable hinzufügen und geben Sie dann für jede hinzugefügte Variable einen Namen und einen Wert ein.
5. (Optional) Geben Sie eine Priorität für die Warteschlangenumgebung ein. Die Priorität gibt die Reihenfolge an, in der diese Warteschlangenumgebung auf dem Worker ausgeführt wird. Warteschlangenumgebungen mit höherer Priorität werden zuerst ausgeführt.
6. Wählen Sie Warteschlangenumgebung erstellen aus.

Standard Conda Warteschlangenumgebung

Wenn Sie eine Warteschlange erstellen, die mit einer vom Service verwalteten Flotte verknüpft ist, haben Sie die Möglichkeit, eine standardmäßige Warteschlangenumgebung hinzuzufügen, die Condaum Pakete für Ihre Jobs herunterzuladen und in einer virtuellen Umgebung zu installieren.

Wenn Sie mit der Deadline Cloud-Konsole eine Standard-Warteschlangenumgebung hinzufügen, wird die Umgebung für Sie erstellt. Wenn Sie eine Warteschlange auf andere Weise hinzufügen, z. B. mit AWS CLI oder AWS CloudFormation, müssen Sie die Warteschlangenumgebung selbst erstellen. Um sicherzustellen, dass Sie über die richtigen Inhalte für die Umgebung verfügen, finden Sie unter YAML-Vorlagendateien für die Warteschlangenumgebung weitere Informationen GitHub. Den Inhalt der Standard-Warteschlangenumgebung finden Sie in der YAML-Standarddatei für die Warteschlangenumgebung unter. GitHub

Auf GitHub dieser Website sind weitere Vorlagen für Warteschlangenumgebungen verfügbar, die Sie als Ausgangspunkt für Ihre eigenen Bedürfnisse verwenden können.

Conda stellt Pakete von Kanälen bereit. Ein Kanal ist ein Ort, an dem Pakete gespeichert werden. Deadline Cloud stellt einen Kanal bereit`deadline-cloud`, der hostet Conda Pakete, die DCC-Anwendungen und -Renderer von Partnern unterstützen. Wählen Sie unten die einzelnen Tabs aus, um die verfügbaren Pakete für anzuzeigen Linux or Windows.

Linux

- Blender
  - `blender=3.6`

    - `blender=4.2`
    - `blender-openjd`
- Houdini
    - `houdini=19.5`
    - `houdini=20.0`
    - `houdini=20.5`
    - `houdini-openjd`
- Maya
    - `maya=2024`

      `maya=2025`
    - `maya-mtoa=2024.5.3`

      `maya-mtoa=2025.5.4`
    - `maya-openjd`
- Atombombe
    - `nuke=15`
    - `nuke-openjd`

Windows

- After Effects
    - `aftereffects=24.6`
    - `aftereffects=25.1`
- Cinema 4D
    - `cinema4d=2024`
    - `cinema4d=2025`
    - `cinema4d-openjd`
- KeyShot
    - `keyshot=2024`
    - `keyshot-openjd`

Wenn Sie einen Job an eine Warteschlange mit der Standardeinstellung senden Conda Umgebung, die Umgebung fügt dem Job zwei Parameter hinzu. Diese Parameter spezifizieren Conda Pakete und Kanäle, die zur Konfiguration der Auftragsumgebung verwendet werden, bevor Aufgaben verarbeitet werden. Die Parameter sind:

- `CondaPackages`— eine durch Leerzeichen getrennte Liste von Paketspezifikationen, wie z. B. `blender=3.6` oder`numpy>1.22`. Die Standardeinstellung ist leer, um die Erstellung einer virtuellen Umgebung zu überspringen.
- `CondaChannels`— eine durch Leerzeichen getrennte Liste von Conda Kanäle wie`deadline-cloud`,`conda-forge`, oder`s3://amzn-s3-demo-bucket/conda/channel`. Die Standardeinstellung ist ein Kanal`deadline-cloud`, der für vom Service verwaltete Flotten verfügbar ist und DCC-Anwendungen und Renderer von Partnern bereitstellt.

Wenn Sie einen integrierten Einreicher verwenden, um einen Job von Ihrem DCC an Deadline Cloud zu senden, füllt der Absender den Wert des Parameters auf der Grundlage der DCC-Anwendung und des Absenders aus. `CondaPackages` Wenn Sie beispielsweise Blender verwenden, ist der Parameter auf eingestellt. `CondaPackage` `blender=3.6.* blender-openjd=0.4.*`

Ordnen Sie eine Warteschlange und eine Flotte zu

Eine Warteschlange muss einer Flotte zugeordnet sein, damit die Jobs gerendert werden können. Eine einzelne Flotte kann mehrere Warteschlangen unterstützen, und eine Warteschlange kann von mehreren Flotten unterstützt werden. Gehen Sie wie folgt vor, um eine bestehende Warteschlange einer vorhandenen Flotte zuzuordnen.

1. Wählen Sie in Ihrer Deadline Cloud-Farm die Warteschlange aus, die Sie einer Flotte zuordnen möchten. Die Warteschlange wird angezeigt.
2. Um eine Flotte auszuwählen, die mit Ihrer Warteschlange verknüpft werden soll, wählen Sie „Flotten zuordnen“.
3. Wählen Sie das Drop-down-Menü „Flotten auswählen“. Eine Liste der verfügbaren Flotten wird angezeigt.
4. Wählen Sie in der Liste der verfügbaren Flotten das Kontrollkästchen neben der Flotte oder den Flotten aus, die Sie Ihrer Warteschlange zuordnen möchten.
5. Wählen Sie Associate aus. Der Flottenzuordnungsstatus sollte jetzt Assoziiert lauten.

Deadline Cloud-Flotten

In diesem Abschnitt wird erklärt, wie Sie servicemanagierte Flotten und kundenverwaltete Flotten (CMF) für Deadline Cloud verwalten.

Sie können zwei Arten von Deadline Cloud-Flotten einrichten:

- Serviceverwaltete Flotten sind Flotten von Mitarbeitern, deren Standardeinstellungen von diesem Service, Deadline Cloud, bereitgestellt werden. Diese Standardeinstellungen sind so konzipiert, dass sie effizient und kostengünstig sind.
- Kundenverwaltete Flotten (CMFs) bieten Ihnen die volle Kontrolle über Ihre Verarbeitungspipeline. Ein CMF kann sich innerhalb der AWS Infrastruktur, vor Ort oder in einem Rechenzentrum an einem anderen Standort befinden. Dazu gehören die Bereitstellung, der Betrieb, die Verwaltung und die Außerbetriebnahme der Mitarbeiter der Flotte.

Themen

Servicemanagierte Flotten

Eine servicemanaged Fleet (SMF) ist eine Flotte von Mitarbeitern, deren Standardeinstellungen von Deadline Cloud bereitgestellt werden. Diese Standardeinstellungen sind so konzipiert, dass sie effizient und kostengünstig sind.

Einige der Standardeinstellungen begrenzen die Zeit, in der Mitarbeiter und Aufgaben ausgeführt werden können. Ein Worker kann nur sieben Tage lang ausgeführt werden und eine Aufgabe kann nur fünf Tage lang ausgeführt werden. Wenn das Limit erreicht ist, wird die Aufgabe oder der Worker beendet. In diesem Fall verlieren Sie möglicherweise die Arbeit, die der Worker oder die Aufgabe ausgeführt hat. Um dies zu vermeiden, sollten Sie Ihre Mitarbeiter und Aufgaben überwachen, um sicherzustellen, dass sie die Höchstdauer nicht überschreiten. Weitere Informationen zur Überwachung Ihrer Mitarbeiter finden Sie unterDen Deadline Cloud-Monitor verwenden.

Richten Sie eine Flotte mit Servicemanagement ein

1. Navigieren Sie in der Deadline Cloud-Konsole zu der Farm, in der Sie die Flotte erstellen möchten.
2. Wählen Sie die Registerkarte Flotten und dann Flotte erstellen aus.
3. Geben Sie einen Namen für Ihre Flotte ein.
4. (Optional) Geben Sie eine Beschreibung ein. Eine klare Beschreibung kann Ihnen helfen, den Zweck Ihrer Flotte schnell zu erkennen.
5. Wählen Sie den Typ „Serviceverwaltete Flotte“ aus.
6. Wählen Sie für Ihre Flotte entweder die Option „Spot“ oder „On-Demand-Instance-Markt“. Spot-Instances sind unreservierte Kapazität, die Sie zu einem vergünstigten Preis nutzen können, die jedoch durch On-Demand-Anfragen unterbrochen werden kann. On-Demand-Instances werden sekundengenau berechnet, sind jedoch nicht langfristig gebunden und werden nicht unterbrochen. Standardmäßig verwenden Flotten Spot-Instances.
7. Wählen Sie für den Servicezugriff für Ihre Flotte eine bestehende Rolle aus oder erstellen Sie eine neue Rolle. Eine Servicerolle stellt Anmeldeinformationen für Instances in der Flotte bereit und gewährt ihnen die Erlaubnis, Jobs zu verarbeiten, sowie für Benutzer im Monitor, sodass sie Protokollinformationen lesen können.
8. Wählen Sie Weiter.
9. Wählen Sie zwischen reinen CPU-Instances und GPU-beschleunigten Instances. GPU-beschleunigte Instances können Ihre Jobs möglicherweise schneller verarbeiten, können aber teurer sein.
10. Wählen Sie das Betriebssystem für Ihre Mitarbeiter aus. Sie können die Standardeinstellung Linux beibehalten oder wählen Windows.
11. (Optional) Wenn Sie GPU-beschleunigte Instanzen ausgewählt haben, legen Sie für jede Instanz die Höchst- und Mindestanzahl GPUs fest. Zu Testzwecken sind Sie auf eine GPU beschränkt. Weitere Informationen zu Ihren Produktions-Workloads finden Sie unter Beantragung einer Kontingenterhöhung im Servicekontingents-Benutzerhandbuch.
12. Geben Sie die minimalen und maximalen vCPUs ein, die Sie für Ihre Flotte benötigen.
13. Geben Sie den minimalen und maximalen Arbeitsspeicher ein, den Sie für Ihre Flotte benötigen.
14. (Optional) Sie können bestimmte Instance-Typen zulassen oder von Ihrer Flotte ausschließen, um sicherzustellen, dass nur diese Instance-Typen für diese Flotte verwendet werden.
15. (Optional) Legen Sie die maximale Anzahl von Instances fest, um die Flotte so zu skalieren, dass Kapazität für die Jobs in der Warteschlange verfügbar ist. Wir empfehlen, die Mindestanzahl an

Instances beizubehalten, **0** um sicherzustellen, dass die Flotte alle Instances freigibt, wenn sich keine Jobs in der Warteschlange befinden.

16. (Optional) Sie können die Größe des GP3-Volumes von Amazon Elastic Block Store (Amazon EBS) angeben, das den Mitarbeitern in dieser Flotte zugewiesen wird. Weitere Informationen finden Sie im EBS-Benutzerhandbuch.
17. Wählen Sie Weiter.
18. (Optional) Definieren Sie benutzerdefinierte Worker-Funktionen, die Funktionen dieser Flotte definieren und mit benutzerdefinierten Hostfunktionen kombiniert werden können, die bei der Auftragsübermittlung angegeben werden. Ein Beispiel ist ein bestimmter Lizenztyp, wenn Sie Ihre Flotte mit Ihrem eigenen Lizenzserver verbinden möchten.
19. Wählen Sie Weiter.
20. (Optional) Um Ihre Flotte einer Warteschlange zuzuordnen, wählen Sie eine Warteschlange aus der Dropdownliste aus. Wenn die Warteschlange mit der Standardeinstellung eingerichtet ist Conda Warteschlangenumgebung: Ihre Flotte wird automatisch mit Paketen versorgt, die DCC-Anwendungen und -Renderer von Partnern unterstützen. Eine Liste der bereitgestellten Pakete finden Sie unter. Standard Conda Warteschlangenumgebung
21. Wählen Sie Weiter.
22. (Optional) Um Ihrer Flotte ein Tag hinzuzufügen, wählen Sie Neues Tag hinzufügen und geben Sie dann den Schlüssel und den Wert für dieses Tag ein.
23. Wählen Sie Weiter.
24. Überprüfen Sie Ihre Flotteneinstellungen und wählen Sie dann Flotte erstellen.

Verwenden Sie einen GPU-Beschleuniger

Sie können Worker-Hosts in Ihren vom Service verwalteten Flotten so konfigurieren, dass sie einen oder mehrere verwenden GPUs, um die Verarbeitung Ihrer Jobs zu beschleunigen. Die Verwendung eines Accelerators kann die Zeit reduzieren, die für die Bearbeitung eines Jobs benötigt wird, kann aber auch die Kosten für jede Worker-Instanz erhöhen. Sie sollten Ihre Workloads testen, um die Kompromisse zwischen einer Flotte, die GPU-Beschleuniger verwendet, und Flotten, die dies nicht tun, zu verstehen.

> **Note**
>
> Zu Testzwecken sind Sie auf eine GPU beschränkt. Weitere Informationen zu Ihren Produktions-Workloads finden Sie unter Beantragung einer Kontingenterhöhung im Servicekontingents-Benutzerhandbuch.

Sie entscheiden, ob Ihre Flotte GPU-Beschleuniger verwenden wird, wenn Sie die Worker-Instance-Funktionen angeben. Wenn Sie sich für die Verwendung entscheiden GPUs, können Sie GPUs für jede Instanz die Mindest- und Höchstanzahl von GPU-Chips, die verwendet werden sollen, und den Laufzeittreiber für die GPUs angeben.

Die verfügbaren GPU-Beschleuniger sind:

- `T4`- NVIDIA T4 Tensor Core-GPU
- `A10G`- NVIDIA A10G Tensorkern-GPU
- `L4`- NVIDIA L4 Tensorkern-GPU
- `L40s`- NVIDIA L40S Tensorkern-GPU

Sie können aus den folgenden Runtime-Treibern wählen:

- `Latest`- Verwenden Sie die neueste verfügbare Laufzeit für den Chip. Wenn Sie angeben `latest` und eine neue Version der Runtime veröffentlicht wird, wird die neue Version der Runtime verwendet.
- `GRID:R550`- NVIDIA vGPU-Software 17
- `GRID:R535`- NVIDIA vGPU-Software 16

Wenn Sie keine Laufzeit angeben, verwendet Deadline Cloud diese `latest` standardmäßig. Wenn Sie jedoch mehrere Beschleuniger haben und `latest` für einige angeben und andere leer lassen, löst Deadline Cloud eine Ausnahme aus.

Softwarelizenzierung für servicemanagierte Flotten

Deadline Cloud bietet nutzungsbasierte Lizenzierung (UBL) für häufig verwendete Softwarepakete. Unterstützte Softwarepakete werden automatisch lizenziert, wenn sie auf einer vom Service verwalteten Flotte ausgeführt werden. Sie müssen keinen Softwarelizenzserver konfigurieren oder

verwalten. Die Lizenzen lassen sich skalieren, sodass Ihnen die Kapazitäten für größere Aufträge nicht ausgehen.

Sie können Softwarepakete, die UBL unterstützen, über den integrierten Deadline Cloud-Conda-Kanal installieren, oder Sie können Ihre eigenen Pakete verwenden. Weitere Informationen zum Conda-Kanal finden Sie unter. Erstellen Sie eine Warteschlangenumgebung

Eine Liste der unterstützten Softwarepakete und Informationen zu den Preisen für UBL finden Sie unter AWS Deadline Cloud-Preise.

Bringen Sie bei vom Service verwalteten Flotten Ihre eigene Lizenz mit

Mit der nutzungsbasierten Lizenzierung (UBL) von Deadline Cloud müssen Sie keine separaten Lizenzvereinbarungen mit Softwareanbietern abschließen. Wenn Sie jedoch über bestehende Lizenzen verfügen oder Software verwenden müssen, die nicht über UBL verfügbar ist, können Sie Ihre eigenen Softwarelizenzen mit Ihren vom Service verwalteten Deadline Cloud-Flotten verwenden. Sie verbinden Ihr SMF über das Internet mit dem Softwarelizenzserver, um für jeden Mitarbeiter in der Flotte eine Lizenz auszuchecken.

Ein Beispiel für die Verbindung zu einem Lizenzserver mithilfe eines Proxys finden Sie unter Vom Service verwaltete Flotten mit einem benutzerdefinierten Lizenzserver Connect im Deadline Cloud Developer Guide.

VFX Reference Platform Kompatibilität

Das Tool VFX Reference Platform ist eine gemeinsame Zielplattform für die VFX-Branche. Um die standardmäßige EC2 Service-Managed-Flotten-Amazon-Instance zu verwenden, auf der Amazon Linux 2023 ausgeführt wird, mit Software, die VFX Reference Platform, sollten Sie bei der Verwendung einer serviceverwalteten Flotte die folgenden Überlegungen berücksichtigen.

Das Tool VFX Reference Platform wird jährlich aktualisiert. Diese Überlegungen zur Nutzung einer vom Service verwalteten Flotten vom Typ AL2 023 einschließlich Deadline Cloud basieren auf den Referenzplattformen für das Kalenderjahr (CY) 2022 bis 2024. Weitere Informationen finden Sie unter VFX Reference Platform.

> **Note**
>
> Wenn Sie ein benutzerdefiniertes erstellen Amazon Machine Image (AMI) für eine vom Kunden verwaltete Flotte können Sie diese Anforderungen hinzufügen, wenn Sie die EC2 Amazon-Instance vorbereiten.

Zur Verwendung VFX Reference Platform unterstützte Software auf einer AL2 EC2 023-Amazon-Instance. Beachten Sie Folgendes:

- Die mit AL2 0.23 installierte Glibc-Version ist für die Runtime-Nutzung kompatibel, aber nicht für die Erstellung von Software, die kompatibel ist mit VFX Reference Platform CY2024 oder früher.
- Python 3.9 und 3.11 werden mit der service-verwalteten Flotte geliefert und sind somit kompatibel mit VFX Reference Platform CY2022 und 024. CY2 Python 3.7 und 3.10 sind in der Service-Managed-Flotte nicht enthalten. Software, die sie benötigt, muss die Python-Installation in der Warteschlangen- oder Jobumgebung bereitstellen.
- Bei einigen Komponenten der Boost-Bibliothek, die in der vom Service verwalteten Flotte enthalten sind, handelt es sich um Version 1.75, die nicht kompatibel ist mit VFX Reference Platform. Wenn Ihre Anwendung Boost verwendet, müssen Sie aus Kompatibilitätsgründen Ihre eigene Version der Bibliothek bereitstellen.
- Intel TBB Update 3 ist Teil der Service-Managed-Flotte. Das ist kompatibel mit VFX Reference Platform CY2022, CY2 023 und CY2 024.
- Andere Bibliotheken mit Versionen spezifiziert durch VFX Reference Platform werden nicht von der vom Service verwalteten Flotte bereitgestellt. Sie müssen der Bibliothek alle Anwendungen zur Verfügung stellen, die in einer Flotte mit verwaltetem Service verwendet werden. Eine Liste der Bibliotheken finden Sie auf der Referenzplattform.

Kundenverwaltete Flotten

Wenn Sie eine Flotte von Mitarbeitern verwenden möchten, die Sie verwalten, können Sie eine vom Kunden verwaltete Flotte (CMF) erstellen, die Deadline Cloud zur Bearbeitung Ihrer Jobs verwendet. Verwenden Sie ein CMF, wenn:

- Sie haben bereits Mitarbeiter vor Ort, die Sie in Deadline Cloud integrieren möchten.
- Sie haben Mitarbeiter in einem Rechenzentrum am gleichen Standort.
- Sie möchten die direkte Kontrolle über die Mitarbeiter von Amazon Elastic Compute Cloud (Amazon EC2) haben.

Wenn Sie ein CMF verwenden, haben Sie die volle Kontrolle über und Verantwortung für die Flotte. Dazu gehören die Bereitstellung, der Betrieb, die Verwaltung und die Außerbetriebnahme der Mitarbeiter in der Flotte.

Weitere Informationen finden Sie unter Kundenverwaltete Flotten von Deadline Cloud erstellen und verwenden im Deadline Cloud Developer Guide.

Benutzer in Deadline Cloud verwalten

AWS Deadline Cloud verwendet AWS IAM Identity Center , um Benutzer und Gruppen zu verwalten. IAM Identity Center ist ein cloudbasierter Single-Sign-On-Service, der in Ihren Enterprise-Single-Sign-On-Anbieter (SSO) integriert werden kann. Mit der Integration können sich Benutzer mit ihrem Unternehmenskonto anmelden.

Deadline Cloud aktiviert IAM Identity Center standardmäßig und ist für die Einrichtung und Verwendung von Deadline Cloud erforderlich. Weitere Informationen finden Sie unter Ihre Identitätsquelle verwalten.

Ein Organisationsinhaber für Sie AWS Organizations ist für die Verwaltung der Benutzer und Gruppen verantwortlich, die Zugriff auf Ihren Deadline Cloud-Monitor haben. Sie können diese Benutzer und Gruppen mithilfe von IAM Identity Center oder der Deadline Cloud-Konsole erstellen und verwalten. Weitere Informationen finden Sie unter Was ist AWS Organizations.

Mithilfe der Deadline Cloud-Konsole können Sie Benutzer und Gruppen erstellen und entfernen, die Farmen, Warteschlangen und Flotten verwalten können. Wenn Sie einen Benutzer zu Deadline Cloud hinzufügen, muss er sein Passwort mithilfe von IAM Identity Center zurücksetzen, bevor er Zugriff erhält.

Themen

Benutzer und Gruppen für den Monitor verwalten

Ein Organisationsinhaber kann die Deadline Cloud-Konsole verwenden, um die Benutzer und Gruppen zu verwalten, die Zugriff auf den Deadline Cloud-Monitor haben. Sie können aus vorhandenen IAM Identity Center-Benutzern und -Gruppen wählen oder neue Benutzer und Gruppen über die Konsole hinzufügen.

1. Melden Sie sich bei der Deadline Cloud-Konsole an AWS Management Console und öffnen Sie sie. Wählen Sie auf der Hauptseite im Bereich Erste Schritte die Option Deadline Cloud einrichten oder Gehe zum Dashboard.
2. Wählen Sie im linken Navigationsbereich Benutzerverwaltung aus. Standardmäßig ist die Registerkarte Gruppen ausgewählt.

Wählen Sie je nach der auszuführenden Aktion entweder die Registerkarte Gruppen oder die Registerkarte Benutzer.

Groups

So erstellen Sie eine Gruppe

1. Wählen Sie Create group (Gruppe erstellen) aus.
2. Geben Sie einen Gruppennamen ein. Der Name muss für alle Gruppen in Ihrer IAM Identity Center-Organisation eindeutig sein.

Um eine Gruppe zu entfernen

1. Wählen Sie die Gruppe aus, die Sie entfernen möchten.
2. Wählen Sie Remove (Entfernen) aus.
3. Wählen Sie im Bestätigungsdialogfeld die Option Gruppe entfernen aus.

> **Note**
>
> Sie entfernen die Gruppe aus dem IAM Identity Center. Gruppenmitglieder können sich nicht mehr bei der Deadline Cloud anmelden oder auf Farmressourcen zugreifen.

Users

So fügen Sie Benutzer hinzu

1. Wählen Sie die Registerkarte Users.
2. Wählen Sie Add Users (Benutzer hinzufügen).
3. Geben Sie den Namen, die E-Mail-Adresse und den Benutzernamen für den neuen Benutzer ein.
4. (Optional) Wählen Sie eine oder mehrere IAM Identity Center-Gruppen aus, zu denen der neue Benutzer hinzugefügt werden soll.
5. Wählen Sie Einladung senden, um dem neuen Benutzer eine E-Mail mit Anweisungen zum Beitritt zu Ihrer IAM Identity Center-Organisation zu senden.

So entfernen Sie einen Benutzer:

1. Wählen Sie den Benutzer aus, den Sie entfernen möchten.
2. Wählen Sie Remove (Entfernen) aus.
3. Wählen Sie im Bestätigungsdialogfeld die Option Benutzer entfernen aus.

> **Note**
>
> Sie entfernen den Benutzer aus IAM Identity Center. Der Benutzer kann sich nicht mehr beim Deadline Cloud-Monitor anmelden oder auf Farmressourcen zugreifen.

Verwalten Sie Benutzer und Gruppen für Farmen, Warteschlangen und Flotten

Im Rahmen der Verwaltung von Benutzern und Gruppen können Sie Zugriffsberechtigungen auf verschiedenen Ebenen gewähren. Jede nachfolgende Ebene umfasst die Berechtigungen für die vorherigen Ebenen. In der folgenden Liste werden die vier Zugriffsebenen von der niedrigsten bis zur höchsten Ebene beschrieben:

- Zuschauer — Berechtigung zum Anzeigen von Ressourcen in den Farmen, Warteschlangen, Flotten und Aufträgen, auf die sie Zugriff haben. Ein Zuschauer kann keine Jobs einreichen oder Änderungen daran vornehmen.
- Mitwirkender — Identisch mit einem Betrachter, aber mit der Erlaubnis, Jobs an eine Warteschlange oder Farm zu senden.
- Manager — Identisch mit dem Mitwirkenden, aber mit der Berechtigung, Jobs in Warteschlangen zu bearbeiten, auf die er Zugriff hat, und Berechtigungen für Ressourcen zu erteilen, auf die er Zugriff hat.
- Besitzer — Identisch mit dem Manager, kann jedoch Budgets anzeigen und erstellen und deren Nutzung einsehen.

> **Note**
>
> Es kann bis zu 10 Minuten dauern, bis Änderungen an den Zugriffsberechtigungen im System übernommen werden.

1. Falls Sie dies noch nicht getan haben, melden Sie sich bei der Deadline Cloud-Konsole an AWS Management Console und öffnen Sie sie.
2. Wählen Sie im linken Navigationsbereich Farmen und andere Ressourcen aus.
3. Wählen Sie die Farm aus, die Sie verwalten möchten. Wählen Sie den Farmnamen, um die Detailseite zu öffnen. Sie können mit der Suchleiste nach der Farm suchen.
4. Um eine Warteschlange oder Flotte zu verwalten, wählen Sie die Registerkarte Warteschlangen oder Flotten und dann die Warteschlange oder Flotte aus, die Sie verwalten möchten.
5. Wählen Sie die Registerkarte Zugriffsverwaltung. Standardmäßig ist die Registerkarte Gruppen ausgewählt. Um Benutzer zu verwalten, wählen Sie Benutzer.

Wählen Sie je nach der zu ergreifenden Aktion entweder die Registerkarte Gruppen oder die Registerkarte Benutzer.

Groups

Um Gruppen hinzuzufügen

1. Wählen Sie den Schalter Gruppen aus.
2. Wählen Sie Add Group (Gruppe hinzufügen) aus.
3. Wählen Sie aus der Dropdownliste die Gruppen aus, die Sie hinzufügen möchten.
4. Wählen Sie für die Gruppenzugriffsebene eine der folgenden Optionen aus:
   - Betrachter
   - Beitragender
   - Manager
   - Eigentümer
5. Wählen Sie Hinzufügen aus.

Um Gruppen zu entfernen

1. Wählen Sie die Gruppen aus, die Sie entfernen möchten.
2. Wählen Sie Remove (Entfernen) aus.
3. Wählen Sie im Bestätigungsdialogfeld die Option Gruppe entfernen aus.

Users

So fügen Sie Benutzer hinzu

1. Um einen Benutzer hinzuzufügen, wählen Sie Benutzer hinzufügen.
2. Wählen Sie aus der Dropdownliste die Benutzer aus, die Sie hinzufügen möchten.
3. Wählen Sie für die Benutzerzugriffsebene eine der folgenden Optionen aus:
   - Betrachter
   - Beitragender
   - Manager
   - Eigentümer
4. Wählen Sie Hinzufügen aus.

Um Benutzer zu entfernen

1. Wählen Sie den Benutzer aus, den Sie entfernen möchten.
2. Wählen Sie Remove (Entfernen) aus.
3. Wählen Sie im Bestätigungsdialogfeld die Option Benutzer entfernen aus.

Deadline Cloud-Jobs

Ein Job ist eine Reihe von Anweisungen, die AWS Deadline Cloud verwendet, um Arbeiten an verfügbaren Mitarbeitern zu planen und auszuführen. Wenn Sie einen Job erstellen, wählen Sie die Farm und die Warteschlange aus, an die der Job gesendet werden soll. Sie stellen auch eine JSON- oder YAML-Datei bereit, die Anweisungen für die Verarbeitung durch die Mitarbeiter enthält. Deadline Cloud akzeptiert Jobvorlagen, die der Open Job Description (OpenJD) -Spezifikation zur Beschreibung von Jobs folgen. Weitere Informationen finden Sie in der Dokumentation zur offenen Stellenbeschreibung auf der GitHub Website.

Ein Job besteht aus:

- Priorität — Die ungefähre Reihenfolge, in der Deadline Cloud einen Job in einer Warteschlange verarbeitet. Sie können die Job-Priorität zwischen 1 und 100 festlegen. Jobs mit einer höheren Priorität werden in der Regel zuerst verarbeitet. Jobs mit derselben Priorität werden in der Reihenfolge bearbeitet, in der sie eingegangen sind.
- Schritte — Definiert das Skript, das auf Workern ausgeführt werden soll. Für Schritte können Anforderungen wie Mindestarbeitsspeicher oder andere Schritte gelten, die zuerst abgeschlossen werden müssen. Jeder Schritt umfasst eine oder mehrere Aufgaben.
- Aufgaben — Eine Arbeitseinheit, die an einen Mitarbeiter zur Ausführung geschickt wird. Eine Aufgabe ist eine Kombination aus dem Skript eines Schritts und Parametern, wie z. B. der Frame-Nummer, die im Skript verwendet werden. Der Job ist abgeschlossen, wenn alle Aufgaben für alle Schritte abgeschlossen sind.
- Umgebungen — Richten Sie Anweisungen ein und entfernen Sie sie, wenn mehrere Schritte oder Aufgaben gemeinsam ausgeführt werden.

Sie können einen Job auf eine der folgenden Arten erstellen:

- Verwenden Sie einen Deadline Cloud-Einreicher.
- Erstellen Sie ein Job-Bundle und verwenden Sie die Deadline Cloud-Befehlszeilenschnittstelle (Deadline Cloud CLI).
- Verwenden Sie das AWS SDK.
- Verwenden Sie die AWS Command Line Interface (AWS CLI).

Ein Submitter ist ein Plugin für Ihre DCC-Software (Digital Content Creation), das die Erstellung eines Jobs in der Schnittstelle zu Ihrer DCC-Software verwaltet. Nachdem Sie den Job erstellt haben, verwenden Sie den Absender, um ihn zur Bearbeitung an Deadline Cloud zu senden. Hinter den Kulissen erstellt der Einreicher eine OpenJD-Jobvorlage, die den Job beschreibt. Gleichzeitig werden Ihre Asset-Dateien in einen Amazon Simple Storage Service (Amazon S3) -Bucket hochgeladen. Um den Zeitaufwand für das Senden von Dateien zu reduzieren, werden nur Dateien, die sich seit dem letzten Hochladen von Dateien geändert haben, an Amazon S3 gesendet.

Sie können Grenzwerte festlegen, um zu verwalten, wie Jobs eingeschränkte Ressourcen wie Softwarelizenzen nutzen. Jobs, die Limits verwenden, verwenden nur die Anzahl der Ressourcen, die unter dem Limit zulässig sind. Weitere Informationen finden Sie unter Erstellen Sie Ressourcenlimits für Jobs.

Um Ihre eigenen Skripts und Pipelines zum Senden von Jobs an Deadline Cloud zu erstellen, können Sie die Deadline Cloud-CLI, das AWS SDK oder die AWS CLI To-Call-Operationen verwenden, um Jobs zu erstellen, abzurufen, anzuzeigen und aufzulisten. In den folgenden Themen wird erklärt, wie Sie die Deadline Cloud CLI verwenden.

Die Deadline Cloud-CLI wird zusammen mit dem Deadline Cloud-Submitter installiert. Weitere Informationen finden Sie unter Deadline Cloud-Einreicher einrichten.

Themen

Jobs mit der Deadline Cloud CLI einreichen

Um einen Job über die Deadline Cloud-Befehlszeilenschnittstelle (Deadline Cloud CLI) einzureichen, verwenden Sie den `deadline bundle submit` Befehl.

Jobs werden in Warteschlangen eingereicht. Wenn Sie noch keine Farm und Warteschlange eingerichtet haben, verwenden Sie die Deadline Cloud-Konsole, um eine Farm und eine

Warteschlange einzurichten und die Farm- und Warteschlangen-ID zu sehen. Weitere Informationen finden Sie unter Farmdetails definieren und Warteschlangendetails definieren.

Verwenden Sie den folgenden Befehl, um die Standardfarm und die Warteschlange für die Deadline Cloud-CLI festzulegen. Wenn Sie die Standardeinstellungen festlegen, können Sie Deadline Cloud CLI-Befehle verwenden, ohne eine Farm oder Warteschlange anzugeben. Ersetzen Sie im folgenden Beispiel *farmId* und *queueId* durch Ihre eigenen Informationen:

```
deadline config set defaults.farm_id farmId
deadline config set defaults.queue_id queueId
```

Um die Schritte und Aufgaben in einem Job zu spezifizieren, erstellen Sie eine OpenJD-Jobvorlage. Weitere Informationen finden Sie unter Template Schemas [Version: 2023-09] im Open Job Description Specification Repository. GitHub

Das folgende Beispiel ist eine YAML-Jobvorlage. Es definiert einen Job mit zwei Schritten und fünf Aufgaben pro Schritt.

```
name: Sample Job
specificationVersion: jobtemplate-2023-09
steps:
- name: Sample Step 1
  parameterSpace:
    taskParameterDefinitions:
    - name: var
      range: 1-5
      type: INT
  script:
    actions:
      onRun:
        args:
        - '1'
        command: /usr/bin/sleep
- name: Sample Step 2
  parameterSpace:
    taskParameterDefinitions:
    - name: var
      range: 1-5
      type: INT
  script:
    actions:
      onRun:
```

```
        args:
        - '1'
        command: /usr/bin/sleep
```

Um einen Job zu erstellen, erstellen Sie einen neuen Ordner mit dem Namen `sample_job` und speichern Sie dann die Vorlagendatei im neuen Ordner unter`template.yaml`. Sie reichen den Job mit dem folgenden Deadline Cloud CLI-Befehl ein:

```
deadline bundle submit path/to/sample_job
```

Die Antwort des Befehls enthält eine Kennung für den Job. Merken Sie sich die ID, damit Sie den Status des Jobs später überprüfen können.

```
Submitting to Queue: test-queue
Waiting for Job to be created...
Submitted job bundle:
   sample_job
Job creation completed successfully
jobId
```

Es gibt zusätzliche Optionen, die Sie beim Einreichen eines Jobs verwenden können. Weitere Informationen finden Sie unter Weitere Optionen zum Einreichen von Jobs mit der Deadline Cloud CLI.

Weitere Optionen zum Einreichen von Jobs mit der Deadline Cloud CLI

Der CLI-Befehl `deadline bundle submit` Deadline Cloud bietet Optionen, mit denen Sie zusätzliche Informationen für einen Job angeben können. In den nachstehenden Beispielen wird Folgendes veranschaulicht:

- Geben Sie die Parameter an, die bei der Verarbeitung der Jobvorlage verwendet werden.
- Hängen Sie Dateien und Ordner in einer gemeinsam genutzten Umgebung an einen Job an.
- Legen Sie die maximale Anzahl von Mitarbeitern fest, die einen Job bearbeiten können.
- Legen Sie die maximale Anzahl von Aufgabenfehlern fest, bevor ein Job abgebrochen wird.
- Legen Sie die maximale Anzahl von Wiederholungen für eine Aufgabe fest.

Auftragsparameter

Die `parameters` Option legt den Wert eines Job-Parameters fest, wenn Sie den Job erstellen. Die Jobvorlage definiert das Feld, und die `parameters` Option legt den Wert fest. Ein Parameter kann einen Standardwert haben. Wenn für den Parameter ein Wert angegeben wird, überschreibt der angegebene Wert den Standardwert.

Die folgende Jobvorlage definiert das `TestParameter` Feld:

```
name: Sample Job With Job Parameter
parameterDefinitions:
- default: test
  name: TestParameter
  type: STRING
specificationVersion: jobtemplate-2023-09
steps:
- description: step description
  name: MyStep
  parameterSpace:
    taskParameterDefinitions:
    - name: var
      range: 1-5
      type: INT
  script:
    actions:
      onRun:
        args:
        - '1'
        command: /usr/bin/sleep
```

Der folgende Befehl setzt den Wert von `TestParameter` auf „Hello AWS“:

```
deadline bundle submit sample_job --parameter "TestParameter=Hello AWS"
```

Speicherprofile

Speicherprofile helfen beim Austausch von Dateien zwischen Mitarbeitern mit unterschiedlichen Betriebssystemen. Erstellen Sie mit der Deadline Cloud-Konsole ein Speicherprofil. Verwenden Sie dann den `storage-profile-id` Parameter, um das Speicherprofil zu verwenden. Weitere Informationen finden Sie unter Speicherprofile und Pfadzuweisung im Deadline Cloud Developer Guide.

Um das Speicherprofil für Jobübermittlungen mithilfe der Deadline Cloud-CLI festzulegen, verwenden Sie den folgenden Befehl, um den `storage-profile-id` Konfigurationsparameter festzulegen:

```
deadline config set settings.storage_profile_id storageProfileId
```

Maximale Anzahl an Mitarbeitern für einen Job

Die `max-worker-count` Option legt die maximale Anzahl von Arbeitskräften fest, die einem Job zugewiesen werden können. Wenn das Maximum erreicht ist, werden dem Job keine weiteren Arbeitskräfte zugewiesen, auch wenn mehr Arbeitskräfte in der Flotte verfügbar sind.

```
deadline bundle submit sample_job --max-worker-count 10
```

Maximale Anzahl fehlgeschlagener Aufgaben

Die `max-failed-tasks-count` Option legt die maximale Anzahl von Aufgaben fest, die fehlschlagen können, bevor der gesamte Job fehlschlägt und alle verbleibenden Aufgaben markiert werden`CANCELED`. Der Standardwert lautet 100.

```
deadline bundle submit sample_job --max-failed-tasks-count 10
```

Maximale Anzahl fehlgeschlagener Aufgabenwiederholungen

Die `max-retries-per-task` Option legt fest, wie oft eine Aufgabe maximal wiederholt wird, bevor sie fehlschlägt. Wenn eine Aufgabe erneut versucht wird, wird sie in den `READY` Status versetzt. Der Standardwert ist 5.

```
deadline bundle submit sample_job --max-retries-per-task 10
```

Jobs in Deadline Cloud planen

Nachdem ein Auftrag erstellt wurde, plant AWS Deadline Cloud, dass er in einer oder mehreren Flotten bearbeitet wird, die einer Warteschlange zugeordnet sind. Die Flotte, die eine bestimmte Aufgabe bearbeitet, wird auf der Grundlage der für die Flotte konfigurierten Funktionen und der Hostanforderungen eines bestimmten Schritts ausgewählt.

Jobs in einer Warteschlange werden in der Reihenfolge der bestmöglichen Priorität geplant, von der höchsten zur niedrigsten Priorität. Wenn zwei Jobs dieselbe Priorität haben, wird der älteste Job zuerst geplant.

In den folgenden Abschnitten wird detailliert beschrieben, wie ein Job geplant wird.

Prüfen Sie die Flottenkompatibilität

Nachdem ein Job erstellt wurde, vergleicht Deadline Cloud die Hostanforderungen für jeden Schritt im Job mit den Fähigkeiten der Flotten, die mit der Warteschlange verknüpft sind, an die der Job übermittelt wurde. Wenn eine Flotte die Hostanforderungen erfüllt, wird der Job in den `READY` Status versetzt.

Wenn für einen Schritt des Jobs Anforderungen gelten, die von einer Flotte, die der Warteschlange zugeordnet ist, nicht erfüllt werden können, wird der Status des Schritts auf gesetzt`NOT_COMPATIBLE`. Außerdem werden die restlichen Schritte des Jobs storniert.

Die Funktionen für eine Flotte werden auf Flottenebene festgelegt. Selbst wenn ein Mitarbeiter in einer Flotte die Anforderungen des Auftrags erfüllt, werden ihm keine Aufgaben aus dem Auftrag zugewiesen, wenn seine Flotte die Anforderungen des Auftrags nicht erfüllt.

Die folgende Jobvorlage enthält einen Schritt, der die Hostanforderungen für den Schritt spezifiziert:

```
name: Sample Job With Host Requirements
specificationVersion: jobtemplate-2023-09
steps:
- name: Step 1
  script:
    actions:
      onRun:
        args:
        - '1'
        command: /usr/bin/sleep
  hostRequirements:
    amounts:
    # Capabilities starting with "amount." are amount capabilities. If they start with
 "amount.worker.",
    # they are defined by the OpenJD specification. Other names are free for custom
 usage.
    - name: amount.worker.vcpu
      min: 4
      max: 8
    attributes:
    - name: attr.worker.os.family
      anyOf:
      - linux
```

Dieser Job kann für eine Flotte mit den folgenden Funktionen geplant werden:

```
{
    "vCpuCount": {"min": 4, "max": 8},
    "memoryMiB": {"min": 1024},
    "osFamily": "linux",
    "cpuArchitectureType": "x86_64"
}
```

Dieser Job kann nicht für eine Flotte mit einer der folgenden Funktionen geplant werden:

```
{
    "vCpuCount": {"min": 4},
    "memoryMiB": {"min": 1024},
    "osFamily": "linux",
    "cpuArchitectureType": "x86_64"
}
    The vCpuCount has no maximum, so it exceeds the maximum vCPU host requirement.

{
    "vCpuCount": {"max": 8},
    "memoryMiB": {"min": 1024},
    "osFamily": "linux",
    "cpuArchitectureType": "x86_64"
}
    The vCpuCount has no minimum, so it doesn't satisfy the minimum vCPU host
 requirement.

{
    "vCpuCount": {"min": 4, "max": 8},
    "memoryMiB": {"min": 1024},
    "osFamily": "windows",
    "cpuArchitectureType": "x86_64"
}
    The osFamily doesn't match.
```

Skalierung der Flotte

Wenn ein Auftrag einer kompatiblen, servicemanagierten Flotte zugewiesen wird, wird die Flotte auto skaliert. Die Anzahl der Mitarbeiter in der Flotte ändert sich je nach der Anzahl der Aufgaben, die der Flotte zur Ausführung zur Verfügung stehen.

Wenn ein Auftrag einer vom Kunden verwalteten Flotte zugewiesen wird, sind Mitarbeiter möglicherweise bereits vorhanden oder können mithilfe von ereignisbasierter Autoskalierung erstellt werden. Weitere Informationen finden Sie unter Verwendung EventBridge zur Behandlung von Auto Scaling-Ereignissen im Amazon EC2 Auto Scaling-Benutzerhandbuch.

Sitzungen

Die Aufgaben in einem Job sind in eine oder mehrere Sitzungen aufgeteilt. Die Mitarbeiter führen die Sitzungen durch, um die Umgebung einzurichten, die Aufgaben auszuführen und dann die Umgebung zu zerstören. Jede Sitzung besteht aus einer oder mehreren Aktionen, die ein Mitarbeiter ausführen muss.

Wenn ein Mitarbeiter Abschnittsaktionen abschließt, können zusätzliche Sitzungsaktionen an den Mitarbeiter gesendet werden. Der Mitarbeiter verwendet in der Sitzung vorhandene Umgebungen und Jobanhänge wieder, um Aufgaben effizienter zu erledigen.

Jobanhänge werden vom Einreicher erstellt, den Sie als Teil Ihres Deadline Cloud CLI-Jobpakets verwenden. Mit der `--attachments` Option für den Befehl können Sie auch Jobanhänge erstellen. `create-job` AWS CLI Umgebungen werden an zwei Stellen definiert: Warteschlangenumgebungen, die an eine bestimmte Warteschlange angehängt sind, und Job- und Schrittumgebungen, die in der Jobvorlage definiert sind.

Es gibt vier Arten von Sitzungsaktionen:

- `syncInputJobAttachments`— Lädt die Eingabe-Job-Anhänge an den Worker herunter.
- `envEnter`— Führt die `onEnter` Aktionen für eine Umgebung aus.
- `taskRun`— Führt die `onRun` Aktionen für eine Aufgabe aus.
- `envExit`— Führt die `onExit` Aktionen für eine Umgebung aus.

Die folgende Jobvorlage hat eine Schrittumgebung. Sie enthält eine `onEnter` Definition zum Einrichten der Schrittumgebung, eine `onRun` Definition, die die auszuführende Aufgabe definiert, und eine `onExit` Definition zum Abbau der Schrittumgebung. Die für diesen Job erstellten Sitzungen umfassen eine `envEnter` Aktion, eine oder mehrere `taskRun` Aktionen und dann eine `envExit` Aktion.

```
name: Sample Job with Maya Environment
specificationVersion: jobtemplate-2023-09
steps:
- name: Maya Step
```

```
  stepEnvironments:
  - name: Maya
    description: Runs Maya in the background.
    script:
      embeddedFiles:
      - name: initData
        filename: init-data.yaml
        type: TEXT
        data: |
          scene_file: MyAwesomeSceneFile
          renderer: arnold
          camera: persp
      actions:
        onEnter:
          command: MayaAdaptor
          args:
          - daemon
          - start
          - --init-data
          - file://{{Env.File.initData}}
        onExit:
          command: MayaAdaptor
          args:
          - daemon
          - stop
  parameterSpace:
    taskParameterDefinitions:
    - name: Frame
      range: 1-5
      type: INT
  script:
    embeddedFiles:
    - name: runData
      filename: run-data.yaml
      type: TEXT
      data: |
        frame: {{Task.Param.Frame}}
    actions:
      onRun:
        command: MayaAdaptor
        args:
        - daemon
        - run
        - --run-data
```

```
        - file://{{ Task.File.runData }}
```

Abhängigkeiten der einzelnen Schritte

Deadline Cloud unterstützt die Definition von Abhängigkeiten zwischen Schritten, sodass ein Schritt wartet, bis ein anderer Schritt abgeschlossen ist, bevor er gestartet wird. Sie können mehr als eine Abhängigkeit für einen Schritt definieren. Ein Schritt mit einer Abhängigkeit wird erst geplant, wenn alle Abhängigkeiten abgeschlossen sind.

Wenn die Jobvorlage eine zirkuläre Abhängigkeit definiert, wird der Job abgelehnt und der Jobstatus wird auf gesetzt`CREATE_FAILED`.

Mit der folgenden Jobvorlage wird ein Job in zwei Schritten erstellt. `StepB`hängt davon ab`StepA`. `StepB`wird erst ausgeführt, nachdem der `StepA` Vorgang erfolgreich abgeschlossen wurde.

Nachdem der Job erstellt wurde, `StepA` befindet er sich im `READY` Status und `StepB` befindet sich im `PENDING` Status. Wenn der `StepA` Vorgang abgeschlossen ist, `StepB` wechselt er in den `READY` Status. `StepA`Schlägt fehl oder wurde der `StepA` Vorgang abgebrochen, `StepB` wechselt er in den `CANCELED` Status.

Sie können eine Abhängigkeit von mehreren Schritten festlegen. Wenn beispielsweise von beiden `StepA` und `StepC` abhängt`StepB`, `StepC` wird erst gestartet, wenn die anderen beiden Schritte abgeschlossen sind.

```
name: Step-Step Dependency Test
specificationVersion: 'jobtemplate-2023-09'
steps:
- name: A
  script:
    actions:
      onRun:
        command: bash
        args: ['{{ Task.File.run }}']
    embeddedFiles:
      - name: run
        type: TEXT
        data: |
          #!/bin/env bash

          set -euo pipefail
```

```
          sleep 1
          echo Task A Done!
- name: B
  dependencies:
  - dependsOn: A # This means Step B depends on Step A
  script:
    actions:
      onRun:
        command: bash
        args: ['{{ Task.File.run }}']
    embeddedFiles:
      - name: run
        type: TEXT
        data: |
          #!/bin/env bash

          set -euo pipefail

          sleep 1
          echo Task B Done!
```

Job in Deadline Cloud

In diesem Thema wird beschrieben, wie Sie die AWS Deadline Cloud-Befehlszeilenschnittstelle (Deadline Cloud CLI) verwenden, um den Status eines Jobs oder Schritts anzuzeigen. Informationen zur Verwendung des Deadline Cloud-Monitors zur Anzeige des Status von Jobs oder Schritten finden Sie unterVerwalten Sie Jobs, Schritte und Aufgaben in Deadline Cloud.

Sie können auch Regeln für den standardmäßigen EventBridge Amazon-Event-Bus erstellen, um ein Ereignis an ein Ziel zu senden, z. B. den Amazon Simple Notification Service, der SMS-Texte oder E-Mails sendet, wenn sich der Status eines Jobs, Schritts oder einer Aufgabe ändert. Weitere Informationen finden Sie unter Deadline Cloud-Events mit Amazon verwalten EventBridge im Deadline Cloud Developer Guide >.

Sie können den Status eines Jobs mit dem Befehl `deadline job get --job-id` Deadline Cloud CLI anzeigen. Die Antwort auf die Befehle umfasst den Status des Jobs oder Schritts und die Anzahl der Aufgaben in jedem Verarbeitungsstatus.

Wenn Sie einen Job zum ersten Mal einreichen, lautet der Status`CREATE_IN_PROGRESS`. Wenn der Job die Validierungsprüfungen besteht, ändert sich sein Status in`CREATE_COMPLETE`. Wenn nicht, ändert sich der Status zu`CREATE_FAILED`.

Zu den möglichen Gründen, warum ein Job die Validierungsprüfungen nicht bestehen kann, gehören die folgenden:

- Die Jobvorlage entspricht nicht der OpenJD-Spezifikation.
- Der Job enthält zu viele Schritte.
- Der Job enthält insgesamt zu viele Aufgaben.

Um die Kontingente für die maximale Anzahl von Schritten und Aufgaben in einem Job zu sehen, verwenden Sie die Service-Kontingents-Konsole. Weitere Informationen finden Sie unter Kontingente für Deadline Cloud.

Möglicherweise liegt auch ein interner Dienstfehler vor, der die Erstellung eines Auftrags verhindert. In diesem Fall lautet der Statuscode des Jobs `INTERNAL_ERROR` und das Feld mit der Statusmeldung enthält eine detailliertere Erklärung.

Verwenden Sie den folgenden Deadline Cloud CLI-Befehl, um die Details für einen Job anzuzeigen. Ersetzen Sie es im folgenden Beispiel *jobID* durch Ihre eigenen Informationen:

```
deadline job get --job-id jobId
```

Die Antwort des `deadline job get` Befehls lautet wie folgt:

```
jobId: jobId
name: Sample Job
lifecycleStatus: CREATE_COMPLETE
lifecycleStatusMessage: Job creation completed successfully
priority: 50
createdAt: 2024-03-26 18:11:19.065000+00:00
createdBy: Test User
startedAt: 2024-03-26 18:12:50.710000+00:00
taskRunStatus: STARTING
taskRunStatusCounts:
  PENDING: 0
  READY: 5
  RUNNING: 0
  ASSIGNED: 0
  STARTING: 0
  SCHEDULED: 0
  INTERRUPTING: 0
```

```
  SUSPENDED: 0
  CANCELED: 0
  FAILED: 0
  SUCCEEDED: 0
  NOT_COMPATIBLE: 0
maxFailedTasksCount: 100
maxRetriesPerTask: 5
```

Jede Aufgabe in einem Job oder Schritt hat einen Status. Die Aufgabenstatus werden kombiniert, um einen Gesamtstatus für Jobs und Schritte zu ergeben. Die Anzahl der Aufgaben in den einzelnen Bundesstaaten wird im `taskRunStatusCounts` Antwortfeld angegeben.

Der Status eines Jobs oder Schritts hängt vom Status seiner Aufgaben ab. Der Status wird durch die Aufgaben bestimmt, die diesen Status der Reihe nach haben. Der Status der Schritte wird genauso bestimmt wie der Status des Jobs.

In der folgenden Liste werden die Status beschrieben:

`NOT_COMPATIBLE`

Der Auftrag ist nicht mit der Farm kompatibel, da es keine Flotten gibt, die eine der Aufgaben des Jobs ausführen können.

`RUNNING`

Ein oder mehrere Mitarbeiter führen Aufgaben aus dem Job aus. Solange mindestens eine laufende Aufgabe vorhanden ist, ist der Job markiert`RUNNING`.

`ASSIGNED`

Einem oder mehreren Arbeitskräften werden als nächste Aktion Aufgaben im Job zugewiesen. Die Umgebung, falls vorhanden, ist eingerichtet.

`STARTING`

Ein oder mehrere Mitarbeiter richten die Umgebung für die Ausführung von Aufgaben ein.

`SCHEDULED`

Aufgaben für den Job werden für einen oder mehrere Mitarbeiter als nächste Aktion des Arbeiters geplant.

`READY`

Mindestens eine Aufgabe für den Job ist zur Bearbeitung bereit.

`INTERRUPTING`

Mindestens eine Aufgabe im Job wird unterbrochen. Unterbrechungen können auftreten, wenn Sie den Status des Jobs manuell aktualisieren. Dies kann auch als Reaktion auf eine Unterbrechung aufgrund von Spot-Preisänderungen von Amazon Elastic Compute Cloud (Amazon EC2) geschehen.

`FAILED`

Eine oder mehrere Aufgaben im Job wurden nicht erfolgreich abgeschlossen.

`CANCELED`

Eine oder mehrere Aufgaben des Jobs wurden storniert.

`SUSPENDED`

Mindestens eine Aufgabe im Job wurde ausgesetzt.

`PENDING`

Eine Aufgabe im Job wartet auf die Verfügbarkeit einer anderen Ressource.

`SUCCEEDED`

Alle Aufgaben im Job wurden erfolgreich verarbeitet.

Ändern Sie einen Job in Deadline Cloud

Sie können die folgenden `update` Befehle AWS Command Line Interface (AWS CLI) verwenden, um die Konfiguration eines Jobs zu ändern oder den Zielstatus eines Jobs, Schritts oder einer Aufgabe festzulegen:

- `aws deadline update-job`
- `aws deadline update-step`
- `aws deadline update-task`

Ersetzen Sie in den folgenden `update` Befehlsbeispielen jeden Befehl *`user input placeholder`* durch Ihre eigenen Informationen.

Sie können den Deadline Cloud-Monitor auch verwenden, um die Konfiguration eines Jobs zu ändern. Weitere Informationen finden Sie unter Verwalten Sie Jobs, Schritte und Aufgaben in Deadline Cloud.

Example — Einen Job erneut in die Warteschlange stellen

Alle Aufgaben im Job wechseln in den READY Status, sofern es keine Schrittabhängigkeiten gibt. Schritte mit Abhängigkeiten wechseln zu entweder READY oderPENDING, wenn sie wiederhergestellt werden.

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--target-task-run-status PENDING
```

Example — Stornieren Sie einen Job

Alle Aufgaben im Job, die nicht den Status haben SUCCEEDED oder markiert FAILED sindCANCELED.

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--target-task-run-status CANCELED
```

Example — Einen Job als fehlgeschlagen markieren

Alle Aufgaben im Job, die den Status haben, SUCCEEDED bleiben unverändert. Alle anderen Aufgaben sind markiertFAILED.

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--target-task-run-status FAILED
```

Example — Markiere einen Job als erfolgreich

Alle Aufgaben im Job werden in den SUCCEEDED Bundesstaat übertragen.

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--target-task-run-status SUCCEEDED
```

Example — Einen Job aussetzen

Die Aufgaben des Jobs im `FAILED` Status `SUCCEEDEDCANCELED`, oder ändern sich nicht. Alle anderen Aufgaben sind markiert`SUSPENDED`.

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--target-task-run-status SUSPENDED
```

Example — Ändern Sie die Priorität eines Jobs

Aktualisiert die Priorität eines Jobs in einer Warteschlange, um die Reihenfolge zu ändern, in der er geplant wird. Jobs mit höherer Priorität werden in der Regel zuerst geplant.

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--priority 100
```

Example — Ändert die Anzahl der zulässigen fehlgeschlagenen Aufgaben

Aktualisiert die maximale Anzahl fehlgeschlagener Aufgaben, die der Job haben kann, bevor die verbleibenden Aufgaben abgebrochen werden.

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--max-failed-tasks-count 200
```

Example — Ändert die Anzahl der zulässigen Aufgabenwiederholungen

Aktualisiert die maximale Anzahl von Wiederholungen für eine Aufgabe, bevor die Aufgabe fehlschlägt. Eine Aufgabe, die die maximale Anzahl von Wiederholungen erreicht hat, kann erst in die Warteschlange gestellt werden, wenn dieser Wert erhöht wird.

```
aws deadline update-job \
--farm-id farmID \
```

```
--queue-id queueID \
--job-id jobID \
--max-retries-per-task 10
```

Example — Archivieren Sie einen Job

Aktualisiert den Lebenszyklusstatus des Jobs auf`ARCHIVED`. Archivierte Jobs können nicht geplant oder geändert werden. Sie können nur einen Job archivieren, der sich im `SUSPENDED` Status `FAILEDCANCELED`,`SUCCEEDED`, oder befindet.

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--lifecycle-status ARCHIVED
```

Example — Einen Schritt erneut in die Warteschlange stellen

Alle Aufgaben im Schritt wechseln in den `READY` Status, sofern keine Schrittabhängigkeiten bestehen. Aufgaben in Schritten mit Abhängigkeiten wechseln entweder zu `READY` oder`PENDING`, und die Aufgabe wird wiederhergestellt.

```
aws deadline update-step \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--step-id stepID \
--target-task-run-status PENDING
```

Example — Einen Schritt abbrechen

Alle Aufgaben in dem Schritt, die nicht den Status haben `SUCCEEDED` oder markiert `FAILED` sind`CANCELED`.

```
aws deadline update-step \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--step-id stepID \
--target-task-run-status CANCELED
```

Example — Einen Schritt als fehlgeschlagen markieren

Alle Aufgaben in dem Schritt, die den Status haben, `SUCCEEDED` bleiben unverändert. Alle anderen Aufgaben sind markiert`FAILED`.

```
aws deadline update-step \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--step-id stepID \
--target-task-run-status FAILED
```

Example — Markiere einen Schritt als erfolgreich

Alle Aufgaben in dem Schritt sind markiert`SUCCEEDED`.

```
aws deadline update-step \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--step-id stepID \
--target-task-run-status SUCCEEDED
```

Example — Einen Schritt aussetzen

Aufgaben im Schritt im `FAILED` Status `SUCCEEDEDCANCELED`, oder ändern sich nicht. Alle anderen Aufgaben sind markiert`SUSPENDED`.

```
aws deadline update-step \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--step-id stepID \
--target-task-run-status SUSPENDED
```

Example — Den Status einer Aufgabe ändern

Wenn Sie den Befehl `update-task` Deadline Cloud CLI verwenden, wechselt die Aufgabe in den angegebenen Status.

```
aws deadline update-task \
--farm-id farmID \
```

```
--queue-id queueID \
--job-id jobID \
--step-id stepID \
--task-id taskID \
--target-task-run-status SUCCEEDED | SUSPENDED | CANCELED | FAILED | PENDING
```

Wie Deadline Cloud Jobs verarbeitet

Um einen Job zu bearbeiten, verwendet AWS Deadline Cloud die Jobvorlage Open Job Description (OpenJD), um die benötigten Ressourcen zu ermitteln. Deadline Cloud wählt aus den Flotten, die zu Ihrer Warteschlange gehören, einen geeigneten Mitarbeiter für einen Schritt aus. Der ausgewählte Mitarbeiter erfüllt alle für den Schritt erforderlichen Fähigkeitsattribute.

Als Nächstes sendet Deadline Cloud Anweisungen an die Mitarbeiter, um eine Sitzung für den Schritt einzurichten. Die für den Schritt erforderliche Software muss auf der Worker-Instanz verfügbar sein, damit der Job ausgeführt werden kann. Der Service kann Sitzungen für mehrere Worker öffnen, sofern die Skalierungseinstellungen für die Flotte ausreichend sind.

Sie können die Software in einem einrichten Amazon Machine Image (AMI), oder Ihr Mitarbeiter kann die Software zur Laufzeit aus einem Repository oder Paketmanager laden. Sie können Warteschlangen-, Job- oder Schrittumgebungen verwenden, um die von Ihnen bevorzugte Software bereitzustellen.

Der Deadline Cloud-Dienst verwendet die OpenJD-Vorlage, um die für den Job erforderlichen Schritte und die für jeden Schritt erforderlichen Aufgaben zu ermitteln. Einige Schritte hängen von anderen Schritten ab, sodass Deadline Cloud die Reihenfolge festlegt, in der die Schritte abgeschlossen werden. Anschließend sendet Deadline Cloud die Aufgaben für jeden Schritt zur Bearbeitung an die Mitarbeiter. Wenn eine Aufgabe abgeschlossen ist, sendet der Service eine weitere Aufgabe in derselben Sitzung, oder der Mitarbeiter kann eine neue Sitzung starten.

Sie können den Fortschritt des Jobs im Deadline Cloud-Monitor, in der Deadline Cloud-Befehlszeilenschnittstelle (Deadline Cloud CLI) oder im verfolgen AWS CLI. Weitere Informationen zur Verwendung des Monitors finden Sie unterDen Deadline Cloud-Monitor verwenden. Weitere Informationen zur Verwendung der Deadline Cloud-CLI finden Sie unterJob in Deadline Cloud.

Nachdem alle Aufgaben in jedem Schritt abgeschlossen sind, ist der Job abgeschlossen und die Ausgabe kann auf Ihre Workstation heruntergeladen werden. Auch wenn der Job nicht abgeschlossen wurde, steht die Ausgabe aller abgeschlossenen Schritte und Aufgaben zum Herunterladen zur Verfügung.

Deadline Cloud entfernt Jobs 120 Tage nach ihrer Einreichung. Wenn ein Job entfernt wird, werden auch alle mit dem Job verknüpften Schritte und Aufgaben entfernt. Wenn Sie den Job erneut ausführen müssen, reichen Sie die OpenJD-Vorlage für den Job erneut ein.

Erstellen Sie Ressourcenlimits für Jobs

Jobs, die an Deadline Cloud übermittelt werden, können von Ressourcen abhängen, die von mehreren Jobs gemeinsam genutzt werden. Beispielsweise kann eine Farm mehr Mitarbeiter als variable Lizenzen für eine bestimmte Ressource haben. Oder ein gemeinsam genutzter Dateiserver kann möglicherweise nur einer begrenzten Anzahl von Workern gleichzeitig Daten bereitstellen. In einigen Fällen können ein oder mehrere Jobs all diese Ressourcen beanspruchen, was aufgrund nicht verfügbarer Ressourcen zu Fehlern führt, wenn neue Mitarbeiter eingestellt werden.

Um dieses Problem zu lösen, können Sie Grenzwerte für diese begrenzten Ressourcen verwenden. Deadline Cloud berücksichtigt die Verfügbarkeit eingeschränkter Ressourcen und verwendet diese Informationen, um sicherzustellen, dass Ressourcen verfügbar sind, wenn neue Mitarbeiter ihre Arbeit aufnehmen, sodass die Wahrscheinlichkeit geringer ist, dass Jobs aufgrund nicht verfügbarer Ressourcen ausfallen.

Grenzwerte werden für die gesamte Farm erstellt. Für Aufträge, die an eine Warteschlange gesendet werden, können nur Limits gelten, die der Warteschlange zugeordnet sind. Wenn Sie ein Limit für einen Job angeben, der nicht mit der Warteschlange verknüpft ist, ist der Job nicht kompatibel und kann nicht ausgeführt werden.

Um ein Limit zu verwenden, müssen Sie

- Erstellen Sie ein Limit
- Ordnen Sie ein Limit und einer Warteschlange zu
- Reichen Sie einen Job ein, der Limits erfordert

> **Note**
>
> Wenn Sie einen Job mit eingeschränkten Ressourcen in einer Warteschlange ausführen, der kein Limit zugeordnet ist, kann dieser Job alle Ressourcen verbrauchen. Wenn Sie über eine eingeschränkte Ressource verfügen, stellen Sie sicher, dass alle Schritte in Aufträgen in Warteschlangen, die die Ressource verwenden, mit einem Limit verknüpft sind.

Bei Grenzwerten, die in einer Farm definiert, einer Warteschlange zugeordnet und in einem Job angegeben sind, kann eines von vier Dingen passieren:

- Wenn Sie ein Limit erstellen, es einer Warteschlange zuordnen und das Limit in der Vorlage eines Jobs angeben, wird der Job ausgeführt und verwendet nur die im Limit definierten Ressourcen.
- Wenn Sie ein Limit erstellen, es in einer Jobvorlage angeben, das Limit aber keiner Warteschlange zuordnen, wird der Job als inkompatibel markiert und kann nicht ausgeführt werden.
- Wenn Sie ein Limit erstellen, es keiner Warteschlange zuordnen und das Limit nicht in der Vorlage eines Jobs angeben, wird der Job ausgeführt, verwendet das Limit aber nicht.
- Wenn Sie überhaupt kein Limit verwenden, wird der Job ausgeführt.

Wenn Sie mehreren Warteschlangen ein Limit zuordnen, teilen sich die Warteschlangen die Ressourcen, die durch das Limit eingeschränkt sind. Wenn Sie beispielsweise ein Limit von 100 erstellen und eine Warteschlange 60 Ressourcen verwendet, können andere Warteschlangen nur 40 Ressourcen verwenden. Wenn eine Ressource freigegeben wird, kann sie von einer Aufgabe aus einer beliebigen Warteschlange übernommen werden.

Deadline Cloud bietet zwei AWS CloudFormation Metriken, mit denen Sie die durch ein Limit bereitgestellten Ressourcen überwachen können. Sie können die aktuelle Anzahl der verwendeten Ressourcen und die maximale Anzahl der Ressourcen, die im Rahmen des Limits verfügbar sind, überwachen. Weitere Informationen finden Sie unter Kennzahlen zum Ressourcenlimit im Deadline Cloud Developer Guide.

Sie wenden ein Limit auf einen Auftragsschritt in einer Jobvorlage an. Wenn Sie im `amounts` Abschnitt eines Schritts den Namen der Mengenanforderung für ein Limit angeben und der Warteschlange des Jobs ein Limit zugeordnet `amountRequirementName` wird, werden die für diesen Schritt geplanten Aufgaben durch das Limit für die Ressource eingeschränkt. `hostRequirements`

Wenn für einen Schritt eine Ressource erforderlich ist, die durch ein erreichtes Limit eingeschränkt ist, werden die Aufgaben in diesem Schritt nicht von weiteren Mitarbeitern übernommen.

Sie können mehr als ein Limit auf einen Arbeitsschritt anwenden. Wenn in diesem Schritt beispielsweise zwei verschiedene Softwarelizenzen verwendet werden, können Sie für jede Lizenz ein eigenes Limit festlegen. Wenn für einen Schritt zwei Grenzwerte erforderlich sind und das Limit für eine der Ressourcen erreicht ist, werden Aufgaben in diesem Schritt nicht von weiteren Mitarbeitern übernommen, bis die Ressourcen verfügbar sind.

Beenden und Löschen von Grenzwerten

Wenn Sie die Zuordnung zwischen einer Warteschlange und einem Limit beenden oder löschen, beendet ein Job, der das Limit verwendet, die Planung von Aufgaben für Schritte, die dieses Limit erfordern, und blockiert die Erstellung neuer Sitzungen für einen Schritt.

Aufgaben, die sich im Status BEREIT befinden, bleiben bereit, und Aufgaben werden automatisch fortgesetzt, sobald die Verbindung zwischen der Warteschlange und dem Limit wieder aktiv wird. Sie müssen keine Jobs in die Warteschlange stellen.

Wenn Sie die Zuordnung zwischen einer Warteschlange und einem Limit beenden oder löschen, haben Sie zwei Möglichkeiten, die Ausführung von Aufgaben zu beenden:

- Aufgaben beenden und stornieren — Mitarbeiter mit Sitzungen, die das Limit erreicht haben, stornieren alle Aufgaben.
- Ausführen von Aufgaben beenden und beenden — Mitarbeiter mit Sitzungen, die das Limit erreicht haben, erledigen ihre Aufgaben.

Wenn Sie ein Limit über die Konsole löschen, beenden die Mitarbeiter zunächst die Ausführung von Aufgaben sofort oder erst, wenn sie abgeschlossen sind. Wenn die Zuordnung gelöscht wird, passiert Folgendes:

- Schritte, die das Limit erfordern, sind als nicht kompatibel gekennzeichnet.
- Der gesamte Job, der diese Schritte enthält, wird abgebrochen, einschließlich der Schritte, für die das Limit nicht erforderlich ist.
- Der Job ist als nicht kompatibel markiert.

Wenn der Warteschlange, die dem Limit zugeordnet ist, eine Flotte mit einer Flottenkapazität zugeordnet ist, die dem Mengenanforderungsnamen des Limits entspricht, verarbeitet diese Flotte weiterhin Aufträge mit dem angegebenen Limit.

Erstellen Sie ein Limit

Sie erstellen ein Limit mit der Deadline Cloud-Konsole oder dem CreateLimit Vorgang in der Deadline Cloud-API. Limits sind für eine Farm definiert, aber mit Warteschlangen verknüpft. Nachdem Sie ein Limit erstellt haben, können Sie es einer oder mehreren Warteschlangen zuordnen.

Um ein Limit zu erstellen

1. Wählen Sie im Dashboard der Deadline Cloud-Konsole (https://console.aws.amazon.com/deadlinecloud/Startseite) die Farm aus, für die Sie eine Warteschlange erstellen möchten.
2. Wählen Sie die Farm aus, zu der Sie das Limit hinzufügen möchten, klicken Sie auf den Tab Limits und dann auf Limit erstellen.
3. Geben Sie die Details für das Limit ein. Der Name der Mengenanforderung ist der Name, der in der Jobvorlage verwendet wird, um das Limit zu identifizieren. Er muss mit dem Präfix beginnen, **`amount.`** gefolgt von der Bezeichnung des Betrags. Der Name der Mengenanforderung muss in den Warteschlangen, die mit dem Limit verknüpft sind, eindeutig sein.
4. Wenn Sie „Höchstbetrag festlegen“ wählen, entspricht dies der Gesamtzahl der Ressourcen, die nach diesem Limit zulässig sind. Wenn Sie „Kein Höchstbetrag“ wählen, ist die Ressourcennutzung nicht begrenzt. Auch wenn die Ressourcennutzung nicht begrenzt ist, wird die `CurrentCount` CloudWatch Amazon-Metrik ausgegeben, sodass Sie die Nutzung verfolgen können. Weitere Informationen finden Sie unter CloudWatchMetriken im Deadline Cloud Developer Guide.
5. Wenn Sie bereits wissen, für welche Warteschlangen das Limit verwendet werden soll, können Sie sie jetzt auswählen. Sie müssen keine Warteschlange zuordnen, um ein Limit zu erstellen.
6. Wählen Sie Limit erstellen aus.

Ordnen Sie ein Limit und einer Warteschlange zu

Nachdem Sie ein Limit erstellt haben, können Sie dem Limit eine oder mehrere Warteschlangen zuordnen. Nur Warteschlangen, die einem Grenzwert zugeordnet sind, verwenden die im Grenzwert angegebenen Werte.

Sie erstellen eine Zuordnung zu einer Warteschlange mithilfe der Deadline Cloud-Konsole oder des CreateQueueLimitAssociation Vorgangs in der Deadline Cloud-API.

Um eine Warteschlange mit einem Limit zu verknüpfen

1. Wählen Sie im Dashboard der Deadline Cloud-Konsole (https://console.aws.amazon.com/deadlinecloud/Startseite) die Farm aus, für die Sie ein Limit mit einer Warteschlange verknüpfen möchten.
2. Wählen Sie den Tab Limits, wählen Sie das Limit aus, dem eine Warteschlange zugeordnet werden soll, und wählen Sie dann Limit bearbeiten aus.

3. Wählen Sie im Abschnitt Warteschlangen zuordnen die Warteschlangen aus, die dem Limit zugeordnet werden sollen.
4. Wählen Sie Änderungen speichern.

Reichen Sie einen Job ein, der Limits erfordert

Sie wenden ein Limit an, indem Sie es als Hostanforderung für den Job oder Job-Schritt angeben. Wenn Sie in einem Schritt kein Limit angeben und dieser Schritt eine zugeordnete Ressource verwendet, wird die Nutzung des Schritts nicht auf das Limit angerechnet, wenn Jobs geplant werden.

Bei einigen Deadline Cloud-Einreichern können Sie eine Hostanforderung festlegen. Sie können den Namen des Limits im Absender angeben, um das Limit anzuwenden.

Wenn Ihr Einreicher das Hinzufügen von Hostanforderungen nicht unterstützt, können Sie auch ein Limit festlegen, indem Sie die Jobvorlage für den Job bearbeiten.

Um ein Limit auf einen Job-Schritt im Job-Bundle anzuwenden

1. Öffnen Sie die Jobvorlage für den Job mit einem Texteditor. Die Jobvorlage befindet sich im Job-Bundle-Verzeichnis für den Job. Weitere Informationen finden Sie unter Job-Pakete im Deadline Cloud Developer Guide.
2. Suchen Sie die Schrittdefinition für den Schritt, auf den das Limit angewendet werden soll.
3. Fügen Sie der Schrittdefinition Folgendes hinzu. *amount.name*Ersetzen Sie es durch den Namen der Mengenanforderung für Ihr Limit. Für den typischen Gebrauch sollten Sie den `min` Wert auf 1 setzen.

   YAML

   ```yaml
   hostRequirements:
     amounts:
     - name: amount.name
       min: 1
   ```

   JSON

   ```json
   "hostRequirements": {
       "amounts": [
           {
               "name": "amount.name",
   ```

```
            "min": "1"
        }
    }
}
```

Sie können einem Auftragsschritt wie folgt mehrere Grenzwerte hinzufügen. Ersetzen Sie *amount.name_1* und *amount.name_2* durch die Namen der Mengenanforderungen Ihrer Limits.

YAML

```
  hostRequirements:
    amounts:
    - name: amount.name_1
      min: 1
    - name: amount.name_2
      min: 1
```

JSON

```
"hostRequirements": {
    "amounts": [
        {
            "name": "amount.name_1",
            "min": "1"
        },
        {
            "name": "amount.name_2",
            "min": "1"
        }
    }
}
```

4. Speichern Sie die Änderungen an der Jobvorlage.

Dateispeicher für Deadline Cloud

Mitarbeiter müssen Zugriff auf die Speicherorte haben, die die für die Bearbeitung eines Auftrags erforderlichen Eingabedateien enthalten, sowie auf die Speicherorte, an denen die Ausgabe gespeichert wird. AWS Deadline Cloud bietet zwei Optionen für Speicherorte:

- Mit Job-Anhängen überträgt Deadline Cloud die Eingabe- und Ausgabedateien für Ihre Jobs zwischen einer Workstation und Deadline Cloud-Mitarbeitern hin und her. Um die Dateiübertragungen zu ermöglichen, verwendet Deadline Cloud einen Amazon Simple Storage Service (Amazon S3) -Bucket in Ihrem AWS-Konto.

  Wenn Sie Auftragsanhänge mit einer vom Service verwalteten Flotte verwenden, können Sie ein virtuelles Dateisystem (VFS) in Ihrem virtuellen privaten Netzwerk (VPN) einrichten. Dann können Mitarbeiter Dateien nur dann laden, wenn sie benötigt werden.
- Bei gemeinsam genutztem Speicher nutzen Sie die Dateifreigabe mit Ihrem Betriebssystem, um Zugriff auf Dateien zu gewähren.

  Wenn Sie plattformübergreifenden gemeinsamen Speicher verwenden, können Sie ein Speicherprofil erstellen, sodass Mitarbeiter den Pfad Dateien zwischen zwei verschiedenen Betriebssystemen zuordnen können.

Themen

Jobanhänge in Deadline Cloud

Job Job-Anhängen können Sie Dateien zwischen Ihrer Workstation und AWS Deadline Cloud hin und her übertragen. Mit Job-Anhängen müssen Sie keinen Amazon S3 S3-Bucket für Ihre Dateien manuell einrichten. Wenn Sie mit der Deadline Cloud-Konsole eine Warteschlange erstellen, wählen Sie stattdessen den Bucket für Ihre Jobanhänge aus.

Wenn Sie zum ersten Mal einen Job bei Deadline Cloud einreichen, werden alle Dateien für den Job in Deadline Cloud übertragen. Bei nachfolgenden Einreichungen werden nur die Dateien übertragen, die sich geändert haben, was sowohl Zeit als auch Bandbreite spart.

Nach Abschluss der Verarbeitung können Sie das Ergebnis von der Jobdetailseite oder mithilfe des Deadline Cloud `deadline job download-output` CLI-Befehls herunterladen.

Sie können denselben S3-Bucket für mehrere Warteschlangen verwenden. Legen Sie für jede Warteschlange ein anderes Root-Präfix fest, um die Anhänge im Bucket zu organisieren.

Wenn Sie mit der Konsole eine Warteschlange erstellen, können Sie entweder eine bestehende AWS Identity and Access Management (IAM-) Rolle auswählen oder die Konsole eine neue Rolle erstellen lassen. Wenn die Konsole die Rolle erstellt, legt sie Berechtigungen für den Zugriff auf den Bucket fest, der für die Warteschlange angegeben ist. Wenn Sie eine bestehende Rolle auswählen, müssen Sie der Rolle Berechtigungen für den Zugriff auf den S3-Bucket gewähren.

Verschlüsselung für S3-Buckets mit Stellenanhängen

Dateien mit Anhängen von Job werden standardmäßig in Ihrem S3-Bucket verschlüsselt. Dies trägt dazu bei, Ihre Informationen vor unbefugtem Zugriff zu schützen. Sie müssen nichts tun, um Ihre Dateien mit Schlüsseln zu verschlüsseln, die von Deadline Cloud bereitgestellt werden. Weitere Informationen finden Sie unter Amazon S3 verschlüsselt jetzt automatisch alle neuen Objekte im Amazon S3 S3-Benutzerhandbuch.

Sie können Ihren eigenen, vom Kunden verwalteten AWS Key Management Service Schlüssel verwenden, um den S3-Bucket zu verschlüsseln, der Ihre Jobanhänge enthält. Dazu müssen Sie die IAM-Rolle für die Warteschlange ändern, die dem Bucket zugeordnet ist, um den Zugriff auf den zu ermöglichen. AWS KMS key

Um den IAM-Policy-Editor für die Warteschlangenrolle zu öffnen

1. Melden Sie sich bei der Deadline Cloud-Konsole an AWS Management Console und öffnen Sie sie. Wählen Sie auf der Hauptseite im Abschnitt Erste Schritte die Option Farmen anzeigen aus.
2. Wählen Sie aus der Liste der Farmen die Farm aus, die die zu ändernde Warteschlange enthält.
3. Wählen Sie aus der Liste der Warteschlangen die Warteschlange aus, die Sie ändern möchten.
4. Wählen Sie im Abschnitt Warteschlangendetails die Servicerolle aus, um die IAM-Konsole für die Servicerolle zu öffnen.

Führen Sie als Nächstes das folgende Verfahren aus.

Um die Rollenrichtlinie mit der Erlaubnis zu aktualisieren AWS KMS

1. Wählen Sie aus der Liste der Berechtigungsrichtlinien die Richtlinie für die Rolle aus.
2. Wählen Sie im Abschnitt „In dieser Richtlinie definierte Berechtigungen“ die Option Bearbeiten aus.

3. Wählen Sie Neue Aussage hinzufügen aus.
4. Kopieren Sie die folgende Richtlinie und fügen Sie sie in den Editor ein. Ändern Sie die *Region* *accountID*, und *keyID* in Ihre eigenen Werte.

```
{
   "Effect": "Allow",
   "Action": [
       "kms:Decrypt",
       "kms:DescribeKey",
       "kms:GenerateDataKey"
   ],
   "Resource": [
       "arn:aws:kms:Region:accountID:key/keyID"
   ]
}
```

5. Wählen Sie Weiter.
6. Überprüfen Sie die Änderungen an der Richtlinie, und wenn Sie damit zufrieden sind, wählen Sie Änderungen speichern aus.

Verwaltung von Job-Anhängen in S3-Buckets

Deadline Cloud speichert die für Ihren Job erforderlichen Dateien mit Anhängen von Jobs in einem S3-Bucket. Diese Dateien sammeln sich im Laufe der Zeit an, was zu erhöhten Amazon S3 S3-Kosten führt. Um die Kosten zu senken, können Sie eine S3-Lifecycle-Konfiguration auf Ihren S3-Bucket anwenden. Diese Konfiguration kann Dateien im Bucket automatisch löschen. Da sich der S3-Bucket in Ihrem Konto befindet, können Sie die S3-Lifecycle-Konfiguration jederzeit ändern oder entfernen. Weitere Informationen finden Sie unter Beispiele für die Konfiguration von S3 Lifecycle im Amazon S3 S3-Benutzerhandbuch.

Für eine detailliertere S3-Bucket-Verwaltungslösung können Sie festlegen, dass Ihre AWS-Konto Objekte in einem S3-Bucket auf der Grundlage des letzten Zugriffs ablaufen. Weitere Informationen finden Sie im AWS Architektur-Blog unter Ablaufen von Amazon S3 S3-Objekten basierend auf dem Datum des letzten Zugriffs zur Kostensenkung.

Virtuelles Dateisystem Deadline Cloud

Die Unterstützung virtueller Dateisysteme für Jobanhänge in AWS Deadline Cloud ermöglicht es der Client-Software auf Mitarbeitern, direkt mit Amazon Simple Storage Service zu kommunizieren.

Mitarbeiter können Dateien nur bei Bedarf laden, anstatt alle Dateien vor der Verarbeitung herunterzuladen. Dateien werden lokal gespeichert. Durch diesen Ansatz wird vermieden, dass Ressourcen heruntergeladen werden, die mehrmals als einmal verwendet wurden. Alle Dateien werden nach Abschluss des Jobs entfernt.

- Das virtuelle Dateisystem bietet eine erhebliche Leistungssteigerung für bestimmte Jobprofile. Im Allgemeinen bieten kleinere Teilmengen aller Dateien mit einer größeren Mitarbeiterflotte den größten Nutzen. Eine geringe Anzahl von Dateien mit weniger Mitarbeitern hat in etwa die gleiche Bearbeitungszeit.
- Unterstützung für virtuelle Dateisysteme ist nur verfügbar für Linux Mitarbeiter in Flotten mit Servicemanagement.
- Das virtuelle Dateisystem von Deadline Cloud unterstützt die folgenden Operationen, ist jedoch nicht POSIX-konform:
  - Datei`create`,`delete`,`open`,`close`,`read`,`write`,,`append`,`truncate`,`rename`,`move`,`copy`, `statfsync`, und `falloc`
  - Verzeichnis`create`,`delete`,`rename`,`move`,`copy`, und `stat`
- Das virtuelle Dateisystem wurde entwickelt, um die Datenübertragung zu reduzieren und die Leistung zu verbessern, wenn Ihre Aufgaben nur auf einen Teil eines großen Datensatzes zugreifen. Es ist nicht für alle Workloads optimiert. Sie sollten Ihre Arbeitslast testen, bevor Sie Produktionsjobs ausführen.

Aktivieren Sie die VFS-Unterstützung

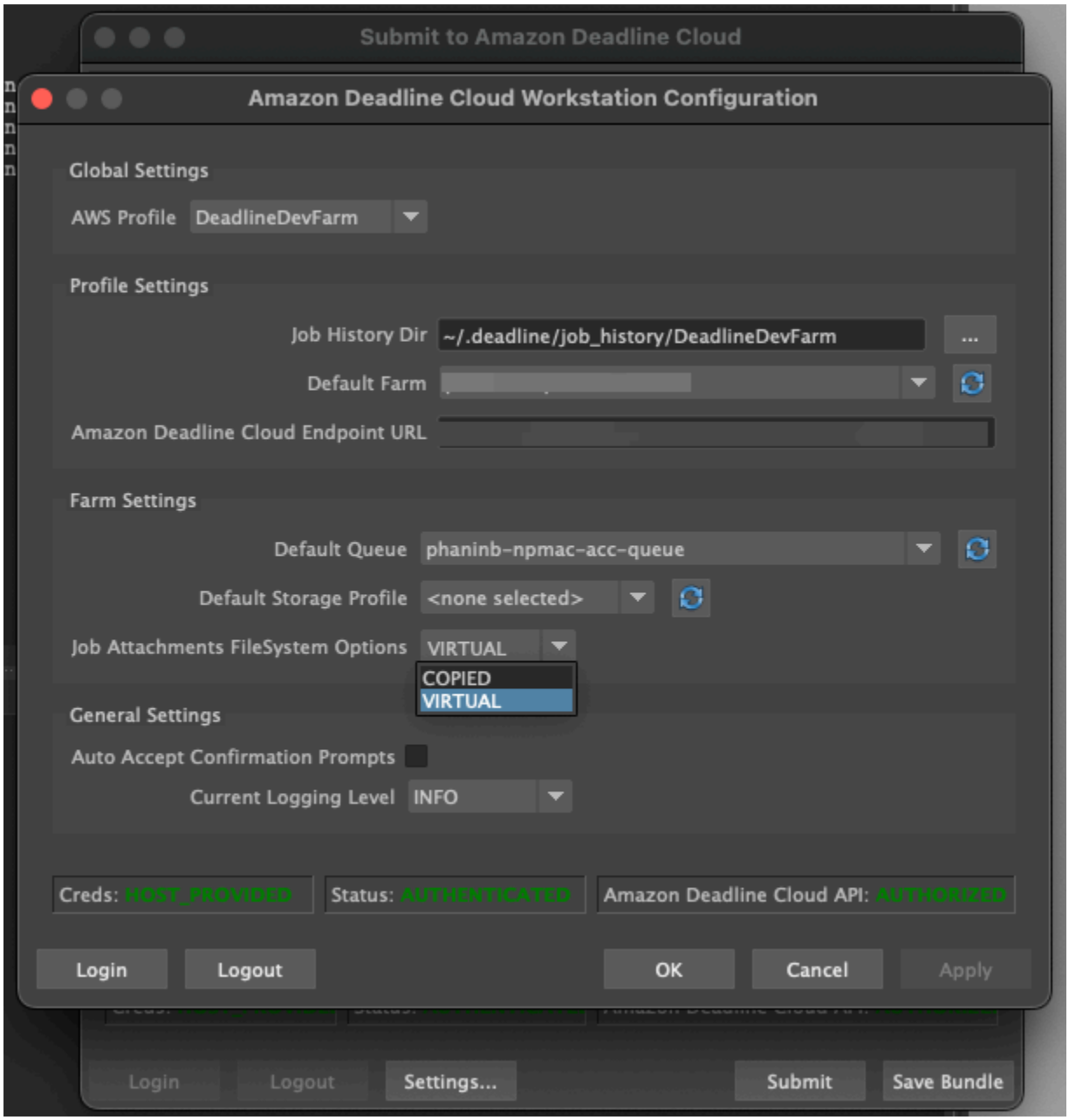
Die Unterstützung virtueller Dateisysteme (VFS) ist für jeden Job aktiviert. In den folgenden Fällen greift ein Job auf das Standard-Framework für Jobanhänge zurück:

- Ein Worker-Instanzprofil unterstützt kein virtuelles Dateisystem.
- Probleme verhindern das Starten des virtuellen Dateisystemprozesses.
- Das virtuelle Dateisystem kann nicht gemountet werden.

Um die Unterstützung virtueller Dateisysteme mithilfe des Absenders zu aktivieren

1. Wenn Sie einen Job einreichen, klicken Sie auf die Schaltfläche Einstellungen, um das Konfigurationsfenster der AWS Deadline Cloud-Workstation zu öffnen.

2. Wählen Sie in der Dropdownliste Dateisystemoptionen für Jobanhänge die Option VIRTUELL aus.



3. Um Ihre Änderungen zu speichern, wählen Sie OK.

Um die Unterstützung virtueller Dateisysteme zu aktivieren, verwenden Sie AWS CLI

- Verwenden Sie den folgenden Befehl, wenn Sie einen gespeicherten Job einreichen:

```
deadline bundle submit-job --job-attachments-file-system VIRTUAL
```

Um zu überprüfen, ob das virtuelle Dateisystem für einen bestimmten Job erfolgreich gestartet wurde, überprüfen Sie Ihre Protokolle in Amazon CloudWatch Logs. Suchen Sie nach den folgenden Meldungen:

```
Using mount_point mount_point
Launching vfs with command command
Launched vfs as pid PID number
```

Wenn das Protokoll die folgende Meldung enthält, ist die Unterstützung für virtuelle Dateisysteme deaktiviert:

```
Virtual File System not found, falling back to COPIED for JobAttachmentsFileSystem.
```

Problembehandlung bei der Unterstützung virtueller Dateisysteme

Mit dem Deadline Cloud-Monitor können Sie Protokolle für Ihr virtuelles Dateisystem anzeigen. Detaillierte Anweisungen finden Sie unter Logs in Deadline Cloud anzeigen.

Virtuelle Dateisystemprotokolle werden auch an die Gruppe CloudWatch Logs gesendet, die der Warteschlange zugeordnet ist, die gemeinsam mit der Ausgabe des Worker-Agents genutzt wird.

Ausgaben und Nutzung für Deadline Cloud-Farmen verfolgen

Der Budgetmanager und der Usage Explorer von AWS Deadline Cloud sind Tools für das Kostenmanagement, die anhand verfügbarer Informationen zu Kostenvariablen die ungefähren Kosten für die Nutzung von Deadline Cloud ermitteln. Die Kostenmanagement-Tools garantieren nicht den Betrag, der Ihnen für Ihre tatsächliche Nutzung von Deadline Cloud und anderen AWS Diensten geschuldet wird.

Um Ihnen bei der Verwaltung der Kosten für Deadline Cloud zu helfen, können Sie die folgenden Funktionen verwenden:

- Budgetmanager — Mit dem Budgetmanager von Deadline Cloud können Sie Budgets erstellen und bearbeiten, um die Projektkosten zu verwalten.
- Nutzungsexplorer — Mit dem Deadline Cloud-Nutzungsexplorer können Sie sehen, wie viele AWS Ressourcen verwendet werden und wie hoch die geschätzten Kosten für diese Ressourcen sind.

Annahmen zu den Kosten

Die grundlegende Berechnung, die von den Kostenmanagement-Tools von Deadline Cloud verwendet wird, lautet:

```
Cost per job =
    (CMF run time x CMF compute rate) +
    (SMF run time x SMF compute rate) +
    (License run time x license rate)
```

- Die Laufzeit ist die Summe aller Aufgaben in einem Job, von der Startzeit bis zur Endzeit.
- Die Rechenrate richtet sich nach den AWS Deadline Cloud-Preisen für servicemanagierte Flotten. Für vom Kunden verwaltete Flotten wird der Rechenpreis auf 1 USD pro Arbeitsstunde geschätzt.
- Der Lizenztarif richtet sich nach dem Basislizenzpreis von Deadline Cloud und ist nur für vom Service verwaltete Flotten verfügbar. Zusätzliche Stufen sind nicht enthalten. Weitere Informationen zu den Lizenzpreisen finden Sie unter AWS Deadline Cloud-Preise.

Der Kostenvoranschlag der Kostenmanagement-Tools von Deadline Cloud kann aus verschiedenen Gründen von Ihren tatsächlichen Kosten abweichen. Zu den häufigsten Gründen gehören:

- Kundeneigene Ressourcen und deren Preisgestaltung. Sie können wählen, ob Sie Ihre eigenen Ressourcen mitbringen möchten, entweder von AWS oder extern von lokalen oder anderen Cloud-Anbietern. Die tatsächlichen Kosten dieser Ressourcen werden nicht berechnet.
- Kosten ungenutzter Arbeitskräfte. Die Kosten ungenutzter Arbeitskräfte sind nicht enthalten, wenn der Status „INAKTIV“ lautet. Dies kann bei Flotten der Fall sein, bei denen die Mindestanzahl der Instanzen größer als Null ist, oder wenn Mitarbeiter zwischen Jobs wechseln. Die Kosten ungenutzter Arbeitskräfte werden in den Berechnungen nicht berücksichtigt.
- Stopp- und Startzeit der Mitarbeiter. Nachdem Mitarbeiter einen Auftrag abgeschlossen haben, sind die Kosten für den Übergang von IDLE zu STOPP und von STOPP zu STOPP nicht in den Kostenschätzungen von Deadline Cloud enthalten.
- Werbegutschriften, Rabatte und individuelle Preisvereinbarungen. Die Kostenmanagement-Tools berücksichtigen keine Werbegutschriften, private Preisvereinbarungen oder andere Rabatte. Möglicherweise haben Sie Anspruch auf andere Rabatte, die nicht Teil des Kostenvoranschlags sind.
- Aufbewahrung von Vermögenswerten. Die Speicherung von Ressourcen ist in den Kosten- und Nutzungsschätzungen nicht enthalten.
- Preisänderungen. AWS bietet pay-as-you-go Preise für die meisten Dienste an. Die Preise können sich im Laufe der Zeit ändern. Die Kostenmanagement-Tools verwenden die meisten öffentlich verfügbaren up-to-date Preise, aber nach Änderungen kann es zu Verzögerungen kommen.
- Steuern. Die Kostenmanagement-Tools beinhalten keine Steuern, die auf unseren Kauf der Dienstleistung erhoben werden.
- Rundung. Das Kostenmanagement-Tool führt eine mathematische Rundung von Preisdaten durch.
- Währung. Kostenschätzungen werden in US-Dollar vorgenommen. Die globalen Wechselkurse variieren im Laufe der Zeit. Wenn Sie Schätzungen anhand des aktuellen Wechselkurses in eine andere Währungsbasis umrechnen, wirken sich Wechselkursänderungen auf die Schätzung aus.
- Externe Lizenzierung. Wenn Sie sich dafür entscheiden, vorab gekaufte Lizenzen (Softwarelizenzierung für servicemanagierte Flotten) zu verwenden, können die Kostenmanagement-Tools von Deadline Cloud diese Kosten nicht berücksichtigen.

Kontrollieren Sie die Kosten mit einem Budget

Der Deadline Cloud-Budgetmanager hilft Ihnen dabei, die Ausgaben für eine bestimmte Ressource zu kontrollieren, z. B. für eine Warteschlange, Flotte oder Farm. Sie können Budgetbeträge und -limits erstellen und automatisierte Aktionen einrichten, um zusätzliche Ausgaben im Rahmen des Budgets zu reduzieren oder zu verhindern.

In den folgenden Abschnitten finden Sie die Schritte zur Verwendung des Deadline Cloud-Budgetmanagers.

Themen

Voraussetzung

Um den Deadline Cloud-Budgetmanager verwenden zu können, benötigen Sie eine `OWNER` Zugriffsebene. Um die `OWNER` Erlaubnis zu erteilen, folgen Sie den Schritten unterBenutzer in Deadline Cloud verwalten.

Öffnen Sie den Deadline Cloud Budget Manager

Gehen Sie wie folgt vor, um den Deadline Cloud-Budgetmanager zu öffnen.

1. Melden Sie sich bei der Deadline Cloud-Konsole an AWS Management Console und öffnen Sie sie.
2. Wählen Sie Farmen anzeigen.
3. Suchen Sie die Farm, über die Sie Informationen erhalten möchten, und wählen Sie dann Jobs verwalten aus.
4. Wählen Sie im Deadline Cloud-Monitor im linken Navigationsbereich Budgets aus.

Auf der Übersichtsseite des Budget-Managers wird eine Liste der aktiven und inaktiven Budgets angezeigt:

- Aktive Budgets werden anhand der ausgewählten Ressource (einer Warteschlange) erfasst.
- Inaktive Budgets sind entweder abgelaufen oder wurden von einem Benutzer storniert und die Kosten werden nicht mehr im Rahmen der Budgetgrenzen erfasst.

Nachdem Sie ein Budget ausgewählt haben, enthält die Seite mit der Budgetübersicht grundlegende Informationen zum Budget. Zu den bereitgestellten Informationen gehören der Budgetname, der Status, die Ressourcen, der verbleibende Prozentsatz, der verbleibende Betrag, das Gesamtbudget, das Startdatum und das Enddatum.

Erstellen Sie ein Budget für eine Deadline Cloud-Warteschlange

Gehen Sie wie folgt vor, um ein Budget zu erstellen.

1. Falls Sie dies noch nicht getan haben, melden Sie sich bei der an AWS Management Console, öffnen Sie die Deadline Cloud-Konsole, wählen Sie eine Farm aus und wählen Sie dann Jobs verwalten aus.
2. Wählen Sie auf der Budget-Manager-Seite die Option Budget erstellen aus.
3. Geben Sie im Detailbereich eine Budgetbezeichnung für das Budget ein.
4. (Optional) Geben Sie im Beschreibungsfeld eine kurze Beschreibung des Budgets ein.
5. Wählen Sie unter Ressource im Dropdownmenü Warteschlange die Warteschlange aus, für die Sie ein Budget erstellen möchten.
6. Geben Sie unter Zeitraum das Start- und Enddatum für das Budget ein, indem Sie die folgenden Schritte ausführen:

   a. Geben Sie als Startdatum das erste Datum der Budgetverfolgung im YYYY/MM/DD Format ein, oder wählen Sie das Kalendersymbol und wählen Sie ein Datum aus.

      Das Standard-Startdatum ist das Datum, an dem das Budget erstellt wird.

   b. Geben Sie als Enddatum das letzte Datum der Budgetverfolgung im YYYY/MM/DD Format ein oder klicken Sie auf das Kalendersymbol und wählen Sie ein Datum aus.

      Das Standard-Enddatum liegt 120 Tage nach dem Startdatum.
7. Geben Sie unter Budgetbetrag den Dollarbetrag des Budgets ein.

8. (Optional) Wir empfehlen Ihnen, Limit-Benachrichtigungen zu erstellen. Im Abschnitt Limitaktionen können Sie automatisierte Aktionen implementieren, die ausgelöst werden, wenn bestimmte Beträge im Budget verbleiben. Führen Sie dazu die folgenden Schritte aus:

    a. Wählen Sie Neue Aktion hinzufügen.

    b. Geben Sie unter Verbleibender Betrag den Dollarbetrag ein, mit dem Sie die Aktion starten möchten.

    c. Wählen Sie in der Dropdownliste Aktion die gewünschte Aktion aus. Zu den Aktionen gehören:

    - Nach Abschluss der aktuellen Arbeit beenden — Alle Arbeiten, die derzeit ausgeführt werden, wenn der Schwellenwert erreicht ist, laufen weiter (und verursachen Kosten), bis sie abgeschlossen sind.
    - Arbeit sofort beenden — Alle Arbeiten werden sofort abgebrochen, wenn der Schwellenwert erreicht ist.

    d. Um zusätzliche Limit-Benachrichtigungen zu erstellen, wählen Sie Neue Aktion hinzufügen und wiederholen Sie die vorherigen Schritte.

9. Wählen Sie Budget erstellen.

Ein Budget für die Deadline Cloud-Warteschlange anzeigen

Nachdem Sie ein Budget erstellt haben, können Sie es auf der Seite Budgetmanager einsehen. Von dort aus können Sie den Gesamtbetrag des Budgets und die dem jeweiligen Budget zugewiesenen Gesamtkosten einsehen.

Gehen Sie wie folgt vor, um ein Budget einzusehen.

1. Falls Sie dies noch nicht getan haben, melden Sie sich bei der an AWS Management Console, öffnen Sie die Deadline Cloud-Konsole, wählen Sie eine Farm aus und klicken Sie dann auf Jobs verwalten.
2. Wählen Sie im linken Navigationsbereich Budgets aus. Die Seite Budget Manager wird angezeigt.
3. Um ein aktives Budget anzuzeigen, wählen Sie die Registerkarte Aktive Budgets und dann den Namen des Budgets, das Sie anzeigen möchten. Die Seite mit den Budgetdetails wird angezeigt.

4. Um die Budgetdetails für ein abgelaufenes Budget anzuzeigen, wählen Sie den Tab Inaktive Budgets. Wählen Sie dann den Namen des Budgets, das Sie anzeigen möchten. Die Seite mit den Budgetdetails wird angezeigt.

Bearbeiten Sie ein Budget für eine Deadline Cloud-Warteschlange

Sie können jedes aktive Budget bearbeiten. Gehen Sie wie folgt vor, um ein aktives Budget zu bearbeiten.

1. Falls Sie dies noch nicht getan haben, melden Sie sich bei der an AWS Management Console, öffnen Sie die Deadline Cloud-Konsole, wählen Sie eine Farm aus und wählen Sie dann Jobs verwalten aus.
2. Wählen Sie auf der Seite Budget Manager auf der Registerkarte Aktive Budgets die Schaltfläche neben dem Budget, das Sie bearbeiten möchten.
3. Wählen Sie im Dropdownmenü Aktionen die Option Budget bearbeiten aus.
4. Nehmen Sie die gewünschten Änderungen vor und wählen Sie dann Budget aktualisieren.

Deaktivieren Sie ein Budget für eine Deadline Cloud-Warteschlange

Sie können jedes aktive Budget deaktivieren. Wenn Sie ein Budget deaktivieren, ändert sich sein Status von Aktiv in Inaktiv. Wenn ein Budget deaktiviert wird, entspricht es einer Ressource nicht mehr dem Betrag dieses Budgets.

Gehen Sie wie folgt vor, um ein Budget zu deaktivieren.

1. Falls Sie dies noch nicht getan haben, melden Sie sich bei der an AWS Management Console, öffnen Sie die Deadline Cloud-Konsole, wählen Sie eine Farm aus und wählen Sie dann Jobs verwalten aus.
2. Wählen Sie auf der Budget-Manager-Seite auf der Registerkarte Aktive Budgets die Schaltfläche neben dem Budget aus, das Sie deaktivieren möchten.
3. Wählen Sie im Dropdownmenü Aktionen die Option Budget deaktivieren aus. In wenigen Augenblicken wechselt das ausgewählte Budget von „Aktiv“ zu „Inaktiv“ und wechselt von der Registerkarte „Aktive Budgets“ in die Registerkarte „Inaktive Budgets“.

Überwachen Sie ein Budget mit EventBridge Ereignissen

Deadline Cloud sendet budgetbezogene Ereignisse mithilfe von Amazon EventBridge an Ihren EventBridge Standard-Eventbus. Sie können benutzerdefinierte Funktionen erstellen, die die Ereignisse empfangen und darauf reagieren, um Benachrichtigungen zu senden, um Benutzer automatisch per E-Mail, Slack oder anderen Kanälen zu benachrichtigen, wenn ein Budget vordefinierte Stufen erreicht. Sie können beispielsweise SMS-Nachrichten senden, wenn ein Budget einen bestimmten Schwellenwert erreicht. Auf diese Weise behalten Sie den Überblick über Ihre Ausgaben und können fundierte Entscheidungen treffen, bevor Ihr Budget aufgebraucht ist.

Deadline Cloud aggregiert regelmäßig Nutzungs- und Kostendaten für jede Renderfarm. Anschließend wird geprüft, ob einer der Budgetschwellenwerte überschritten wurde. Wenn ein Schwellenwert überschritten wird, löst Deadline Cloud ein Ereignis aus, das Sie benachrichtigt, sodass Sie die entsprechenden Maßnahmen ergreifen können. Ein Ereignis wird ausgelöst, wenn ein Budget einen dieser Schwellenwerte überschreitet, die in Prozent des verwendeten Budgets angegeben sind:

- 10, 20, 30, 40, 50, 60, 70, 75, 80, 85, 90, 95, 96, 97, 98, 99, 100

Die Schwellenwerte für die Budgetnutzung rücken näher zusammen, wenn sich ein Budget der 100-prozentigen Nutzung nähert. Auf diese Weise können Sie die Nutzung genau überwachen, wenn das Budget seine Grenzen erreicht. Sie können auch Ihre eigenen Budgetschwellenwerte festlegen. Deadline Cloud sendet ein Ereignis, wenn die Nutzung Ihre benutzerdefinierten Schwellenwerte überschreitet. Sobald Ihr Budget 100 Prozent erreicht hat, sendet Deadline Cloud keine Ereignisse mehr. Wenn Sie Ihr Budget anpassen, sendet Deadline Cloud Ereignisse für Ihre Schwellenwerte, die auf dem neuen Budgetbetrag basieren.

Sie können die EventBridge Konsole (https://console.aws.amazon.com/events/) verwenden, um Regeln zu erstellen, um die Deadline Cloud-Ereignisse an das entsprechende Ziel für das Ereignis zu senden. Sie können das Ereignis beispielsweise an eine Amazon Simple Queue Service-Warteschlange und von dort an mehrere Ziele senden, z. B. an AWS End User Messaging SMS oder eine Amazon Relational Database Service Service-Datenbank zur Protokollierung.

Beispiele für eine EventBridge Regel finden Sie in den folgenden Themen:

- Senden Sie über Amazon eine E-Mail, wenn Ereignisse eintreten EventBridge.
- Erstellen einer EventBridge Amazon-Regel, die Benachrichtigungen an Amazon Q Developer in Chat-Anwendungen sendet.

- Erste Schritte mit Amazon EventBridge.

Weitere Informationen zu Budgetereignissen finden Sie unter der Veranstaltung Budget Threshold Reached im Deadline Cloud Developer Guide.

Verfolgen Sie Nutzung und Kosten mit dem Deadline Cloud-Nutzungsexplorer

Mit dem Deadline Cloud-Nutzungsexplorer können Sie Echtzeit-Metriken zu den Aktivitäten auf jeder Farm einsehen. Sie können sich die Kosten der Farm anhand verschiedener Variablen wie Warteschlange, Auftrag, Lizenzprodukt oder Instanztyp ansehen. Wählen Sie verschiedene Zeitrahmen aus, um sich die Nutzung in einem bestimmten Zeitraum und die Nutzungstrends im Laufe der Zeit anzusehen. Sie können sich auch eine detaillierte Aufschlüsselung der ausgewählten Datenpunkte ansehen, sodass Sie sich die Kennzahlen genauer ansehen können. Die Nutzung kann nach Zeit (Minuten und Stunden) oder nach Kosten (USD) angezeigt werden.

In den folgenden Abschnitten werden die Schritte für den Zugriff auf und die Verwendung des Deadline Cloud-Nutzungsexplorers beschrieben.

Themen

Voraussetzung

Um den Deadline Cloud-Nutzungsexplorer verwenden zu können, benötigen Sie `MANAGER` entweder `OWNER` Farmberechtigungen. Weitere Informationen finden Sie unter Verwalten Sie Benutzer und Gruppen für Farmen, Warteschlangen und Flotten.

Öffnen Sie den Usage Explorer

Gehen Sie wie folgt vor, um den Deadline Cloud-Nutzungsexplorer zu öffnen.

1. Melden Sie sich bei der Deadline Cloud-Konsole an AWS Management Console und öffnen Sie sie.
2. Um alle verfügbaren Farmen zu sehen, wählen Sie Farmen anzeigen.

3. Suchen Sie die Farm, zu der Sie Informationen abrufen möchten, und wählen Sie dann Jobs verwalten aus. Der Deadline Cloud-Monitor wird auf einer neuen Registerkarte geöffnet.
4. Wählen Sie im Deadline Cloud-Monitor im linken Menü die Option Nutzungsexplorer aus.

Verwenden Sie den Usage Explorer

Auf der Seite des Usage Explorers können Sie bestimmte Parameter auswählen, in denen die Daten angezeigt werden können. Standardmäßig wird die Gesamtnutzung in Zeit (Stunden und Minuten) innerhalb der letzten 7 Tage angezeigt. Sie können diese Parameter ändern, und die angezeigten Informationen ändern sich dynamisch entsprechend den Parametereinstellungen.

Sie können die Ergebnisse nach Warteschlange, Auftrag, Computernutzung, Instanztyp oder Lizenzprodukt gruppieren. Wenn Sie sich für ein Lizenzprodukt entscheiden, werden die Kosten für bestimmte Lizenzen berechnet. Für alle anderen Gruppen wird die Zeit berechnet, indem die für die Ausführung der einzelnen Aufgaben benötigte Zeit addiert wird.

Der Usage Explorer gibt auf der Grundlage der von Ihnen festgelegten Filterkriterien nur 100 Ergebnisse zurück. Die Ergebnisse werden in absteigender Reihenfolge nach dem Erstellungsdatum und dem Zeitstempel aufgelistet. Wenn es mehr als 100 Ergebnisse gibt, erhalten Sie eine Fehlermeldung. Sie können Ihre Abfrage verfeinern, um die Anzahl der Ergebnisse zu reduzieren:

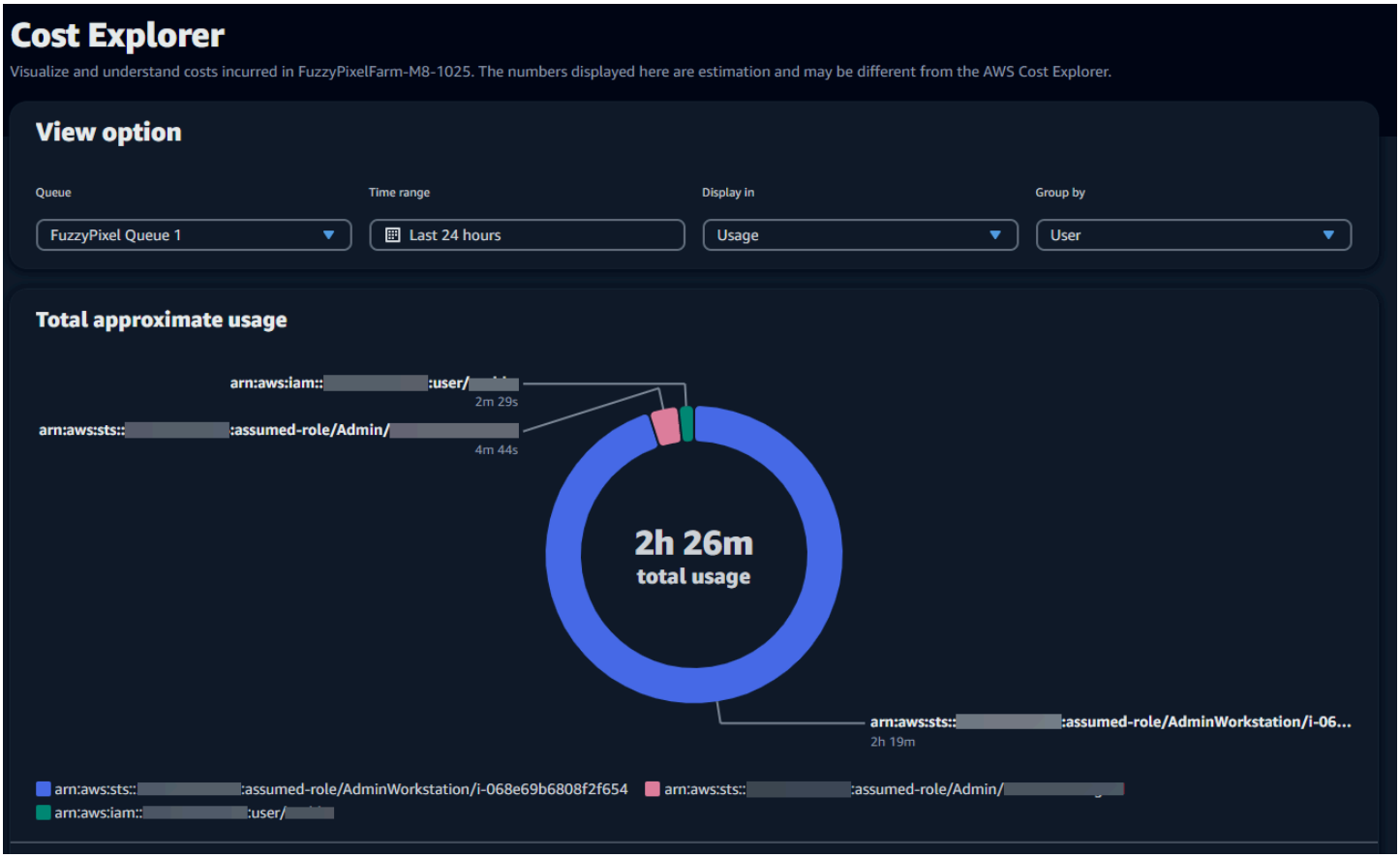
- Wählen Sie einen kleineren Zeitraum
- Wählen Sie weniger Warteschlangen aus
- Wählen Sie eine andere Gruppierung, z. B. eine Gruppierung nach Warteschlange statt nach Job

Themen

Verwenden Sie visuelle Grafiken, um Daten zu überprüfen

Sie können Daten in einem visuellen Format überprüfen, um Trends und potenzielle Bereiche zu identifizieren, die möglicherweise mehr Analyse oder Aufmerksamkeit erfordern. Der Usage Explorer bietet ein Kreisdiagramm, in dem der Gesamtverbrauch und die Kosten angezeigt werden. Es besteht die Möglichkeit, die Gesamtsummen in kleinere Zwischensummen zu gruppieren.

> **Note**
>
> In dem Diagramm werden nur die fünf besten Ergebnisse angezeigt, wobei andere Ergebnisse in einem Abschnitt „Andere“ zusammengefasst sind. Sie können alle Ergebnisse im Aufschlüsselungsbereich unter dem Diagramm einsehen.



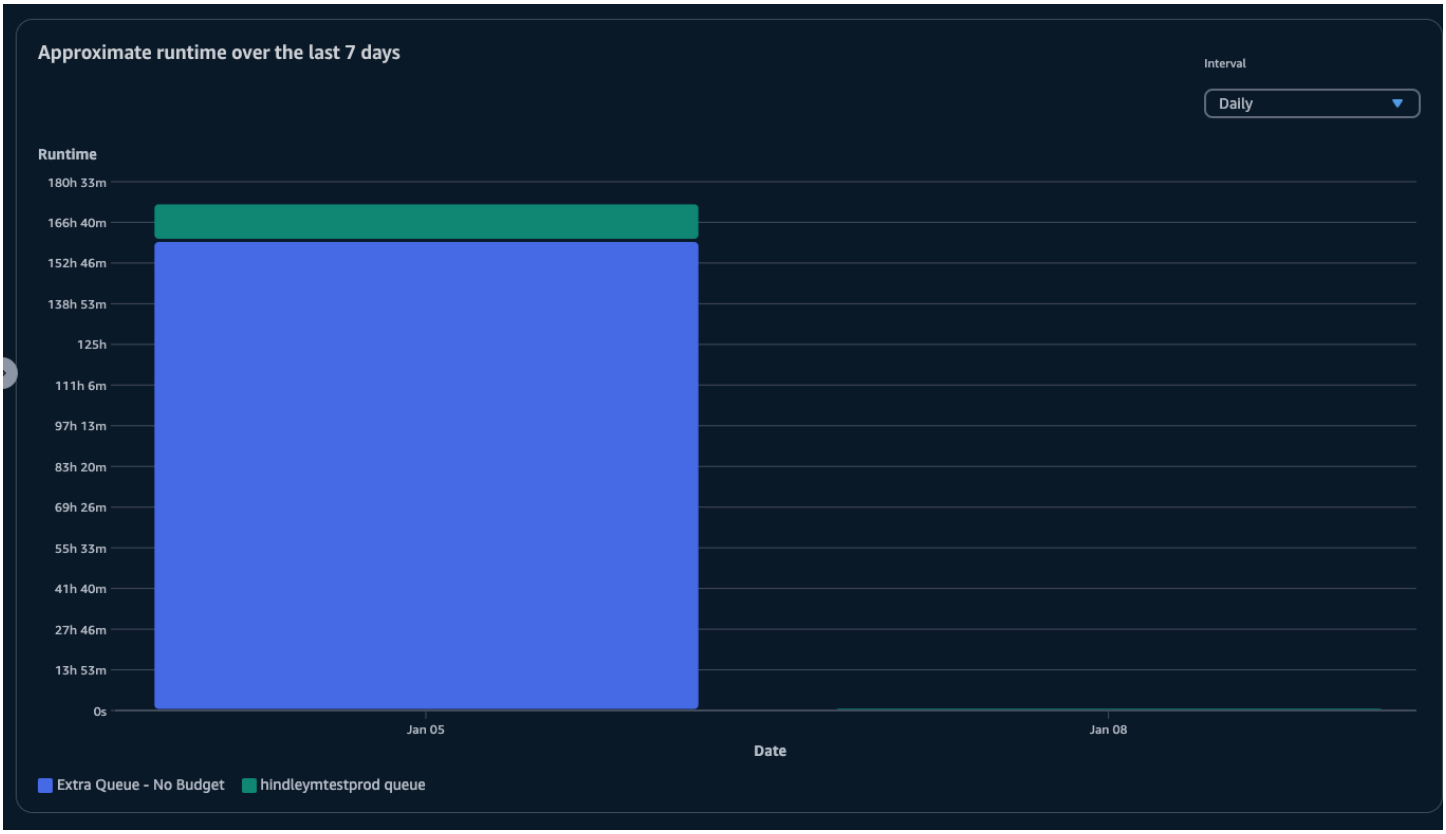
Eine Aufschlüsselung der Messwerte anzeigen

Unter dem Kreisdiagramm bietet der Usage Explorer eine detailliertere Aufschlüsselung bestimmter Metriken, die sich ändern, wenn sich die Parameter ändern. Standardmäßig werden im Usage Explorer fünf Ergebnisse angezeigt. Mithilfe der Seitennummerierungspfeile im Aufschlüsselungsbereich können Sie durch die Ergebnisse blättern.

Die Aufschlüsselung ist standardmäßig minimiert. Um die Ergebnisse zu erweitern und anzuzeigen, wählen Sie den Pfeil Alle Aufschlüsselung anzeigen aus. Um die Aufschlüsselung herunterzuladen, wählen Sie Daten herunterladen.

Ungefähre Laufzeit der Warteschlangen anzeigen

Sie können auch die ungefähre Laufzeit Ihrer Warteschlangen anhand verschiedener von Ihnen festgelegter Intervalle anzeigen. Die Intervalloptionen sind stündlich, täglich, wöchentlich und monatlich. Nachdem Sie ein Intervall ausgewählt haben, zeigt das Diagramm die ungefähre Laufzeit Ihrer Warteschlangen an.



Kostenmanagement

AWS Deadline Cloud bietet Budgets und den Usage Explorer, mit dem Sie die Kosten für Ihre Jobs kontrollieren und visualisieren können. Deadline Cloud verwendet jedoch andere AWS Dienste wie Amazon S3. Die Kosten für diese Dienste sind nicht in den Budgets von Deadline Cloud oder im Usage Explorer enthalten und werden je nach Nutzung separat berechnet. Je nachdem, wie Sie Deadline Cloud konfigurieren, können Sie die folgenden und andere AWS Dienste nutzen:

Service	Seite mit der Preisgestaltung
CloudWatch Amazon-Protokolle	Preise für Amazon CloudWatch Logs

Service	Seite mit der Preisgestaltung
Amazon Elastic Compute Cloud	Preise für Amazon Elastic Compute Cloud
AWS Key Management Service	AWS Key Management Service -Preise
AWS PrivateLink	AWS PrivateLink -Preise
Amazon Simple Storage Service	Amazon Simple Storage Service – Preise
Amazon Virtual Private Cloud	Preise für Amazon Virtual Private Cloud

Bewährte Methoden für das Kostenmanagement

Mithilfe der folgenden bewährten Methoden können Sie Ihre Kosten bei der Verwendung von Deadline Cloud sowie die Kompromisse, die Sie zwischen Kosten und Effizienz eingehen können, besser verstehen und kontrollieren.

> **Note**
>
> Die endgültigen Kosten für die Nutzung von Deadline Cloud hängen von der Interaktion zwischen einer Reihe von AWS Diensten, dem Arbeitsaufwand, den Sie verarbeiten, und dem Ort ab, an AWS-Region dem Sie Ihre Jobs ausführen. Die folgenden bewährten Methoden sind Richtlinien und können die Kosten möglicherweise nicht wesentlich senken.

Bewährte Methoden für CloudWatch Protokolle

Deadline Cloud sendet Mitarbeiter- und CloudWatch Aufgabenprotokolle an Logs. Es wird Ihnen in Rechnung gestellt, diese Protokolle zu sammeln, zu speichern und zu analysieren. Sie können die Kosten senken, indem Sie nur die Mindestmenge an Daten protokollieren, die für die Überwachung Ihrer Aufgaben erforderlich sind.

Wenn Sie eine Warteschlange oder Flotte erstellen, erstellt Deadline Cloud eine CloudWatch Logs-Protokollgruppe mit den folgenden Namen:

- `/aws/deadline/<FARM_ID>/<FLEET_ID>`
- `/aws/deadline/<FARM_ID>/<QUEUE_ID>`

Standardmäßig laufen diese Protokolle nie ab. Sie können die Aufbewahrungsrichtlinie von Protokollgruppen anpassen, um alte Protokolle zu entfernen und die Speicherkosten zu senken. Sie können Protokolle auch nach Amazon S3 exportieren. Die Speicherkosten von Amazon S3 sind niedriger als die für CloudWatch. Weitere Informationen finden Sie unter Exportieren von Protokolldaten zu Amazon S3.

Bewährte Methoden für Amazon EC2

Sie können EC2 Amazon-Instances sowohl für vom Service verwaltete als auch für kundenverwaltete Flotten verwenden. Es gibt drei Überlegungen:

- Bei servicemanagierten Flotten können Sie wählen, ob eine oder mehrere Instances jederzeit verfügbar sein sollen, indem Sie die Mindestanzahl an Mitarbeitern für die Flotte festlegen. Wenn Sie die Mindestanzahl an Arbeitskräften auf 0 setzen, sind in der Flotte immer so viele Mitarbeiter im Einsatz. Dadurch kann die Zeit reduziert werden, die Deadline Cloud benötigt, um mit der Verarbeitung von Jobs zu beginnen. Allerdings wird Ihnen die Leerlaufzeit der Instanz in Rechnung gestellt.
- Legen Sie für servicemanagierte Flotten eine maximale Größe für die Flotte fest. Dadurch wird die Anzahl der Instanzen begrenzt, auf die eine Flotte auto skaliert werden kann. Flotten werden diese Größe nicht überschreiten, selbst wenn mehr Jobs darauf warten, bearbeitet zu werden.
- Sowohl für vom Service verwaltete als auch für kundenverwaltete Flotten können Sie die EC2 Amazon-Instance-Typen in Ihren Flotten angeben. Die Verwendung kleinerer Instances kostet weniger pro Minute, kann aber länger dauern, bis ein Auftrag abgeschlossen ist. Umgekehrt kostet eine größere Instanz mehr pro Minute, kann aber die Zeit bis zur Fertigstellung eines Jobs reduzieren. Wenn Sie die Anforderungen verstehen, die Ihre Jobs an eine Instanz stellen, können Sie Ihre Kosten senken.
- Wählen Sie nach Möglichkeit Amazon EC2 Spot-Instances für Ihre Flotte aus. Spot-Instances sind zu einem reduzierten Preis erhältlich, können jedoch durch On-Demand-Anfragen unterbrochen werden. On-Demand-Instances werden sekundengenau berechnet und nicht unterbrochen.

Bewährte Methoden für AWS KMS

Standardmäßig verschlüsselt Deadline Cloud Ihre Daten mit einem AWS eigenen Schlüssel. Dieser Schlüssel wird Ihnen nicht in Rechnung gestellt.

Sie können sich dafür entscheiden, einen vom Kunden verwalteten Schlüssel zur Verschlüsselung Ihrer Daten zu verwenden. Wenn Sie Ihren eigenen Schlüssel verwenden, wird Ihnen die Gebühr auf

der Grundlage der Verwendung Ihres Schlüssels berechnet. Wenn Sie einen vorhandenen Schlüssel verwenden, fallen zusätzliche Kosten für die zusätzliche Nutzung an.

Bewährte Methoden für AWS PrivateLink

Sie können AWS PrivateLink es verwenden, um mithilfe eines Schnittstellenendpunkts eine Verbindung zwischen Ihrer VPC und Deadline Cloud herzustellen. Wenn Sie eine Verbindung herstellen, können Sie alle Deadline Cloud-API-Aktionen aufrufen. Für jeden Endpunkt, den Sie erstellen, wird Ihnen pro Stunde eine Gebühr berechnet. Wenn Sie verwenden PrivateLink, müssen Sie mindestens drei Endpunkte erstellen, und je nach Konfiguration benötigen Sie möglicherweise bis zu fünf.

Bewährte Methoden für Amazon S3

Deadline Cloud verwendet Amazon S3, um Ressourcen für die Verarbeitung, Jobanhänge, Ausgaben und Protokolle zu speichern. Um die mit Amazon S3 verbundenen Kosten zu senken, reduzieren Sie die Datenmenge, die Sie speichern. Einige Vorschläge:

- Speichern Sie nur Ressourcen, die derzeit verwendet werden oder in Kürze verwendet werden.
- Verwenden Sie eine S3-Lifecycle-Konfiguration, um ungenutzte Dateien automatisch aus einem S3-Bucket zu löschen.

Bewährte Methoden für Amazon VPC

Wenn Sie die nutzungsbasierte Lizenzierung für Ihre vom Kunden verwaltete Flotte verwenden, erstellen Sie einen Deadline Cloud-Lizenzendpunkt, bei dem es sich um einen Amazon VPC-Endpunkt handelt, der in Ihrem Konto erstellt wurde. Dieser Endpunkt wird mit einem Stundensatz berechnet. Um die Kosten zu senken, entfernen Sie die Endgeräte, wenn Sie keine nutzungsbasierten Lizenzen verwenden.

Sicherheit in Deadline Cloud

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

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

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS-Services in der läuft AWS Cloud. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für gelten AWS Deadline Cloud, finden Sie AWS-Services unter Umfang nach Compliance-ProgrammenAWS-Services und unter .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS-Service , was 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 gemeinsamen Verantwortung bei der Verwendung anwenden können Deadline Cloud. In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen Deadline Cloud , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere verwenden können AWS-Services , die Ihnen bei der Überwachung und Sicherung Ihrer Deadline Cloud Ressourcen helfen.

Themen

Datenschutz in Deadline Cloud

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

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

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit der Konsole, der Deadline Cloud API oder auf andere AWS-Services Weise arbeiten oder diese verwenden. AWS CLI AWS SDKs Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet

werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Die in die Namensfelder von Deadline Cloud Jobvorlagen eingegebenen Daten können auch in Abrechnungs- oder Diagnoseprotokollen enthalten sein und sollten keine vertraulichen oder sensiblen Informationen enthalten.

Themen

Verschlüsselung im Ruhezustand

AWS Deadline Cloud schützt sensible Daten, indem sie im Ruhezustand mit den in AWS Key Management Service ()AWS KMS gespeicherten Verschlüsselungsschlüsseln verschlüsselt werden. Verschlüsselung im Ruhezustand ist überall verfügbar, AWS-Regionen wo sie verfügbar Deadline Cloud ist.

Die Verschlüsselung von Daten bedeutet, dass sensible Daten, die auf Festplatten gespeichert sind, für einen Benutzer oder eine Anwendung ohne gültigen Schlüssel nicht lesbar sind. Nur eine Partei mit einem gültigen verwalteten Schlüssel kann die Daten entschlüsseln.

Informationen darüber, wie Deadline Cloud Daten im Ruhezustand verschlüsselt werden können, finden Sie unter. AWS KMS Schlüsselverwaltung

Verschlüsselung während der Übertragung

AWS Deadline Cloud Verwendet für Daten während der Übertragung Transport Layer Security (TLS) 1.2 oder 1.3, um Daten zu verschlüsseln, die zwischen dem Dienst und den Workern gesendet werden. Wir benötigen TLS 1.2 und empfehlen TLS 1.3. Wenn Sie eine Virtual Private Cloud (VPC) verwenden, können Sie darüber hinaus eine private Verbindung zwischen Ihrer VPC und herstellen. AWS PrivateLink Deadline Cloud

Schlüsselverwaltung

Wenn Sie eine neue Farm erstellen, können Sie einen der folgenden Schlüssel zum Verschlüsseln Ihrer Farmdaten wählen:

- AWS eigener KMS-Schlüssel — Standardverschlüsselungstyp, wenn Sie beim Erstellen der Farm keinen Schlüssel angeben. Der KMS-Schlüssel gehört AWS Deadline Cloud. Sie können AWS eigene Schlüssel nicht anzeigen, verwalten oder verwenden. Sie müssen jedoch keine Maßnahmen ergreifen, um die Schlüssel zu schützen, mit denen Ihre Daten verschlüsselt werden. Weitere Informationen finden Sie AWS im AWS Key Management Service Entwicklerhandbuch unter Eigene Schlüssel.
- Kundenverwalteter KMS-Schlüssel — Sie geben einen vom Kunden verwalteten Schlüssel an, wenn Sie eine Farm erstellen. Der gesamte Inhalt der Farm ist mit dem KMS-Schlüssel verschlüsselt. Der Schlüssel wird in Ihrem Konto gespeichert und wird von Ihnen erstellt, gehört und verwaltet. Es AWS KMS fallen Gebühren an. Sie haben die volle Kontrolle über den KMS-Schlüssel. Sie können folgende Aufgaben ausführen:
  - Festlegung und Aufrechterhaltung wichtiger Richtlinien
  - Festlegung und Aufrechterhaltung von IAM-Richtlinien und -Zuschüssen
  - Aktivieren und Deaktivieren wichtiger Richtlinien
  - Hinzufügen von Tags
  - Erstellen von Schlüsselaliasen

  Sie können einen kundeneigenen Schlüssel, der in einer Deadline Cloud Farm verwendet wird, nicht manuell rotieren. Die automatische Rotation des Schlüssels wird unterstützt.

  Weitere Informationen finden Sie im AWS Key Management Service Entwicklerhandbuch unter Schlüssel, die dem Kunden gehören.

  Um einen vom Kunden verwalteten Schlüssel zu erstellen, folgen Sie den Schritten unter Erstellen symmetrischer kundenverwalteter Schlüssel im AWS Key Management Service Entwicklerhandbuch.

Wie werden Deadline Cloud Zuschüsse verwendet AWS KMS

Deadline Cloud erfordert einen Zuschuss, um Ihren vom Kunden verwalteten Schlüssel verwenden zu können. Wenn Sie eine Farm erstellen, die mit einem vom Kunden verwalteten Schlüssel verschlüsselt ist, Deadline Cloud erstellt das Programm in Ihrem Namen einen Zuschuss, indem es

eine `CreateGrant` Anfrage an sendet AWS KMS , um Zugriff auf den von Ihnen angegebenen KMS-Schlüssel zu erhalten.

Deadline Cloud verwendet mehrere Zuschüsse. Jeder Grant wird von einem anderen Teil verwendet Deadline Cloud , der Ihre Daten ver- oder entschlüsseln muss. Deadline Cloud verwendet auch Zuschüsse, um den Zugriff auf andere AWS Dienste zu ermöglichen, die zum Speichern von Daten in Ihrem Namen verwendet werden, wie Amazon Simple Storage Service, Amazon Elastic Block Store oder OpenSearch.

Zuschüsse, die Deadline Cloud die Verwaltung von Maschinen in einer vom `GranteePrincipal` Service verwalteten Flotte ermöglichen, beinhalten eine Deadline Cloud Kontonummer und eine Rolle als Service Principal. Dies ist zwar nicht üblich, aber notwendig, um Amazon EBS-Volumes für Mitarbeiter in serviceverwalteten Flotten mit dem für die Farm angegebenen kundenverwalteten KMS-Schlüssel zu verschlüsseln.

Kundenverwaltete CMK-Schlüsselrichtlinie

Schlüsselrichtlinien steuern den Zugriff auf den vom Kunden verwalteten Schlüssel. Jeder Schlüssel muss über genau eine Schlüsselrichtlinie verfügen, die Aussagen enthält, die festlegen, wer den Schlüssel verwenden darf und wie er verwendet werden darf. Wenn Sie Ihren vom Kunden verwalteten Schlüssel erstellen, können Sie eine Schlüsselrichtlinie angeben. Weitere Informationen finden Sie unter Verwalten des Zugriffs auf kundenverwaltete Schlüssel im Entwicklerhandbuch zum AWS Key Management Service .

Minimale IAM-Richtlinie für CreateFarm

Um Ihren vom Kunden verwalteten Schlüssel zum Erstellen von Farmen mithilfe der Konsole oder des `CreateFarm` API-Vorgangs zu verwenden, müssen die folgenden AWS KMS API-Operationen zugelassen sein:

- `kms:CreateGrant`: Fügt einem kundenverwalteten Schlüssel eine Erteilung hinzu. Gewährt Konsolenzugriff auf einen angegebenen AWS KMS Schlüssel. Weitere Informationen finden Sie im AWS Key Management Service Entwicklerhandbuch unter Using Grants.
- `kms:Decrypt`— Ermöglicht Deadline Cloud das Entschlüsseln von Daten in der Farm.
- `kms:DescribeKey`— Stellt dem Kunden verwaltete Schlüsseldetails zur Verfügung, damit Deadline Cloud der Schlüssel validiert werden kann.
- `kms:GenerateDataKey`— Ermöglicht Deadline Cloud die Verschlüsselung von Daten mit einem eindeutigen Datenschlüssel.

Die folgende Richtlinienerklärung gewährt die erforderlichen Berechtigungen für den `CreateFarm` Vorgang.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DeadlineCreateGrants",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey",
                "kms:CreateGrant",
                "kms:DescribeKey"
            ],
            "Resource": "arn:aws::kms:us-west-2:111122223333:key/1234567890abcdef0",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "deadline.us-west-2.amazonaws.com"
                }
            }
        }
    ]
}
```

Minimale IAM-Richtlinie für schreibgeschützte Operationen

Um Ihren vom Kunden verwalteten Schlüssel für schreibgeschützte Deadline Cloud Operationen zu verwenden, z. B. für das Abrufen von Informationen über Farmen, Warteschlangen und Flotten. Die folgenden AWS KMS API-Operationen müssen zulässig sein:

- `kms:Decrypt`— Ermöglicht Deadline Cloud das Entschlüsseln von Daten in der Farm.
- `kms:DescribeKey`— Stellt dem Kunden verwaltete Schlüsseldetails zur Verfügung, damit Deadline Cloud der Schlüssel validiert werden kann.

Die folgende Richtlinienerklärung gewährt die erforderlichen Berechtigungen für schreibgeschützte Operationen.

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

```
        {
            "Sid": "DeadlineReadOnly",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
            "Resource": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "deadline.us-west-2.amazonaws.com"
                }
            }
        }
    ]
}
```

Minimale IAM-Richtlinie für Lese- und Schreibvorgänge

Um Ihren vom Kunden verwalteten Schlüssel für Lese- und Deadline Cloud Schreibvorgänge wie das Erstellen und Aktualisieren von Farmen, Warteschlangen und Flotten zu verwenden. Die folgenden AWS KMS API-Operationen müssen zulässig sein:

- `kms:Decrypt`— Ermöglicht Deadline Cloud das Entschlüsseln von Daten in der Farm.
- `kms:DescribeKey`— Stellt dem Kunden verwaltete Schlüsseldetails zur Verfügung, damit Deadline Cloud der Schlüssel validiert werden kann.
- `kms:GenerateDataKey`— Ermöglicht Deadline Cloud die Verschlüsselung von Daten mit einem eindeutigen Datenschlüssel.

Die folgende Richtlinienerklärung gewährt die erforderlichen Berechtigungen für den `CreateFarm` Vorgang.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DeadlineReadWrite",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
```

```
                "kms:DescribeKey",
                "kms:GenerateDataKey",
            ],
            "Resource": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "deadline.us-west-2.amazonaws.com"
                }
            }
        }
    ]
}
```

Überwachen Ihrer Verschlüsselungsschlüssel

Wenn Sie einen vom AWS KMS Kunden verwalteten Schlüssel für Ihre Deadline Cloud Farmen verwenden, können Sie Amazon CloudWatch Logs verwenden AWS CloudTrail, um Anfragen zu verfolgen, die Deadline Cloud an gesendet AWS KMS werden.

CloudTrail Veranstaltung für Zuschüsse

Das folgende CloudTrail Beispielereignis tritt ein, wenn Zuschüsse erstellt werden, in der Regel, wenn Sie die `CreateFleet` Operation `CreateFarmCreateMonitor`, oder aufrufen.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:SampleUser01",
        "arn": "arn:aws::sts::111122223333:assumed-role/Admin/SampleUser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws::iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
```

```
                "creationDate": "2024-04-23T02:05:26Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "deadline.amazonaws.com"
    },
    "eventTime": "2024-04-23T02:05:35Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "deadline.amazonaws.com",
    "userAgent": "deadline.amazonaws.com",
    "requestParameters": {
        "operations": [
            "CreateGrant",
            "Decrypt",
            "DescribeKey",
            "Encrypt",
            "GenerateDataKey"
        ],
        "constraints": {
            "encryptionContextSubset": {
                "aws:deadline:farmId": "farm-abcdef1234567890098765432 1fedcba",
                "aws:deadline:accountId": "111122223333"
            }
        },
        "granteePrincipal": "deadline.amazonaws.com",
        "keyId": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
        "retiringPrincipal": "deadline.amazonaws.com"
    },
    "responseElements": {
        "grantId": "6bbe819394822a400fe5e3a75d0e9ef16c1733143fff0c1fc00dc7ac282a18a0",
        "keyId": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
    },
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "readOnly": false,
    "resources": [
        {
            "accountId": "AWS Internal",
            "type": "AWS::KMS::Key",
```

```
            "ARN": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE44444"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

CloudTrail Ereignis für die Entschlüsselung

Das folgende CloudTrail Beispielereignis tritt ein, wenn Werte mithilfe des vom Kunden verwalteten KMS-Schlüssels entschlüsselt werden.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:SampleUser01",
        "arn": "arn:aws::sts::111122223333:assumed-role/SampleRole/SampleUser01",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws::iam::111122223333:role/SampleRole",
                "accountId": "111122223333",
                "userName": "SampleRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-04-23T18:46:51Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "deadline.amazonaws.com"
    },
    "eventTime": "2024-04-23T18:51:44Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
```

```
    "sourceIPAddress": "deadline.amazonaws.com",
    "userAgent": "deadline.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:deadline:farmId": "farm-abcdef12345678900987654321fedcba",
            "aws:deadline:accountId": "111122223333",
            "aws-crypto-public-key": "AotL+SAMPLEVALUEiOMEXAMPLEaaqNOTREALaGTESTONLY
+p/5H+EuKd4Q=="
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "keyId": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
    },
    "responseElements": null,
    "requestID": "aaaaaaaa-bbbb-cccc-dddd-eeeeeeffffff",
    "eventID": "ffffffff-eeee-dddd-cccc-bbbbbbaaaaaa",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

CloudTrail Ereignis für die Verschlüsselung

Das folgende CloudTrail Beispielereignis tritt ein, wenn Werte mit dem vom Kunden verwalteten KMS-Schlüssel verschlüsselt werden.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROAIGDTESTANDEXAMPLE:SampleUser01",
        "arn": "arn:aws::sts::111122223333:assumed-role/SampleRole/SampleUser01",
        "accountId": "111122223333",
```

```
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROAIGDTESTANDEXAMPLE",
                "arn": "arn:aws::iam::111122223333:role/SampleRole",
                "accountId": "111122223333",
                "userName": "SampleRole"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2024-04-23T18:46:51Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "deadline.amazonaws.com"
    },
    "eventTime": "2024-04-23T18:52:40Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "deadline.amazonaws.com",
    "userAgent": "deadline.amazonaws.com",
    "requestParameters": {
        "numberOfBytes": 32,
        "encryptionContext": {
            "aws:deadline:farmId": "farm-abcdef1234567890098765432 1fedcba",
            "aws:deadline:accountId": "111122223333",
            "aws-crypto-public-key": "AotL+SAMPLEVALUEiOMEXAMPLEaaqNOTREALaGTESTONLY
+p/5H+EuKd4Q=="
        },
        "keyId": "arn:aws::kms:us-
west-2:111122223333:key/abcdef12-3456-7890-0987-654321fedcba"
    },
    "responseElements": null,
    "requestID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "eventID": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws::kms:us-west-2:111122223333:key/a1b2c3d4-5678-90ab-cdef-
EXAMPLE33333"
```

```
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Löschen eines vom Kunden verwalteten KMS-Schlüssels

Das Löschen eines vom Kunden verwalteten KMS-Schlüssels in AWS Key Management Service (AWS KMS) ist destruktiv und potenziell gefährlich. Dadurch werden das Schlüsselmaterial und alle mit dem Schlüssel verknüpften Metadaten unwiderruflich gelöscht. Nachdem ein vom Kunden verwalteter KMS-Schlüssel gelöscht wurde, können Sie die mit diesem Schlüssel verschlüsselten Daten nicht mehr entschlüsseln. Das bedeutet, dass die Daten nicht mehr wiederhergestellt werden können.

Aus diesem Grund AWS KMS haben Kunden eine Wartezeit von bis zu 30 Tagen, bevor der KMS-Schlüssel gelöscht wird. Die Standardwartezeit beträgt 30 Tage.

Über die Wartezeit

Da das Löschen eines vom Kunden verwalteten KMS-Schlüssels zerstörerisch und potenziell gefährlich ist, müssen Sie eine Wartezeit von 7—30 Tagen festlegen. Die Standardwartezeit beträgt 30 Tage.

Die tatsächliche Wartezeit kann jedoch bis zu 24 Stunden länger sein als der von Ihnen geplante Zeitraum. Um das tatsächliche Datum und die Uhrzeit der Löschung des Schlüssels zu ermitteln, verwenden Sie den DescribeKeyOperation. Sie können das geplante Löschdatum eines Schlüssels auch in der AWS KMS Konsole auf der Detailseite des Schlüssels im Abschnitt Allgemeine Konfiguration sehen. Beachten Sie die Zeitzone.

Während der Wartezeit lautet der Status und der Schlüsselstatus des vom Kunden verwalteten Schlüssels „Ausstehende Löschung“.

- Ein vom Kunden verwalteter KMS-Schlüssel, dessen Löschung aussteht, kann für keine kryptografischen Operationen verwendet werden.
- AWS KMS rotiert nicht die Backing-Schlüssel von vom Kunden verwalteten KMS-Schlüsseln, deren Löschung noch aussteht.

Weitere Informationen zum Löschen eines vom Kunden verwalteten KMS-Schlüssels finden Sie unter Löschen von Kundenhauptschlüsseln im AWS Key Management Service Entwicklerhandbuch.

Datenschutz für den Datenverkehr zwischen Netzwerken

AWS Deadline Cloud unterstützt Amazon Virtual Private Cloud (Amazon VPC) zur Sicherung von Verbindungen. Amazon VPC bietet Funktionen, mit denen Sie die Sicherheit Ihrer Virtual Private Cloud (VPC) erhöhen und überwachen können.

Sie können eine vom Kunden verwaltete Flotte (CMF) mit Amazon Elastic Compute Cloud (Amazon EC2) -Instances einrichten, die in einer VPC ausgeführt werden. Durch die Bereitstellung von Amazon VPC-Endpunkten zur Nutzung AWS PrivateLink bleibt der Datenverkehr zwischen Workern in Ihrem CMF und dem Deadline Cloud Endpunkt innerhalb Ihrer VPC. Darüber hinaus können Sie Ihre VPC so konfigurieren, dass der Internetzugang auf Ihre Instances beschränkt wird.

In serviceverwalteten Flotten sind die Mitarbeiter nicht über das Internet erreichbar, sie haben jedoch Internetzugang und stellen über das Internet eine Verbindung zum Deadline Cloud Service her.

Abmelden

AWS Deadline Cloud sammelt bestimmte Betriebsinformationen, um uns bei der Entwicklung und Verbesserung zu unterstützen Deadline Cloud. Zu den gesammelten Daten gehören Dinge wie Ihre AWS Konto-ID und Benutzer-ID, sodass wir Sie korrekt identifizieren können, falls Sie ein Problem mit der haben Deadline Cloud. Wir erfassen auch Deadline Cloud spezifische Informationen wie Ressourcen IDs (eine FarmID oder QueueID, falls zutreffend), den Produktnamen (z. B. JobAttachments WorkerAgent, und mehr) und die Produktversion.

Sie können diese Datenerfassung mithilfe der Anwendungskonfiguration deaktivieren. Jeder Computer Deadline Cloud, mit dem sowohl Client-Workstations als auch Flottenmitarbeiter interagiert, muss sich separat abmelden.

Deadline Cloud Monitor — Desktop

Deadline Cloud monitor — desktop sammelt Betriebsinformationen, z. B. wann Abstürze auftreten und wann die Anwendung geöffnet wird, damit wir wissen, wenn Sie Probleme mit der Anwendung haben. Um die Erfassung dieser Betriebsinformationen zu deaktivieren, deaktivieren Sie auf der Einstellungsseite die Option Datenerfassung aktivieren, um die Leistung von Deadline Cloud Monitor zu messen.

Nachdem Sie sich abmelden, sendet der Desktop-Monitor die Betriebsdaten nicht mehr. Alle zuvor gesammelten Daten werden gespeichert und können weiterhin zur Verbesserung des Dienstes verwendet werden. Weitere Informationen finden Sie in den Häufig gestellten Fragen zum Datenschutz.

AWS Deadline Cloud CLI und Tools

Die AWS Deadline Cloud CLI, die Einreicher und der Worker Agent sammeln alle Betriebsinformationen, z. B. wann Abstürze auftreten und wann Jobs eingereicht werden, damit wir wissen, wenn Sie Probleme mit diesen Anwendungen haben. Verwenden Sie eine der folgenden Methoden, um sich von der Erfassung dieser Betriebsinformationen abzumelden:

- Geben Sie im Terminal ein**`deadline config set telemetry.opt_out true`**.

  Dadurch werden die CLI, die Einreicher und der Worker-Agent deaktiviert, wenn sie als aktueller Benutzer ausgeführt werden.
- Fügen Sie bei der Installation des Deadline Cloud Worker-Agenten das **`--telemetry-opt-out`** Befehlszeilenargument hinzu. Beispiel, **`./install.sh --farm-id $FARM_ID --fleet-id $FLEET_ID --telemetry-opt-out`**.
- Bevor Sie den Worker-Agent, die CLI oder den Submitter ausführen, legen Sie eine Umgebungsvariable fest: **`DEADLINE_CLOUD_TELEMETRY_OPT_OUT=true`**

Nach dem Abmelden senden die Deadline Cloud Tools keine Betriebsdaten mehr. Alle zuvor gesammelten Daten werden gespeichert und können weiterhin zur Verbesserung des Dienstes verwendet werden. Weitere Informationen finden Sie in den Häufig gestellten Fragen zum Datenschutz.

Identity and Access Management in Deadline Cloud

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Deadline Cloud-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Deadline Cloud erledigen.

Dienstbenutzer — Wenn Sie den Deadline Cloud-Dienst für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Wenn Sie für Ihre Arbeit mehr Funktionen von Deadline Cloud verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Wenn Sie auf eine Funktion in Deadline Cloud nicht zugreifen können, finden Sie weitere Informationen unterFehlerbehebung bei AWS Deadline Cloud-Identität und -Zugriff.

Serviceadministrator — Wenn Sie in Ihrem Unternehmen für die Ressourcen von Deadline Cloud verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Deadline Cloud. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen von Deadline Cloud Ihre Servicebenutzer zugreifen sollen. Anschließend müssen Sie Anforderungen an Ihren IAM-Administrator senden, um die Berechtigungen der Servicebenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit Deadline Cloud nutzen kann, finden Sie unterSo funktioniert Deadline Cloud mit IAM.

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Deadline Cloud zu verwalten. Beispiele für identitätsbasierte Richtlinien von Deadline Cloud, die Sie in IAM verwenden können, finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Deadline Cloud

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS , übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportal anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter So melden Sie sich bei Ihrem an AWS-Konto im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, um Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch zu signieren. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode für die Selbstsignierung von Anforderungen finden Sie unter AWS Signature Version 4 für API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen bereitstellen. AWS Empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter Multi-Faktor-Authentifizierung im AWS IAM Identity Center -Benutzerhandbuch und AWS Multi-Faktor-Authentifizierung (MFA) in IAM im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen. Verwenden Sie diese nur, 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 sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, 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 in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten 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 innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. 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 eine Gruppe benennen IAMAdminsund dieser Gruppe Berechtigungen zur Verwaltung 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 Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität innerhalb von Ihnen AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, jedoch nicht mit einer bestimmten Person verknüpft. Um vorübergehend eine IAM-Rolle in der zu übernehmen AWS Management Console, können Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln. Sie können eine Rolle übernehmen, 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 Methoden für die Übernahme einer Rolle 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 (Verbund) 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. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise in einem Service einen Anruf tätigen, ist es üblich, dass dieser Service Anwendungen in Amazon ausführt EC2 oder Objekte in Amazon S3 speichert. 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 verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. 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 aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. 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.
  - Dienstbezogene Rolle — Eine dienstbezogene Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- Auf Amazon ausgeführte Anwendungen EC2 — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2 Instance ausgeführt werden und AWS API-Anfragen stellen AWS CLI . Dies ist dem Speichern von Zugriffsschlüsseln innerhalb der EC2 Instance vorzuziehen. Um einer EC2 Instanz eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instanzprofil, das an die Instanz angehängt ist. Ein Instanzprofil enthält die Rolle und ermöglicht Programmen, die auf der EC2 Instanz ausgeführt werden, temporäre Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Verwenden einer IAM-Rolle, um Berechtigungen für Anwendungen zu gewähren, die auf EC2 Amazon-Instances ausgeführt werden.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Die Berechtigungen in den Richtlinien legen fest, ob eine Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden 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 angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

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 Rolleninformationen von der AWS Management Console AWS CLI, der oder der 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 Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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 System zuordnen können AWS-Konto.

Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer Inline-Richtlinie wählen, finden Sie unter Auswählen 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. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF Weitere Informationen finden Sie unter Übersicht über ACLs die Zugriffskontrollliste (ACL) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete 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. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im IAM-Benutzerhandbuch.

- Dienststeuerungsrichtlinien (SCPs) — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie alle Funktionen in einer Organisation aktivieren, können Sie Richtlinien zur Servicesteuerung (SCPs) auf einige oder alle Ihre Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Root-Benutzer des AWS-Kontos Entitäten. Weitere Informationen zu Organizations und SCPs finden Sie unter Richtlinien zur Servicesteuerung im AWS Organizations Benutzerhandbuch.
- Ressourcenkontrollrichtlinien (RCPs) — RCPs sind JSON-Richtlinien, mit denen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten festlegen können, ohne die IAM-Richtlinien aktualisieren zu müssen, die jeder Ressource zugeordnet sind, deren Eigentümer Sie sind. Das RCP schränkt die Berechtigungen für Ressourcen in Mitgliedskonten ein und kann sich auf die effektiven Berechtigungen für Identitäten auswirken, einschließlich der Root-Benutzer des AWS-Kontos, unabhängig davon, ob sie zu Ihrer Organisation gehören. Weitere Informationen zu Organizations RCPs, einschließlich einer Liste AWS-Services dieser Support-Leistungen RCPs, finden Sie unter Resource Control Policies (RCPs) 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 darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

So funktioniert Deadline Cloud mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Deadline Cloud zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen mit Deadline Cloud verwendet werden können.

IAM-Funktionen, die Sie mit Deadline Cloud verwenden können AWS

IAM-Feature	Deadline Cloud-Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Richtlinienbedingungsschlüssel (services pezifisch)	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja
Forward Access Sessions (FAS)	Ja
Servicerollen	Ja
Service-verknüpfte Rollen	Nein

Einen allgemeinen Überblick darüber, wie Deadline Cloud und andere mit den meisten IAM-Funktionen AWS-Services funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Dienste, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für Deadline Cloud

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 Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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 Deadline Cloud

Beispiele für identitätsbasierte Richtlinien von Deadline Cloud finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Deadline Cloud

Ressourcenbasierte Richtlinien in Deadline Cloud

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. Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

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 unterscheiden AWS-Konten, muss ein IAM-Administrator des vertrauenswürdigen Kontos 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 Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Richtlinienaktionen für Deadline Cloud

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

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 der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang 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 Deadline Cloud-Aktionen finden Sie unter Von AWS Deadline Cloud definierte Aktionen in der Serviceautorisierungsreferenz.

Richtlinienaktionen in Deadline Cloud verwenden vor der Aktion das folgende Präfix:

```
deadline
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "deadline:action1",
      "deadline:action2"
         ]
```

Beispiele für identitätsbasierte Richtlinien von Deadline Cloud finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Deadline Cloud

Richtlinienressourcen für Deadline Cloud

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und 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 Deadline Cloud-Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter Von AWS Deadline Cloud definierte Ressourcen in der Service Authorization Reference. Informationen dazu, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter Von AWS Deadline Cloud definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien von Deadline Cloud finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Deadline Cloud

Bedingungsschlüssel für Richtlinien für Deadline Cloud

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. 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, AWS wertet die Bedingung mithilfe 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 dienstspezifische Bedingungsschlüssel. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der Deadline Cloud-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für AWS Deadline Cloud in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von AWS Deadline Cloud definierte Aktionen.

Beispiele für identitätsbasierte Richtlinien von Deadline Cloud finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Deadline Cloud

ACLs in Deadline Cloud

Unterstützt ACLs: Nein

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

ABAC mit Deadline Cloud

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 an viele AWS Ressourcen anhängen. 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 Bedingung `aws:TagKeys` 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 Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Verwenden temporärer Anmeldeinformationen mit Deadline Cloud

Unterstützt temporäre Anmeldeinformationen: Ja

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services funktionieren AWS-Services , finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. 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 von einer Benutzerrolle zu einer IAM-Rolle (Konsole) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden

AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Zugriffssitzungen für Deadline Cloud weiterleiten

Unterstützt Forward Access Sessions (FAS): Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. 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 aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. 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 Deadline Cloud

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.

> **Warning**
>
> Das Ändern der Berechtigungen für eine Servicerolle kann die Funktionalität von Deadline Cloud beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Deadline Cloud Sie dazu anleitet.

Servicebezogene Rollen für Deadline Cloud

Unterstützt serviceverknüpfte Rollen: Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen.

Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Details zum Erstellen oder Verwalten von serviceverknüpften Rollen finden Sie unter AWS -Services, die mit IAM funktionieren. 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.

Beispiele für identitätsbasierte Richtlinien für Deadline Cloud

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Deadline Cloud-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder 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 (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von Deadline Cloud definierten Aktionen und Ressourcentypen, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für AWS Deadline Cloud in der Service Authorization Reference.

Themen

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Deadline Cloud-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:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um Ihren Benutzern und Workloads zunächst Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS -verwaltete Richtlinien oder AWS -verwaltete Richtlinien für Auftrags-Funktionen 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 Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. 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 mit IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, 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 Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Bewährte Methoden für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden Sie die Deadline Cloud-Konsole

Um auf die AWS Deadline Cloud-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Deadline Cloud-Ressourcen in Ihrem aufzulisten und einzusehen AWS-Konto. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die Deadline Cloud-Konsole weiterhin verwenden können, fügen Sie den Entitäten auch die Deadline Cloud *ConsoleAccess* oder die *ReadOnly* AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zu einem Benutzer im IAM-Benutzerhandbuch.

Richtlinie zum Einreichen von Jobs an eine Warteschlange

In diesem Beispiel erstellen Sie eine Richtlinie mit eingeschränktem Geltungsbereich, die die Berechtigung zum Senden von Aufträgen an eine bestimmte Warteschlange in einer bestimmten Farm erteilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "SubmitJobsFarmAndQueue",
            "Effect": "Allow",
            "Action": "deadline:CreateJob",
            "Resource": "arn:aws:deadline:REGION:ACCOUNT_ID:farm/FARM_A/queue/QUEUE_B/
job/*"
        }
    ]
```

```
}
```

Richtlinie, die die Erstellung eines Lizenzendpunkts ermöglicht

In diesem Beispiel erstellen Sie eine nach unten abgegrenzte Richtlinie, die die erforderlichen Berechtigungen zum Erstellen und Verwalten von Lizenzendpunkten gewährt. Verwenden Sie diese Richtlinie, um den Lizenzendpunkt für die VPC zu erstellen, die Ihrer Farm zugeordnet ist.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "SID": "CreateLicenseEndpoint",
        "Effect": "Allow",
        "Action": [
            "deadline:CreateLicenseEndpoint",
            "deadline:DeleteLicenseEndpoint",
            "deadline:GetLicenseEndpoint",
            "deadline:UpdateLicenseEndpoint",
            "deadline:ListLicenseEndpoints",
            "deadline:PutMeteredProduct",
            "deadline:DeleteMeteredProduct",
            "deadline:ListMeteredProducts",
            "deadline:ListAvailableMeteredProducts",
            "ec2:CreateVpcEndpoint",
            "ec2:DescribeVpcEndpoints",
            "ec2:DeleteVpcEndpoints"
        ],
        "Resource": "*"
    }]
}
```

Richtlinie, die die Überwachung einer bestimmten Farmwarteschlange ermöglicht

In diesem Beispiel erstellen Sie eine Richtlinie mit eingeschränktem Geltungsbereich, die die Erlaubnis erteilt, Jobs in einer bestimmten Warteschlange für eine bestimmte Farm zu überwachen.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "MonitorJobsFarmAndQueue",
        "Effect": "Allow",
        "Action": [
```

```
            "deadline:SearchJobs",
            "deadline:ListJobs",
            "deadline:GetJob",
            "deadline:SearchSteps",
            "deadline:ListSteps",
            "deadline:ListStepConsumers",
            "deadline:ListStepDependencies",
            "deadline:GetStep",
            "deadline:SearchTasks",
            "deadline:ListTasks",
            "deadline:GetTask",
            "deadline:ListSessions",
            "deadline:GetSession",
            "deadline:ListSessionActions",
            "deadline:GetSessionAction"
        ],
        "Resource": [
            "arn:aws:deadline:REGION:123456789012:farm/FARM_A/queue/QUEUE_B",
            "arn:aws:deadline:REGION:123456789012:farm/FARM_A/queue/QUEUE_B/*"
        ]
    }]
}
```

AWS verwaltete Richtlinien für Deadline Cloud

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AWSDeadlineCloud-FleetWorker

Sie können die `AWSDeadlineCloud-FleetWorker` Richtlinie an Ihre AWS Identity and Access Management (IAM-) Identitäten anhängen.

Diese Richtlinie gewährt den Mitarbeitern dieser Flotte die Berechtigungen, die sie benötigen, um eine Verbindung mit dem Service herzustellen und Aufgaben vom Service zu empfangen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `deadline`— Ermöglicht es Prinzipalen, Mitarbeiter in einer Flotte zu verwalten.

Eine JSON-Liste der Richtliniendetails finden Sie AWSDeadlineCloud-FleetWorkerim Referenzhandbuch zu AWS Managed Policy.

AWS verwaltete Richtlinie: AWSDeadlineCloud-WorkerHost

Sie können die `AWSDeadlineCloud-WorkerHost`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt die Berechtigungen, die für die anfängliche Verbindung mit dem Dienst erforderlich sind. Es kann als Amazon Elastic Compute Cloud (Amazon EC2) -Instanzprofil verwendet werden.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `deadline`— Ermöglicht es Prinzipalen, Worker zu erstellen.

Eine JSON-Liste der Richtliniendetails finden Sie AWSDeadlineCloud-WorkerHostim Referenzhandbuch zu AWS Managed Policy.

AWS verwaltete Richtlinie: AWSDeadlineCloud-UserAccessFarms

Sie können die `AWSDeadlineCloud-UserAccessFarms`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie ermöglicht Benutzern den Zugriff auf Farmdaten auf der Grundlage der Farmen, in denen sie Mitglied sind, und ihrer Mitgliedschaftsstufe.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `deadline`— Ermöglicht dem Benutzer den Zugriff auf Farmdaten.
- `ec2`— Ermöglicht Benutzern, Details zu EC2 Amazon-Instance-Typen zu sehen.
- `identitystore`— Ermöglicht Benutzern, Benutzer- und Gruppennamen zu sehen.

Eine JSON-Liste der Richtliniendetails finden Sie AWSDeadlineCloud-UserAccessFarmsim Referenzhandbuch zu AWS Managed Policy.

AWS verwaltete Richtlinie: AWSDeadlineCloud-UserAccessFleets

Sie können die `AWSDeadlineCloud-UserAccessFleets`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie ermöglicht Benutzern den Zugriff auf Flottendaten auf der Grundlage der Farmen, in denen sie Mitglied sind, und ihrer Mitgliedschaftsstufe.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `deadline`— Ermöglicht dem Benutzer den Zugriff auf Farmdaten.
- `ec2`— Ermöglicht Benutzern, Details zu EC2 Amazon-Instance-Typen zu sehen.
- `identitystore`— Ermöglicht Benutzern, Benutzer- und Gruppennamen zu sehen.

Eine JSON-Liste der Richtliniendetails finden Sie AWSDeadlineCloud-UserAccessFleetsim Referenzhandbuch zu AWS Managed Policy.

AWS verwaltete Richtlinie: AWSDeadlineCloud-UserAccessJobs

Sie können die `AWSDeadlineCloud-UserAccessJobs`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie ermöglicht Benutzern den Zugriff auf Auftragsdaten auf der Grundlage der Farmen, in denen sie Mitglied sind, und ihrer Mitgliedschaftsstufe.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `deadline`— Ermöglicht dem Benutzer den Zugriff auf Farmdaten.
- `ec2`— Ermöglicht Benutzern, Details zu EC2 Amazon-Instance-Typen zu sehen.
- `identitystore`— Ermöglicht Benutzern, Benutzer- und Gruppennamen zu sehen.

Eine JSON-Liste der Richtliniendetails finden Sie AWSDeadlineCloud-UserAccessJobsim Referenzhandbuch zu AWS Managed Policy.

AWS verwaltete Richtlinie: AWSDeadlineCloud-UserAccessQueues

Sie können die `AWSDeadlineCloud-UserAccessQueues`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie ermöglicht Benutzern den Zugriff auf Warteschlangendaten auf der Grundlage der Farmen, in denen sie Mitglied sind, und ihrer Mitgliedschaftsstufe.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `deadline`— Ermöglicht dem Benutzer den Zugriff auf Farmdaten.
- `ec2`— Ermöglicht Benutzern, Details zu EC2 Amazon-Instance-Typen zu sehen.
- `identitystore`— Ermöglicht Benutzern, Benutzer- und Gruppennamen zu sehen.

Eine JSON-Liste der Richtliniendetails finden Sie AWSDeadlineCloud-UserAccessQueuesim Referenzhandbuch zu AWS Managed Policy.

Deadline Cloud-Updates für AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Deadline Cloud an, seit dieser Dienst begonnen hat, diese Änderungen zu verfolgen. Um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Deadline Cloud-Dokumentverlaufsseite.

Änderung	Beschreibung	Datum
AWSDeadlineCloud-UserAccessFarms— Änderung AWSDeadlineCloud-UserAccessJobs— Veränderung AWSDeadlineCloud-UserAccessQueues— Veränderung	Deadline Cloud hat neue Aktionen `deadline:GetJobTemplate` hinzugefügt`deadline:ListJobParameterDefinitions` , sodass Sie Jobs erneut einreichen können.	7. Oktober 2024
Deadline Cloud hat begonnen, Änderungen zu verfolgen	Deadline Cloud begann, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	2. April 2024

Fehlerbehebung bei AWS Deadline Cloud-Identität und -Zugriff

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

Themen

- Ich bin nicht berechtigt, eine Aktion in Deadline Cloud durchzuführen
- Ich bin nicht berechtigt, iam durchzuführen: PassRole
- Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Deadline Cloud-Ressourcen ermöglichen

Ich bin nicht berechtigt, eine Aktion in Deadline Cloud durchzuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `deadline:`*`GetWidget`*-Berechtigungen verfügt.

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

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `deadline:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam durchzuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion durchzuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Deadline Cloud übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Dienst zu übergeben, anstatt eine neue Servicerolle oder eine dienstverknüpfte Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Deadline Cloud 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.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Deadline Cloud-Ressourcen ermöglichen

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

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Deadline Cloud diese Funktionen unterstützt, finden Sie unter. So funktioniert Deadline Cloud mit IAM
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Zugriff auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- 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 Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Überprüfung der Einhaltung von Vorschriften für Deadline Cloud

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

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

- Compliance und Governance im Bereich Sicherheit – In diesen Anleitungen für die Lösungsimplementierung werden Überlegungen zur Architektur behandelt. Außerdem werden Schritte für die Bereitstellung von Sicherheits- und Compliance-Features beschrieben.
- Referenz für berechtigte HIPAA-Services – Listet berechtigte HIPAA-Services auf. Nicht alle AWS-Services sind HIPAA-fähig.
- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Die Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerelementreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.
- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Resilienz in Deadline Cloud

Die AWS globale Infrastruktur basiert auf Availability AWS-Regionen Zones. AWS-Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen 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 zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

AWS Deadline Cloud sichert keine Daten, die in Ihrem S3-Bucket für Jobanhänge gespeichert sind. Sie können Backups Ihrer Job-Anhangsdaten mit jedem standardmäßigen Amazon S3 S3-Backup-Mechanismus wie S3 Versioning oder AWS Backupaktivieren.

Sicherheit der Infrastruktur in Deadline Cloud

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

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Deadline Cloud 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.

Deadline Cloud unterstützt die Verwendung von AWS PrivateLink Virtual Private Cloud (VPC) - Endpunktrichtlinien nicht. Es verwendet die AWS PrivateLink Standardrichtlinie, die vollen Zugriff auf den Endpunkt gewährt. Weitere Informationen finden Sie im AWS PrivateLink Benutzerhandbuch unter Standard-Endpunktrichtlinie.

Konfiguration und Schwachstellenanalyse in Deadline Cloud

AWS kümmert sich um grundlegende Sicherheitsaufgaben wie das Patchen von Gastbetriebssystemen (OS) und Datenbanken, die Firewall-Konfiguration und die Notfallwiederherstellung. Diese Verfahren wurden von qualifizierten Dritten überprüft und zertifiziert. Weitere Informationen finden Sie in den folgenden Ressourcen:

- Modell der übergreifenden Verantwortlichkeit
- Amazon Web Services: Übersicht über Sicherheitsverfahren (Whitepaper)

AWS Deadline Cloud verwaltet Aufgaben auf vom Service oder vom Kunden verwalteten Flotten:

- Für vom Service verwaltete Flotten verwaltet Deadline Cloud das Gastbetriebssystem.
- Bei vom Kunden verwalteten Flotten sind Sie für die Verwaltung des Betriebssystems verantwortlich.

Weitere Informationen zur Konfiguration und Schwachstellenanalyse für AWS Deadline Cloud finden Sie unter

- Bewährte Sicherheitsmethoden für Deadline Cloud

Serviceübergreifende 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 ein dienstübergreifendes Identitätswechsels zum Problem des verwirrten Stellvertreters 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 des aws:SourceArn und aws:SourceAccountKontextschlüssel für globale Bedingungen in Ressourcenrichtlinien, um die Berechtigungen einzuschränken, AWS Deadline Cloud die der Ressource einen anderen Dienst gewähren. 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 effektivste Weg, um sich vor dem Verwirrter-Stellvertreter-Problem zu schützen, ist die Verwendung des `aws:SourceArn` globalen Bedingungskontextschlüssels mit dem vollständigen Amazon-Ressourcenname (ARN) der Ressource. Wenn Sie den vollständigen ARN der Ressource nicht kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den globalen Kontextbedingungsschlüssel `aws:SourceArn` mit Platzhalterzeichen (*) für die unbekannten Teile des ARN. Beispiel, `arn:aws:deadline:*:123456789012:*`.

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.

Das folgende Beispiel zeigt, wie Sie die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globalen Bedingungsschlüssel verwenden können, Deadline Cloud um das Problem des verwirrten Stellvertreters zu vermeiden.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "deadline.amazonaws.com"
    },
    "Action": "deadline:ActionName",
    "Resource": [
      "*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:deadline:*:123456789012:*"
      },
```

```
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

Zugriff AWS Deadline Cloud über einen Schnittstellenendpunkt (AWS PrivateLink)

Sie können verwenden AWS PrivateLink , um eine private Verbindung zwischen Ihrer VPC und AWS Deadline Cloud herzustellen. Sie können darauf zugreifen, Deadline Cloud als ob es in Ihrer VPC wäre, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder AWS Direct Connect eine Verbindung zu verwenden. Instances in Ihrer VPC benötigen für den Zugriff Deadline Cloud keine öffentlichen IP-Adressen.

Sie stellen diese private Verbindung her, indem Sie einen Schnittstellen-Endpunkt erstellen, der von AWS PrivateLink unterstützt wird. Wir erstellen eine Endpunkt-Netzwerkschnittstelle in jedem Subnetz, das Sie für den Schnittstellen-Endpunkt aktivieren. Hierbei handelt es sich um vom Anforderer verwaltete Netzwerkschnittstellen, die als Eingangspunkt für den Datenverkehr dienen, der für Deadline Cloud bestimmt ist.

Weitere Informationen finden Sie unter Zugriff auf AWS-Services über AWS PrivateLink im AWS PrivateLink -Leitfaden.

Überlegungen zu Deadline Cloud

Bevor Sie einen Schnittstellenendpunkt für einrichten Deadline Cloud, finden Sie weitere Informationen unter Zugreifen auf einen AWS-Service mithilfe eines Schnittstellen-VPC-Endpunkts im AWS PrivateLink Handbuch.

Deadline Cloud unterstützt Aufrufe aller API-Aktionen über den Schnittstellenendpunkt.

Standardmäßig Deadline Cloud ist der vollständige Zugriff auf über den Schnittstellenendpunkt zulässig. Alternativ können Sie den Endpunkt-Netzwerkschnittstellen eine Sicherheitsgruppe zuordnen, um den Datenverkehr Deadline Cloud über den Schnittstellenendpunkt zu kontrollieren.

Deadline Cloud unterstützt keine VPC-Endpunktrichtlinien. Weitere Informationen finden Sie im Handbuch unter Steuern des Zugriffs auf VPC-Endpunkte mithilfe von Endpunktrichtlinien.AWS PrivateLink

Deadline Cloud Endpunkte

Deadline Cloud verwendet zwei Endpunkte für den Zugriff auf den Dienst mithilfe von. AWS PrivateLink

Mitarbeiter verwenden den `com.amazonaws.region.deadline.scheduling` Endpunkt, um Aufgaben aus der Warteschlange abzurufen, ihnen den Fortschritt zu Deadline Cloud melden und die Aufgabenausgabe zurückzusenden. Wenn Sie eine vom Kunden verwaltete Flotte verwenden, ist der Terminplanungsendpunkt der einzige Endpunkt, den Sie erstellen müssen, es sei denn, Sie verwenden Verwaltungsoperationen. Wenn durch einen Auftrag beispielsweise mehr Jobs erstellt werden, müssen Sie den Verwaltungsendpunkt so einrichten, dass er den `CreateJob` Vorgang aufrufen kann.

Der Deadline Cloud Monitor verwendet den, `com.amazonaws.region.deadline.management` um die Ressourcen in Ihrer Farm zu verwalten, z. B. Warteschlangen und Flotten zu erstellen und zu ändern oder Listen mit Aufträgen, Schritten und Aufgaben abzurufen.

Deadline Cloud erfordert außerdem Endpunkte für die folgenden AWS Dienstendpunkte:

- Deadline Cloud verwendet AWS STS , um Mitarbeiter zu authentifizieren, sodass sie auf Arbeitsressourcen zugreifen können. Weitere Informationen zu AWS STS finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM im AWS Identity and Access Management Benutzerhandbuch.
- Wenn Sie Ihre vom Kunden verwaltete Flotte in einem Subnetz ohne Internetverbindung einrichten, müssen Sie einen VPC-Endpunkt für Amazon CloudWatch Logs einrichten, damit Mitarbeiter Protokolle schreiben können. Weitere Informationen finden Sie unter Überwachung mit. CloudWatch
- Wenn Sie Jobanhänge verwenden, müssen Sie einen VPC-Endpunkt für Amazon Simple Storage Service (Amazon S3) erstellen, damit Mitarbeiter auf die Anlagen zugreifen können. Weitere Informationen finden Sie unter Stellenanhänge in Deadline Cloud.

Erstellen Sie Endpunkte für Deadline Cloud

Sie können Schnittstellen-Endpunkte für die Deadline Cloud Verwendung entweder der Amazon VPC-Konsole oder der AWS Command Line Interface ()AWS CLI erstellen. Weitere Informationen finden Sie unter Erstellen eines Schnittstellenendpunkts im AWS PrivateLink -Leitfaden.

Erstellen Sie Verwaltungs- und Scheduling-Endpunkte für die Deadline Cloud Verwendung der folgenden Servicenamen. Ersetzen Sie es *region* durch den AWS-Region Ort, an dem Sie es bereitgestellt Deadline Cloud haben.

```
com.amazonaws.region.deadline.management
```

```
com.amazonaws.region.deadline.scheduling
```

Wenn Sie privates DNS für die Schnittstellenendpunkte aktivieren, können Sie API-Anfragen an die Deadline Cloud Verwendung des standardmäßigen regionalen DNS-Namens stellen. Zum Beispiel `worker.deadline.us-east-1.amazonaws.com` für Arbeitsoperationen oder `management.deadline.us-east-1.amazonaws.com` für alle anderen Operationen.

Sie müssen auch einen Endpunkt für die AWS STS Verwendung des folgenden Dienstnamens erstellen:

```
com.amazonaws.region.sts
```

Wenn sich Ihre vom Kunden verwaltete Flotte in einem Subnetz ohne Internetverbindung befindet, müssen Sie einen CloudWatch Logs-Endpunkt mit dem folgenden Dienstnamen erstellen:

```
com.amazonaws.region.logs
```

Wenn Sie Auftragsanhänge zum Übertragen von Dateien verwenden, müssen Sie einen Amazon S3 S3-Endpunkt mit dem folgenden Servicenamen erstellen:

```
com.amazonaws.region.s3
```

Bewährte Sicherheitsmethoden für Deadline Cloud

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

> **Note**
>
> Weitere Informationen zur Bedeutung vieler Sicherheitsthemen finden Sie im Modell der gemeinsamen Verantwortung.

Datenschutz

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

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie fortschrittliche verwaltete Sicherheitsdienste wie Amazon Macie, die Sie bei der Erkennung und Sicherung personenbezogener Daten unterstützen, die in Amazon Simple Storage Service (Amazon S3) gespeichert sind.
- Wenn Sie für den Zugriff auf AWS über eine Befehlszeilenschnittstelle oder über eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern wie z. B. im Feld Name keine sensiblen, identifizierenden Informationen wie Kontonummern von Kunden einzugeben. Dazu gehört auch, wenn Sie mit AWS Deadline Cloud oder anderen AWS-Services über die Konsole AWS CLI, API oder AWS SDKs arbeiten. Alle Daten, die Sie in Deadline Cloud oder andere Dienste eingeben, werden möglicherweise zur Aufnahme in Diagnoseprotokolle aufgenommen. 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.

AWS Identity and Access Management Berechtigungen

Verwalten Sie den Zugriff auf AWS Ressourcen mithilfe von Benutzern und AWS Identity and Access Management (IAM-) Rollen und indem Sie Benutzern die geringsten Rechte gewähren. Richten Sie Richtlinien und Verfahren zur Verwaltung von Anmeldeinformationen für die Erstellung, Verteilung, Rotation und den Widerruf AWS von Zugangsdaten ein. Weitere Informationen finden Sie unter Bewährte Methoden für IAM im IAM-Benutzerhandbuch.

Führen Sie Jobs als Benutzer und Gruppen aus

Bei der Verwendung der Warteschlangenfunktion in Deadline Cloud hat es sich bewährt, einen Betriebssystembenutzer (OS) und seine primäre Gruppe anzugeben, sodass der Betriebssystembenutzer über die geringsten Rechte für die Jobs der Warteschlange verfügt.

Wenn Sie die Option „Als Benutzer ausführen“ (und Gruppe) angeben, werden alle Prozesse für Jobs, die an die Warteschlange gesendet werden, mit diesem Betriebssystembenutzer ausgeführt und erben die zugehörigen Betriebssystemberechtigungen dieses Benutzers.

Die Kombination der Flotten- und Warteschlangenkonfigurationen sorgt für ein gewisses Maß an Sicherheit. Auf der Warteschlangenseite können die Rolle „Job wird als Benutzer ausgeführt“ und die IAM-Rolle angegeben werden, um das Betriebssystem und die AWS Berechtigungen für die Jobs der Warteschlange zu verwenden. Die Flotte definiert die Infrastruktur (Worker-Hosts, Netzwerke, bereitgestellter gemeinsam genutzter Speicher), über die Jobs innerhalb der Warteschlange ausgeführt werden, sofern sie einer bestimmten Warteschlange zugeordnet sind. Auf die auf den Worker-Hosts verfügbaren Daten müssen Jobs aus einer oder mehreren zugehörigen Warteschlangen zugreifen können. Die Angabe eines Benutzers oder einer Gruppe trägt dazu bei, die Daten in Jobs vor anderen Warteschlangen, anderer installierter Software oder anderen Benutzern mit Zugriff auf die Worker-Hosts zu schützen. Wenn es in einer Warteschlange keinen Benutzer gibt, wird sie als Agent-Benutzer ausgeführt, der sich als (`sudo`) beliebiger Warteschlangenbenutzer ausgeben kann. Auf diese Weise kann eine Warteschlange ohne Benutzer Rechte an eine andere Warteschlange weiterleiten.

Netzwerk

Um zu verhindern, dass der Datenverkehr abgefangen oder umgeleitet wird, müssen Sie unbedingt sicherstellen, wie und wohin Ihr Netzwerkverkehr geleitet wird.

Wir empfehlen Ihnen, Ihre Netzwerkumgebung auf folgende Weise zu sichern:

- Sichere Subnetz-Routing-Tabellen für Amazon Virtual Private Cloud (Amazon VPC), um zu kontrollieren, wie der Datenverkehr auf IP-Ebene weitergeleitet wird.
- Wenn Sie Amazon Route 53 (Route 53) als DNS-Anbieter in Ihrem Farm- oder Workstation-Setup verwenden, sichern Sie den Zugriff auf die Route 53-API.
- Wenn Sie eine Verbindung zu Deadline Cloud außerhalb herstellen, AWS z. B. über lokale Workstations oder andere Rechenzentren, sichern Sie jede lokale Netzwerkinfrastruktur. Dazu gehören DNS-Server und Routing-Tabellen auf Routern, Switches und anderen Netzwerkgeräten.

Jobs und Jobdaten

Deadline Cloud-Jobs werden innerhalb von Sitzungen auf Worker-Hosts ausgeführt. In jeder Sitzung werden ein oder mehrere Prozesse auf dem Worker-Host ausgeführt. Für die Ausgabe müssen Sie in der Regel Daten eingeben.

Um diese Daten zu sichern, können Sie Betriebssystembenutzer mit Warteschlangen konfigurieren. Der Worker-Agent verwendet den Warteschlangen-OS-Benutzer, um Sitzungsunterprozesse auszuführen. Diese Unterprozesse erben die Berechtigungen des Queue-OS-Benutzers.

Wir empfehlen, dass Sie sich an bewährte Methoden halten, um den Zugriff auf die Daten, auf die diese Unterprozesse zugreifen, zu sichern. Weitere Informationen finden Sie unter Modell der geteilten Verantwortung.

Struktur der Farm

Sie können Deadline Cloud-Flotten und Warteschlangen auf viele Arten anordnen. Bestimmte Vereinbarungen haben jedoch Auswirkungen auf die Sicherheit.

Eine Farm hat eine der sichersten Grenzen, da sie Deadline Cloud-Ressourcen nicht mit anderen Farmen teilen kann, einschließlich Flotten, Warteschlangen und Speicherprofilen. Sie können jedoch externe AWS Ressourcen innerhalb einer Farm gemeinsam nutzen, wodurch die Sicherheitsgrenze gefährdet wird.

Mit der entsprechenden Konfiguration können Sie auch Sicherheitsgrenzen zwischen Warteschlangen innerhalb derselben Farm einrichten.

Folgen Sie diesen bewährten Methoden, um sichere Warteschlangen in derselben Farm zu erstellen:

- Ordnen Sie eine Flotte nur Warteschlangen innerhalb derselben Sicherheitsgrenze zu. Beachten Sie Folgendes:

  - Nachdem der Job auf dem Worker-Host ausgeführt wurde, können Daten zurückbleiben, z. B. in einem temporären Verzeichnis oder im Home-Verzeichnis des Warteschlangenbenutzers.
  - Derselbe Betriebssystembenutzer führt alle Jobs auf einem firmeneigenen Fleet-Worker-Host aus, unabhängig davon, an welche Warteschlange Sie den Job senden.
  - Ein Job kann dazu führen, dass Prozesse auf einem Worker-Host ausgeführt werden, sodass Jobs aus anderen Warteschlangen andere laufende Prozesse beobachten können.
- Stellen Sie sicher, dass sich nur Warteschlangen innerhalb derselben Sicherheitsgrenze einen Amazon S3 S3-Bucket für Jobanhänge teilen.
- Stellen Sie sicher, dass nur Warteschlangen innerhalb derselben Sicherheitsgrenze denselben Betriebssystembenutzer verwenden.
- Sichern Sie alle anderen AWS Ressourcen, die in die Farm integriert sind, bis zur Grenze.

Warteschlangen für Arbeitsanhänge

Jobanhänge sind mit einer Warteschlange verknüpft, die Ihren Amazon S3 S3-Bucket verwendet.

- Auftragsanhänge schreiben in ein Root-Präfix im Amazon S3 S3-Bucket und lesen aus diesem. Sie geben dieses Root-Präfix im `CreateQueue` API-Aufruf an.
- Der Bucket hat ein entsprechendes`Queue Role`, das die Rolle spezifiziert, die Warteschlangenbenutzern Zugriff auf den Bucket und das Root-Präfix gewährt. Beim Erstellen einer Warteschlange geben Sie den `Queue Role` Amazon-Ressourcennamen (ARN) zusammen mit dem Bucket und dem Root-Präfix für Jobanhänge an.
- Autorisierte Aufrufe von `AssumeQueueRoleForReadAssumeQueueRoleForUser`, und `AssumeQueueRoleForWorker` API-Operationen geben einen Satz temporärer Sicherheitsanmeldedaten für die zurück`Queue Role`.

Wenn Sie eine Warteschlange erstellen und einen Amazon S3 S3-Bucket und ein Root-Präfix wiederverwenden, besteht die Gefahr, dass Informationen an Unbefugte weitergegeben werden. QueueA und QueueB verwenden beispielsweise denselben Bucket und dasselbe Root-Präfix. In einem sicheren Workflow hat ArtistA Zugriff auf QueueA, aber nicht auf QueueB. Wenn sich jedoch mehrere Warteschlangen einen Bucket teilen, kann ArtistA auf die Daten in QueueB-Daten zugreifen, da es denselben Bucket und dasselbe Root-Präfix wie QueueA verwendet.

Die Konsole richtet Warteschlangen ein, die standardmäßig sicher sind. Stellen Sie sicher, dass die Warteschlangen eine eindeutige Kombination aus Amazon S3 S3-Bucket und Root-Präfix haben, sofern sie nicht Teil einer gemeinsamen Sicherheitsgrenze sind.

Um Ihre Warteschlangen zu isolieren, müssen Sie das so konfigurieren, `Queue Role` dass nur der Warteschlangenzugriff auf den Bucket und das Root-Präfix zulässig ist. Ersetzen Sie im folgenden Beispiel jedes *`placeholder`* durch Ihre ressourcenspezifischen Informationen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::JOB_ATTACHMENTS_BUCKET_NAME",
        "arn:aws:s3:::JOB_ATTACHMENTS_BUCKET_NAME/JOB_ATTACHMENTS_ROOT_PREFIX/*"
      ],
      "Condition": {
        "StringEquals": { "aws:ResourceAccount": "ACCOUNT_ID" }
      }
    },
    {
      "Action": ["logs:GetLogEvents"],
      "Effect": "Allow",
      "Resource": "arn:aws:logs:REGION:ACCOUNT_ID:log-group:/aws/deadline/FARM_ID/*"
    }
  ]
}
```

Sie müssen außerdem eine Vertrauensrichtlinie für die Rolle festlegen. Ersetzen Sie im folgenden Beispiel den *`placeholder`* Text durch Ihre ressourcenspezifischen Informationen.

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

```
      "Action": ["sts:AssumeRole"],
      "Effect": "Allow",
      "Principal": { "Service": "deadline.amazonaws.com" },
      "Condition": {
        "StringEquals": { "aws:SourceAccount": "ACCOUNT_ID" },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:deadline:REGION:ACCOUNT_ID:farm/FARM_ID"
        }
      }
    },
    {
      "Action": ["sts:AssumeRole"],
      "Effect": "Allow",
      "Principal": { "Service": "credentials.deadline.amazonaws.com" },
      "Condition": {
        "StringEquals": { "aws:SourceAccount": "ACCOUNT_ID" },
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:deadline:REGION:ACCOUNT_ID:farm/FARM_ID"
        }
      }
    }
  ]
}
```

Amazon S3 S3-Buckets mit benutzerdefinierter Software

Sie können die folgende Anweisung zu Ihrem hinzufügen, `Queue Role` um auf benutzerdefinierte Software in Ihrem Amazon S3 S3-Bucket zuzugreifen. Im folgenden Beispiel ersetzen Sie es *SOFTWARE_BUCKET_NAME* durch den Namen Ihres S3-Buckets.

```
"Statement": [
    {
        "Action": [
            "s3:GetObject",
            "s3:ListBucket"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::SOFTWARE_BUCKET_NAME",
            "arn:aws:s3:::SOFTWARE_BUCKET_NAME/*"
        ]
    }
```

```
]
```

Weitere Informationen zu den bewährten Sicherheitsmethoden von Amazon S3 finden Sie unter Bewährte Sicherheitsmethoden für Amazon S3 im Amazon Simple Storage Service-Benutzerhandbuch.

Worker-Hosts

Schützen Sie Worker-Hosts, um sicherzustellen, dass jeder Benutzer nur Operationen für die ihm zugewiesene Rolle ausführen kann.

Wir empfehlen die folgenden bewährten Methoden zur Sicherung von Worker-Hosts:

- Verwenden Sie nicht denselben `jobRunAsUser` Wert für mehrere Warteschlangen, es sei denn, an diese Warteschlangen übermittelte Jobs liegen innerhalb derselben Sicherheitsgrenze.
- Stellen Sie die Warteschlange nicht `jobRunAsUser` auf den Namen des Betriebssystembenutzers ein, unter dem der Worker-Agent ausgeführt wird.
- Gewähren Sie Warteschlangenbenutzern die Betriebssystemberechtigungen mit den geringsten Rechten, die für die vorgesehenen Warteschlangenworkloads erforderlich sind. Stellen Sie sicher, dass sie keine Dateisystem-Schreibberechtigungen für Work-Agent-Programmdateien oder andere gemeinsam genutzte Software haben.
- Stellen Sie sicher, dass nur der Root-Benutzer aktiviert ist Linux und das `Administrator` eigene Konto auf Windows besitzt die Worker-Agent-Programmdateien und kann sie ändern.
- Ein Linux Worker-Hosts sollten erwägen, einen `umask` Override-Modus zu konfigurieren`/etc/sudoers`, der es dem Worker-Agent-Benutzer ermöglicht, Prozesse als Warteschlangenbenutzer zu starten. Diese Konfiguration trägt dazu bei, dass andere Benutzer nicht auf Dateien zugreifen können, die in die Warteschlange geschrieben wurden.
- Gewähren Sie vertrauenswürdigen Personen den Zugriff auf Worker-Hosts mit den geringsten Rechten.
- Beschränken Sie die Berechtigungen auf lokale DNS-Override-Konfigurationsdateien (ein) `/etc/hosts` Linux und `C:\Windows\system32\etc\hosts` weiter Windows) und um Tabellen auf Workstations und Worker-Host-Betriebssystemen weiterzuleiten.
- Beschränken Sie die Berechtigungen für die DNS-Konfiguration auf Workstations und Worker-Host-Betriebssystemen.

- Patchen Sie regelmäßig das Betriebssystem und die gesamte installierte Software. Dieser Ansatz umfasst Software, die speziell mit Deadline Cloud verwendet wird, wie z. B. Einreicher, Adapter, Worker Agents, OpenJD Pakete und andere.
- Verwenden Sie sichere Passwörter für Windows Warteschlange.`jobRunAsUser`
- Wechseln Sie regelmäßig die Passwörter für Ihre Warteschlange`jobRunAsUser`.
- Sorgen Sie für den Zugriff mit den geringsten Rechten Windows kennwortgeschützte Geheimnisse und löscht ungenutzte Geheimnisse.
- Erteilen Sie der Warteschlange nicht die `jobRunAsUser` Erlaubnis, die Befehle für den Zeitplan in der future auszuführen:
  - Ein Linux, verweigern Sie diesen Konten den Zugriff auf `cron` und`at`.
  - Ein Windows, verweigern Sie diesen Konten den Zugriff auf Windows Taskplaner.

> **Note**
>
> Weitere Informationen darüber, wie wichtig es ist, das Betriebssystem und die installierte Software regelmäßig zu patchen, finden Sie im Modell der gemeinsamen Verantwortung.

Workstations

Es ist wichtig, Workstations mit Zugriff auf Deadline Cloud zu sichern. Dieser Ansatz trägt dazu bei, dass mit Jobs, die Sie an Deadline Cloud einreichen, keine beliebigen Workloads ausgeführt werden können, die Ihnen in Rechnung gestellt werden. AWS-Konto

Wir empfehlen die folgenden bewährten Methoden zur Sicherung von Künstler-Workstations. Weitere Informationen finden Sie unter -Modell der geteilten Verantwortung.

- Sichern Sie alle dauerhaften Anmeldeinformationen, die Zugriff auf, einschließlich Deadline AWS Cloud, ermöglichen. Weitere Informationen finden Sie unter Verwalten der Zugriffsschlüssel für IAM-Benutzer im -IAM-Benutzerhandbuch.
- Installieren Sie nur vertrauenswürdige, sichere Software.
- Erfordern Sie, dass Benutzer sich mit einem Identitätsanbieter zusammenschließen, um AWS mit temporären Anmeldeinformationen zugreifen zu können.
- Verwenden Sie sichere Berechtigungen für Programmdateien von Deadline Cloud-Absendern, um Manipulationen zu verhindern.

- Gewähren Sie vertrauenswürdigen Personen den Zugriff auf die Workstations von Künstlern mit den geringsten Rechten.
- Verwenden Sie nur Einreicher und Adapter, die Sie über den Deadline Cloud Monitor erhalten.
- Beschränken Sie die Berechtigungen auf lokale DNS-Override-Konfigurationsdateien (ein) `/etc/hosts` Linux and macOS, und `C:\Windows\system32\etc\hosts` weiter Windows) und um Tabellen auf Workstations und Worker-Host-Betriebssystemen weiterzuleiten.
- Beschränken Sie die Berechtigungen `/etc/resolve.conf` auf Workstations und Worker-Host-Betriebssystemen.
- Patchen Sie regelmäßig das Betriebssystem und die gesamte installierte Software. Dieser Ansatz umfasst Software, die speziell mit Deadline Cloud verwendet wird, wie z. B. Einreicher, Adapter, Worker Agents, OpenJD Pakete und andere.

AWS Deadline Cloud überwachen

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung von AWS Deadline Cloud (Deadline Cloud) und Ihrer AWS Lösungen. Sammeln Sie Überwachungsdaten aus allen Teilen Ihrer AWS Lösung, damit Sie einen Fehler an mehreren Stellen leichter debuggen können, falls einer auftritt. Bevor Sie mit der Überwachung von Deadline Cloud beginnen, sollten Sie einen Überwachungsplan erstellen, der Antworten auf die folgenden Fragen enthält:

- Was sind Ihre Überwachungsziele?
- Welche Ressourcen möchten Sie überwachen?
- Wie oft werden diese Ressourcen überwacht?
- Welche Überwachungs-Tools möchten Sie verwenden?
- Wer soll die Überwachungsaufgaben ausführen?
- Wer soll benachrichtigt werden, wenn Fehler auftreten?

AWS und Deadline Cloud bieten Tools, mit denen Sie Ihre Ressourcen überwachen und auf potenzielle Vorfälle reagieren können. Einige dieser Tools übernehmen die Überwachung für Sie, andere Tools erfordern manuelles Eingreifen. Sie sollten die Überwachungsaufgaben so weit wie möglich automatisieren.

- Amazon CloudWatch überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Sie können Kennzahlen 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. Sie können beispielsweise die CPU-Auslastung oder andere Kennzahlen Ihrer EC2 Amazon-Instances CloudWatch verfolgen und bei Bedarf automatisch neue Instances starten. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

  Deadline Cloud hat drei CloudWatch Metriken.

- Mit Amazon CloudWatch Logs können Sie Ihre Protokolldateien von EC2 Amazon-Instances und anderen Quellen überwachen CloudTrail, 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-Benutzerhandbuch.

- Amazon EventBridge kann verwendet werden, um Ihre AWS Services zu automatisieren und automatisch auf Systemereignisse wie Probleme mit der Anwendungsverfügbarkeit oder Ressourcenänderungen zu reagieren. Ereignisse aus AWS Services werden nahezu EventBridge in Echtzeit zugestellt. Sie können einfache Regeln schreiben, um anzugeben, welche Ereignisse für Sie interessant sind und welche automatisierten Aktionen ausgeführt werden sollen, wenn ein Ereignis mit einer Regel übereinstimmt. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.
- AWS CloudTrailerfasst API-Aufrufe und zugehörige Ereignisse, die von oder im Namen Ihres AWS Kontos getätigt wurden, und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können feststellen, welche Benutzer und Konten angerufen wurden AWS, von welcher Quell-IP-Adresse aus die Anrufe getätigt wurden und wann die Aufrufe erfolgten. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch.

Weitere Informationen finden Sie in den folgenden Themen im Deadline Cloud Developer Guide:

- CloudTrail Protokolle
- Verwaltung von Ereignissen mit EventBridge
- Überwachen mit CloudWatch

Kontingente für Deadline Cloud

AWS Deadline Cloud stellt Ressourcen wie Farmen, Flotten und Warteschlangen bereit, die Sie zur Verarbeitung von Aufträgen verwenden können. Wenn Sie Ihre erstellen AWS-Konto, legen wir für jede Ressource Standardkontingente für diese Ressourcen fest. AWS-Region

Service Quotas ist ein zentraler Ort, an dem Sie Ihre Kontingente für anzeigen und verwalten können AWS-Services. Sie können auch eine Erhöhung des Kontingents für viele der von Ihnen genutzten Ressourcen beantragen.

Um die Kontingente für anzuzeigen Deadline Cloud, öffnen Sie die Konsole Service Quotas. Wählen Sie im Navigationsbereich AWS-Services und anschließend Deadline Cloud aus.

Informationen zur Erhöhung eines Kontingents finden Sie unter Anfordern einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch. Wenn das Kontingent noch nicht unter Servicekontingente verfügbar ist, verwenden Sie das Formular zur Erhöhung der Service Quotas.

AWS Deadline Cloud-Ressourcen erstellen mit AWS CloudFormation

AWS Deadline Cloud ist integriert AWS CloudFormation, ein Service, der Ihnen hilft, Ihre AWS Ressourcen zu modellieren und einzurichten, sodass Sie weniger Zeit mit der Erstellung und Verwaltung Ihrer Ressourcen und Infrastruktur verbringen müssen. Sie erstellen eine Vorlage, die alle benötigten AWS Ressourcen beschreibt (wie Farmen, Warteschlangen und Flotten) und diese Ressourcen für Sie AWS CloudFormation bereitstellt und konfiguriert.

Wenn Sie sie verwenden AWS CloudFormation, können Sie Ihre Vorlage wiederverwenden, um Ihre Deadline Cloud-Ressourcen konsistent und wiederholt einzurichten. Beschreiben Sie Ihre Ressourcen einmal und stellen Sie dann dieselben Ressourcen immer wieder in mehreren AWS-Konten Regionen bereit.

Deadline Cloud und AWS CloudFormation Vorlagen

Um Ressourcen für Deadline Cloud und verwandte Dienste bereitzustellen und zu konfigurieren, müssen Sie AWS CloudFormation Vorlagen verstehen. Vorlagen sind formatierte Textdateien in JSON oder YAML. Diese Vorlagen beschreiben die Ressourcen, die Sie in Ihren AWS CloudFormation Stacks bereitstellen möchten. Wenn Sie mit JSON oder YAML nicht vertraut sind, können Sie AWS CloudFormation Designer verwenden, um Ihnen die ersten Schritte mit Vorlagen zu erleichtern. AWS CloudFormation Weitere Informationen finden Sie unter Was ist AWS CloudFormation -Designer? im AWS CloudFormation -Benutzerhandbuch.

Deadline Cloud unterstützt das Erstellen von Farmen, Warteschlangen und Flotten in. AWS CloudFormationWeitere Informationen, einschließlich Beispielen für JSON- und YAML-Vorlagen für Farmen, Warteschlangen und Flotten, finden Sie in der AWS Deadline Cloud im Benutzerhandbuch.AWS CloudFormation

Erfahren Sie mehr über AWS CloudFormation

Weitere Informationen AWS CloudFormation dazu finden Sie in den folgenden Ressourcen:

- AWS CloudFormation
- AWS CloudFormation Benutzerhandbuch
- AWS CloudFormation API Reference

- AWS CloudFormation Benutzerhandbuch für die Befehlszeilenschnittstelle

Fehlerbehebung

Die folgenden Verfahren und Tipps können Ihnen bei der Behebung von Problemen mit Ihren AWS Deadline Cloud-Farmen und -Ressourcen helfen.

Themen

Warum kann ein Benutzer meine Farm, Flotte oder Warteschlange nicht sehen?

Benutzerzugriff

Wenn Ihre Benutzer Ihre Farmen, Flotten oder Warteschlangen nicht im Deadline Cloud-Monitor sehen, liegt möglicherweise ein Problem mit ihrem Zugriff auf Ihre Farm und Ressourcen vor.

Benutzer ohne Zugriff auf Farmen erhalten im Deadline Cloud-Monitor die Meldung „Keine Farmen verfügbar“.

Um zu überprüfen, ob Sie Ihrer Farm, Flotte oder Warteschlange den richtigen Benutzer oder die richtige Gruppe zugewiesen haben

1. Suchen Sie in der AWS Deadline Cloud-Konsole nach Ihrer Farm, Flotte oder Warteschlange und wählen Sie dann Zugriffsverwaltung aus.
2. Die Registerkarte Gruppen ist standardmäßig ausgewählt. Wenn Sie Berechtigungen nach Gruppen zuweisen, was empfohlen wird, sollte Ihre Gruppe in der Liste angezeigt werden und ihr eine Zugriffsebene zugewiesen sein.

   Wenn die Gruppe nicht in der Liste enthalten ist, wählen Sie Gruppe hinzufügen aus, um der Gruppe Berechtigungen zuzuweisen.
3. Wenn Sie Berechtigungen nach Benutzern zuweisen, wählen Sie die Registerkarte Benutzer aus. Ihr Benutzer sollte in der Liste angezeigt werden und ihm sollte eine Zugriffsebene zugewiesen sein.

Wenn Ihr Benutzer nicht in der Liste aufgeführt ist, wählen Sie Benutzer hinzufügen aus, um dem Benutzer eine Berechtigung zuzuweisen.

Um zu bestätigen, dass Sie den Benutzer Ihrer Gruppe zugewiesen haben

1. Suchen Sie in der AWS Deadline Cloud-Konsole nach Ihrer Farm, Flotte oder Warteschlange und wählen Sie dann Zugriffsverwaltung aus.
2. Die Registerkarte Gruppen ist standardmäßig ausgewählt. Wählen Sie den Gruppennamen aus, um die Mitglieder der Gruppe anzuzeigen.
3. Wenn der Benutzer nicht in der Gruppe aufgeführt ist, muss er hinzugefügt werden.

   Wenn Sie das standardmäßige Identitäts-Setup verwenden, können Sie den Benutzer in der Identity Center-Konsole direkt zur Gruppe hinzufügen. Wenn Sie mit einem externen Identitätsanbieter verbunden sind, wie Okta or Google Workspace, können Sie Ihren Benutzer der Gruppe in Ihrem Identitätsanbieter hinzufügen.

   > **Note**
   >
   > Einige externe Identitätsanbieter synchronisieren Benutzer, aber keine Gruppen mit Identity Center. In diesem Fall sollten Sie erwägen, einem Benutzer Berechtigungen direkt und nicht nach Gruppen zuzuweisen.

Weitere Informationen zur Verwaltung des Benutzerzugriffs auf Deadline Cloud finden Sie unterBenutzer in Deadline Cloud verwalten.

Warum nehmen Arbeitnehmer meine Jobs nicht an?

Konfiguration der Flottenrollen

Manchmal liegt es daran, dass die Flottenrolle nicht richtig konfiguriert wurde, wenn Mitarbeiter zwar erstellt werden, die Initialisierung aber nicht abschließen und nicht mit der Arbeit an Aufträgen beginnen.

Um zu überprüfen, ob dies der Fall ist, überprüfen Sie Ihre CloudTrail Protokolle auf Fehler, bei denen der Zugriff verweigert wurde. Nachdem Sie das Problem mit der Zugriffsverweigerung bestätigt

haben, wechseln Sie zu Ihrer Flotte und aktualisieren Sie die Rollenkonfiguration mit den richtigen Berechtigungen. Weitere Informationen finden Sie in den CloudTrailProtokollen im Deadline Cloud-Entwicklerhandbuch.

Fehlerbehebung bei Deadline Cloud-Jobs

Informationen zu häufigen Problemen mit Jobs in AWS Deadline Cloud finden Sie in den folgenden Themen.

Warum ist die Erstellung meines Jobs fehlgeschlagen?

Zu den möglichen Gründen, warum ein Job die Gültigkeitsprüfungen nicht bestehen kann, gehören die folgenden:

- Die Jobvorlage entspricht nicht der OpenJD-Spezifikation.
- Der Job enthält zu viele Schritte.
- Der Job enthält insgesamt zu viele Aufgaben.
- Es ist ein interner Dienstfehler aufgetreten, der die Erstellung des Jobs verhindert hat.

Um die Kontingente für die maximale Anzahl von Schritten und Aufgaben in einem Job zu sehen, verwenden Sie die Service-Kontingents-Konsole. Weitere Informationen finden Sie unter Kontingente für Deadline Cloud.

Warum ist mein Job nicht kompatibel?

Zu den häufigsten Gründen, warum Jobs nicht mit Warteschlangen kompatibel sind, gehören die folgenden:

- Der Warteschlange, an die der Job übermittelt wurde, sind keine Flotten zugeordnet. Öffnen Sie den Deadline Cloud-Monitor und überprüfen Sie, ob der Warteschlange Flotten zugeordnet sind. Weitere Informationen zum Anzeigen von Warteschlangen finden Sie unter. Warteschlangen- und Flottendetails in Deadline Cloud anzeigen
- Für den Job gelten Hostanforderungen, die von keiner der Flotten erfüllt werden, die der Warteschlange zugeordnet sind. Vergleichen Sie zur Überprüfung den `hostRequirements` Eintrag in der Auftragsvorlage mit der Konfiguration der Flotten in Ihrer Farm. Stellen Sie sicher, dass eine der Flotten die Hostanforderungen erfüllt. Weitere Informationen zur Flottenkompatibilität

finden Sie unter. Prüfen Sie die Flottenkompatibilität Informationen zur Flottenkonfiguration finden Sie unterWarteschlangen- und Flottendetails in Deadline Cloud anzeigen.

Warum ist mein Job immer noch fertig?

Zu den möglichen Gründen, warum Ihr Job im `READY` Bundesstaat festgefahren zu sein scheint, gehören die folgenden:

- Die maximale Anzahl von Mitarbeitern für Flotten, die der Warteschlange zugeordnet sind, ist auf Null gesetzt. Informationen zur Überprüfung finden Sie unterWarteschlangen- und Flottendetails in Deadline Cloud anzeigen.
- In der Warteschlange befindet sich ein Job mit höherer Priorität. Informationen zur Überprüfung finden Sie unterWarteschlangen- und Flottendetails in Deadline Cloud anzeigen.
- Überprüfen Sie für vom Kunden verwaltete Flotten die Auto Scaling-Konfiguration. Weitere Informationen finden Sie unter Erstellen einer Flotteninfrastruktur mit einer Amazon EC2 Auto Scaling Scaling-Gruppe im Deadline Cloud Developer Guide.

Warum ist mein Job gescheitert?

Ein Job kann aus vielen Gründen scheitern. Um nach dem Problem zu suchen, öffnen Sie den Deadline Cloud-Monitor und wählen Sie den fehlgeschlagenen Job aus. Wählen Sie eine Aufgabe aus, die fehlgeschlagen ist, und sehen Sie sich dann die Protokolle für die Aufgabe an. Detaillierte Anweisungen finden Sie unter Logs in Deadline Cloud anzeigen.

- Wenn Sie Lizenzfehler sehen oder ein Wasserzeichen angezeigt wird, das angezeigt wird, weil die Software nicht über eine gültige Lizenz verfügt, stellen Sie sicher, dass der Worker eine Verbindung zum erforderlichen Lizenzserver herstellen kann. Weitere Informationen finden Sie im Deadline Cloud Developer Guide unter Vom Kunden verwaltete Flotten mit einem Lizenzendpunkt Connect.
- Die Aktionsnachricht der letzten Sitzung oder der Code zum Beenden des Prozesses können Aufschluss darüber geben, warum Ihr Job fehlgeschlagen ist. Wenn Sie verwenden Windows und Ihr Exit-Code negativ ist, versuchen Sie, nach der unsignierten Version Ihres Exit-Codes zu suchen:

```
2,147,483,647 - |your exit code|
```

Warum steht mein Schritt noch aus?

Schritte können im `PENDING` Status verbleiben, wenn eine oder mehrere ihrer Abhängigkeiten nicht abgeschlossen sind. Sie können den Status der Abhängigkeiten mithilfe des Deadline Cloud-Monitors überprüfen. Detaillierte Anweisungen finden Sie unter Einen Schritt in Deadline Cloud anzeigen.

Weitere Ressourcen

Weitere Informationen und Ressourcen finden Sie unter GitHub.

Dokumentenverlauf für das Deadline Cloud-Benutzerhandbuch

In der folgenden Tabelle werden wichtige Änderungen in den einzelnen Versionen des AWS Deadline Cloud-Benutzerhandbuchs beschrieben.

Änderung	Beschreibung	Datum
Installationsprogramm für Adobe After Effects Submitter	Es wurden Anweisungen zum Hinzufügen des Installationsprogramms für Adobe After Effects Submitter zu Ihrer Software zur Erstellung digitaler Inhalte hinzugefügt. Weitere Informationen finden Sie unter Adobe After Effects.	13. Februar 2025
Fehlersuche	Es wurden Informationen zur Behebung von Problemen mit Deadline Cloud hinzugefügt. Weitere Informationen finden Sie unter Fehlerbehebung.	7. Februar 2025
Limits der Arbeitsressourcen	Es wurde eine Dokumentation für das neue Job-Ressourcenlimit und die maximale Anzahl von Worker-Hosts hinzugefügt. Weitere Informationen finden Sie unter Ressourcenlimits für Jobs erstellen.	30. Januar 2025
Adobe After Effects UBL	Es wurden Informationen zur nutzungsbasierten Lizenzierung (UBL) von Adobe After Effects für Deadline Cloud	30. Januar 2025

	hinzugefügt. Weitere Informationen finden Sie unter Connect zu einem Lizenzendpunkt herstellen.	
Der Inhalt des Benutzerhandbuchs wurde neu organisiert	Inhalte, die sich auf Entwickler konzentrieren, wurden aus dem Benutzerhandbuch in das Entwicklerhandbuch verschoben: • Die Anweisungen zum Erstellen einer kundenverwalteten Flotte wurden in ein neues Kapitel „Kundenverwaltete Flotten“ im Entwicklerhandbuch verschoben. • Informationen zur Verwendung eigener Lizenzen wurden in das neue Kapitel Verwenden von Softwarelizenzen im Entwicklerhandbuch verschoben. • Einzelheiten zur Überwachung mit CloudTrail CloudWatch, und wurden in EventBridge das Kapitel Überwachung im Entwicklerhandbuch verschoben.	6. Januar 2025
Ereignis zum Budgetschwellenwert	Neues EventBridge Ereignis für den Budgetschwellenwert hinzugefügt. Weitere Informationen finden Sie in der Detailreferenz zu Deadline Cloud-Ereignissen.	30. Oktober 2024

Ereignisse zum Jobstatus	Neue EventBridge Statusereignisse für Jobs und Aufgaben hinzugefügt. Weitere Informationen finden Sie in der Detailreferenz zu Deadline Cloud-Ereignissen.	24. Oktober 2024
Job erneut einreichen	Es wurden Informationen darüber hinzugefügt, wie ein Job erneut eingereicht werden kann. Weitere Informationen finden Sie unter Job erneut einreichen.	7. Oktober 2024
AWS Verwaltete Richtlinienaktualisierungen	Bestehende AWS verwaltete Richtlinien wurden aktualisiert. Weitere Informationen finden Sie unter AWS Verwaltete Richtlinien für Deadline Cloud.	7. Oktober 2024
Bringen Sie Ihre eigene Lizenz mit	Es wurden Informationen darüber hinzugefügt, wie Sie Ihren eigenen Lizenzserver oder Ihre eigene Lizenzproxyinstanz mit Deadline Cloud verwenden können. Weitere Informationen finden Sie unter Vom Service verwaltete Flotten.	26. Juli 2024

Autodesk 3ds Max UBL	Es wurden Informationen zur nutzungsbasierten Lizenzierung (UBL) für Autodesk 3ds Max für Deadline Cloud hinzugefügt. Weitere Informationen finden Sie unter Connect zu einem Lizenzendpunkt herstellen.	18. Juni 2024
Funktionen für Überwachung und Kostenmanagement	Sie können sie EventBridge zur Unterstützung der Überwachung in Deadline Cloud verwenden. Weitere Informationen finden Sie unter Auf EventBridge Ereignisse reagieren. Deadline Cloud bietet Budgets und den Usage Explorer, mit denen Sie die Kosten für Ihre Jobs kontrollieren und visualisieren können. Erfahren Sie mehr über einige bewährte Methoden zur Verwaltung dieser Kosten. Weitere Informationen finden Sie unter Kostenmanagement.	23. Mai 2024
Erstversion	Dies ist die erste Version des Deadline Cloud-Benutzerhandbuchs.	2. April 2024

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.