aws

Entwicklerhandbuch

Deadline Cloud

Deadline Cloud: Entwicklerhandbuch

Table of Contents

Was ist AWS Deadline Cloud?

AWS Deadline Cloud ist ein vollständig verwalteter AWS Service, mit dem Sie innerhalb von Minuten eine skalierbare Verarbeitungsfarm einrichten und in Betrieb nehmen können. Es bietet eine Verwaltungskonsole für die Verwaltung von Benutzern, Farmen, Warteschlangen für die Planung von Jobs und Flotten von Mitarbeitern, die die Verarbeitung durchführen.

Dieses Entwicklerhandbuch richtet sich an Entwickler von Pipelines, Tools und Anwendungen für eine Vielzahl von Anwendungsfällen, darunter die folgenden:

- Pipeline-Entwickler und technische Direktoren können Deadline Cloud APIs und ihre Funktionen in ihre individuellen Produktionspipelines integrieren.
- Unabhängige Softwareanbieter können Deadline Cloud in ihre Anwendungen integrieren, sodass Künstler und Benutzer, die digitale Inhalte erstellen, Renderaufträge von Deadline Cloud nahtlos von ihren Workstations aus einreichen können.
- Entwickler von Web- und Cloud-basierten Diensten können Deadline Cloud-Rendering in ihre Plattformen integrieren, sodass Kunden Ressourcen bereitstellen können, um Produkte virtuell anzusehen.

Wir bieten Tools, mit denen Sie direkt mit jedem Schritt Ihrer Pipeline arbeiten können:

- Eine Befehlszeilenschnittstelle, die Sie direkt oder über Skripts verwenden können.
- Das AWS SDK für 11 beliebte Programmiersprachen.
- Eine REST-basierte Weboberfläche, die Sie von Ihren Anwendungen aus aufrufen können.

Sie können auch andere AWS-Services in Ihren benutzerdefinierten Anwendungen verwenden. Sie können beispielsweise Folgendes verwenden:

- AWS CloudFormationum das Erstellen und Entfernen von Farmen, Warteschlangen und Flotten zu automatisieren.
- Amazon CloudWatch sammelt Kennzahlen für Jobs.
- Amazon Simple Storage Service zum Speichern und Verwalten digitaler Ressourcen und der Auftragsausgabe.
- AWS IAM Identity Centerum Benutzer und Gruppen für Ihre Farmen zu verwalten.

Stellenbeschreibung öffnen

Deadline Cloud verwendet die Open Job Description (OpenJD) -Spezifikation, um die Details eines Jobs zu spezifizieren. OpenJD wurde entwickelt, um Jobs zu definieren, die zwischen Lösungen portierbar sind. Sie verwenden es, um einen Job zu definieren, der aus einer Reihe von Befehlen besteht, die auf Worker-Hosts ausgeführt werden.

Sie können eine OpenJD-Jobvorlage mithilfe eines von Deadline Cloud bereitgestellten Absenders erstellen, oder Sie können ein beliebiges Tool verwenden, mit dem Sie die Vorlage erstellen möchten. Nachdem Sie die Vorlage erstellt haben, senden Sie sie an Deadline Cloud. Wenn Sie einen Submitter verwenden, kümmert sich dieser um den Versand der Vorlage. Wenn Sie die Vorlage auf andere Weise erstellt haben, rufen Sie eine Deadline Cloud-Befehlszeilenaktion auf, oder Sie können eine der Aktionen verwenden, AWS SDKs um den Job zu senden. In beiden Fällen fügt Deadline Cloud den Job der angegebenen Warteschlange hinzu und plant die Arbeit.

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.

Sitzung

Eine Sitzung ist eine kurzlebige Laufzeitumgebung auf einem Worker-Host, die erstellt wurde, um eine Reihe von Aufgaben aus demselben Job auszuführen. Die Sitzung endet, wenn der Worker-Host die Ausführung der Aufgaben für diesen Job beendet hat.

Die Sitzung bietet eine Möglichkeit, die Umgebung mit Ressourcen zu konfigurieren, die von mehreren Aufgabenausführungen gemeinsam genutzt werden, z. B. das Definieren von Umgebungsvariablen oder das Starten eines Hintergrundprozesses oder Containers.

Aktion der Sitzung

Eine Sitzungsaktion ist eine separate Arbeitseinheit, die von einem Mitarbeiter innerhalb einer Sitzung ausgeführt wird. Sie kann die wichtigsten Ausführungsvorgänge einer Aufgabe umfassen oder vorbereitende Schritte wie die Einrichtung der Umgebung und Prozesse nach der Ausführung wie Abbau und Säuberung umfassen.

Schritt

Ein Schritt ist ein bestimmter Prozess, der im Rahmen des Jobs ausgeführt werden muss.

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.

Was ist ein Deadline Cloud-Workload?

Mit AWS Deadline Cloud können Sie Jobs einreichen, um Ihre Anwendungen in der Cloud auszuführen und Daten für die Produktion von Inhalten oder Erkenntnissen zu verarbeiten, die für Ihr Unternehmen von entscheidender Bedeutung sind. Deadline Cloud verwendet Open Job Description (OpenJD) als Syntax für Jobvorlagen, eine Spezifikation, die auf die Bedürfnisse von Visual Compute-Pipelines zugeschnitten ist, aber auch auf viele andere Anwendungsfälle anwendbar ist. Einige Beispiele für Workloads umfassen Computergrafik-Rendering, Physiksimulation und Photogrammetrie.

Workloads reichen von einfachen Job-Bundles, die Benutzer entweder mit der CLI oder einer automatisch generierten GUI an eine Warteschlange senden, bis hin zu integrierten Submitter-Plug-ins, die dynamisch ein Job-Bundle für einen anwendungsdefinierten Workload generieren.

Wie Workloads bei der Produktion entstehen

Um Workloads in Produktionskontexten zu verstehen und zu verstehen, wie sie mit Deadline Cloud unterstützt werden können, sollten Sie sich überlegen, wie sie entstehen. Die Produktion kann die Erstellung von visuellen Effekten, Animationen, Spielen, Produktkatalogbildern, 3D-Rekonstruktionen für Building Information Modeling (BIM) und mehr beinhalten. Diese Inhalte werden in der Regel von einem Team von künstlerischen oder technischen Spezialisten erstellt, die eine Vielzahl von Softwareanwendungen und kundenspezifischen Skripten ausführen. Die Mitglieder des Teams tauschen Daten mithilfe einer Produktionspipeline untereinander aus. Viele Aufgaben, die von der Pipeline ausgeführt werden, erfordern intensive Berechnungen, die Tage dauern würden, wenn sie auf der Workstation eines Benutzers ausgeführt würden.

Einige Beispiele für Aufgaben in diesen Produktionspipelines sind:

- Verwendung einer Photogrammetrie-Anwendung zur Verarbeitung von Fotos, die von einem Filmset aufgenommen wurden, um ein strukturiertes digitales Netz zu rekonstruieren.
- Durchführung einer Partikelsimulation in einer 3D-Szene, um einem visuellen Explosionseffekt für eine Fernsehsendung Detailebenen hinzuzufügen.
- Daten für ein Spiellevel in die Form bringen, die für die externe Veröffentlichung erforderlich ist, und Anwenden der Optimierungs- und Komprimierungseinstellungen.
- Rendern einer Reihe von Bildern für einen Produktkatalog, einschließlich Variationen in Farbe, Hintergrund und Beleuchtung.

- Ein speziell entwickeltes Drehbuch auf einem 3D-Modell ausführen, um einen Look anzuwenden, der von einem Filmregisseur maßgeschneidert und genehmigt wurde.

Bei diesen Aufgaben müssen viele Parameter angepasst werden, um ein künstlerisches Ergebnis zu erzielen oder die Ausgabequalität zu optimieren. Oft gibt es eine grafische Benutzeroberfläche, mit der diese Parameterwerte über eine Schaltfläche oder ein Menü ausgewählt werden können, um den Prozess lokal in der Anwendung auszuführen. Wenn ein Benutzer den Prozess ausführt, können die Anwendung und möglicherweise der Host-Computer selbst nicht für andere Operationen verwendet werden, da er den Anwendungsstatus im Arbeitsspeicher verwendet und möglicherweise alle CPU- und Speicherressourcen des Host-Computers beansprucht.

In vielen Fällen ist der Vorgang schnell. Im Laufe der Produktion verlangsamt sich die Geschwindigkeit des Prozesses, wenn die Anforderungen an Qualität und Komplexität steigen. Aus einem Charaktertest, der während der Entwicklung 30 Sekunden gedauert hat, können leicht 3 Stunden werden, wenn er auf den endgültigen Produktionscharakter angewendet wird. Durch diesen Fortschritt kann ein Workload, der seinen Ursprung in einer GUI hatte, zu groß werden, um hineinzupassen. Die Portierung auf Deadline Cloud kann die Produktivität der Benutzer steigern, die diese Prozesse ausführen, da sie wieder die volle Kontrolle über ihre Workstation erhalten und weitere Iterationen vom Deadline Cloud-Monitor aus verfolgen können.

Bei der Entwicklung von Support für einen Workload in Deadline Cloud sollten zwei Unterstützungsebenen angestrebt werden:

- Verlagerung der Arbeitslast von der Benutzerarbeitsstation auf eine Deadline Cloud-Farm ohne Parallelität oder Beschleunigung. Dadurch werden die verfügbaren Rechenressourcen in der Farm möglicherweise nicht ausreichend genutzt, aber die Möglichkeit, lange Operationen auf ein Stapelverarbeitungssystem zu verlagern, ermöglicht es Benutzern, mehr mit ihrer eigenen Workstation zu erledigen.
- Optimierung der Parallelität der Arbeitslast, sodass die horizontale Skalierung der Deadline Cloud-Farm für eine schnelle Ausführung genutzt wird.

Manchmal ist es offensichtlich, wie ein Workload parallel ausgeführt werden kann. Beispielsweise kann jeder Frame eines Computergrafik-Renders unabhängig voneinander ausgeführt werden. Es ist jedoch wichtig, dass Sie sich nicht an dieser Parallelität festsetzen. Machen Sie sich stattdessen bewusst, dass die Auslagerung eines Workloads mit langer Laufzeit in Deadline Cloud erhebliche Vorteile bietet, auch wenn es keine offensichtliche Möglichkeit gibt, den Workload aufzuteilen.

Die Bestandteile eines Workloads

Um einen Deadline Cloud-Workload anzugeben, implementieren Sie ein Job-Bundle, das Benutzer mit der Deadline Cloud-CLI an eine Warteschlange senden. Ein Großteil der Arbeit bei der Erstellung eines Job-Bundles besteht darin, die Jobvorlage zu schreiben, aber es gibt noch mehr Faktoren wie die Bereitstellung der Anwendungen, die für den Workload erforderlich sind. Hier sind die wichtigsten Dinge, die Sie bei der Definition eines Workloads für Deadline Cloud beachten sollten:

- Die Anwendung, die ausgeführt werden soll. Der Job muss in der Lage sein, Anwendungsprozesse zu starten, und erfordert daher eine Installation der verfügbaren Anwendung sowie aller von der Anwendung verwendeten Lizenzen, z. B. den Zugriff auf einen Floating-Lizenzserver. Dies ist in der Regel Teil der Farmkonfiguration und nicht in das Auftragspaket selbst eingebettet.
  - Jobs mithilfe von Warteschlangenumgebungen konfigurieren
  - Vom Kunden verwaltete Flotten mit einem Lizenzendpunkt Connect
- Definitionen von Jobparametern. Die Benutzererfahrung beim Absenden des Jobs wird stark von den bereitgestellten Parametern beeinflusst. Zu den Beispielparametern gehören Datendateien, Verzeichnisse und die Anwendungskonfiguration.
  - Parameterwerte, Elemente für Job-Bundles
- Dateidatenfluss. Wenn ein Job ausgeführt wird, liest er Eingaben aus Dateien, die vom Benutzer bereitgestellt wurden, und schreibt seine Ausgabe dann als neue Dateien. Um mit den Funktionen für Auftragsanhänge und Pfadzuordnungen arbeiten zu können, muss der Job die Pfade der Verzeichnisse oder bestimmter Dateien für diese Eingaben und Ausgaben angeben.
  - Dateien in Ihren Jobs verwenden
- Das Schrittskript. Das Schrittskript führt die Anwendungsbinärdatei mit den richtigen Befehlszeilenoptionen aus, um die angegebenen Jobparameter anzuwenden. Es verarbeitet auch Details wie die Pfadzuweisung, wenn die Workload-Datendateien absolute statt relative Pfadverweise enthalten.
  - Jobvorlagenelemente für Jobpakete

Portabilität von Workloads

Ein Workload ist portabel, wenn er auf mehreren verschiedenen Systemen ausgeführt werden kann, ohne dass er jedes Mal geändert wird, wenn Sie einen Job einreichen. Er kann beispielsweise auf verschiedenen Renderfarmen ausgeführt werden, auf denen unterschiedliche gemeinsam genutzte Dateisysteme installiert sind, oder auf verschiedenen Betriebssystemen wie Linux or Windows.

Wenn Sie ein portables Auftragspaket implementieren, ist es für Benutzer einfacher, den Job in ihrer spezifischen Farm auszuführen oder ihn für andere Anwendungsfälle anzupassen.

Im Folgenden finden Sie einige Möglichkeiten, wie Sie Ihr Job-Bundle portabel machen können.

- Geben Sie mithilfe von Job-Parametern und Asset-Referenzen im `PATH` Job-Bundle die für einen Workload benötigten Eingabedatendateien vollständig an. Dadurch kann der Job auf Farmen übertragen werden, die auf gemeinsam genutzten Dateisystemen basieren, und auf Farmen, die Kopien der Eingabedaten erstellen, wie z. B. die Deadline Cloud-Funktion für Jobanhänge.
- Machen Sie Dateipfadverweise für die Eingabedateien des Jobs verschiebbar und auf verschiedenen Betriebssystemen nutzbar. Zum Beispiel, wenn Benutzer Jobs einreichen von Windows Arbeitsstationen zum Ausführen auf einem Linux Flotte.
  - Verwenden Sie relative Dateipfadverweise. Wenn also das Verzeichnis, das sie enthält, an einen anderen Ort verschoben wird, werden Verweise trotzdem aufgelöst. Einige Anwendungen, wie Blender, unterstützen die Wahl zwischen relativen und absoluten Pfaden.
  - Wenn Sie keine relativen Pfade verwenden können, unterstützen Sie OpenJD-Pfad-Mapping-Metadaten und übersetzen Sie die absoluten Pfade entsprechend der Art und Weise, wie Deadline Cloud die Dateien für den Job bereitstellt.
- Implementieren Sie Befehle in einem Job mithilfe portabler Skripts. Python und Bash sind zwei Beispiele für Skriptsprachen, die auf diese Weise verwendet werden können. Sie sollten erwägen, beide auf allen Worker-Hosts Ihrer Flotten bereitzustellen.
  - Verwenden Sie die Binärdatei des Skriptinterpreters, wie `python` oder`bash`, mit dem Namen der Skriptdatei als Argument. Dies funktioniert auf allen Betriebssystemen, einschließlich Windows, verglichen mit der Verwendung einer Skriptdatei, bei der das Ausführungsbit aktiviert ist Linux.
  - Schreiben Sie portable Bash-Skripte, indem Sie die folgenden Methoden anwenden:
    - Erweitern Sie die Pfadparameter der Vorlage in einfache Anführungszeichen, um Pfade mit Leerzeichen zu behandeln und Windows Pfadtrennzeichen.
    - Beim Laufen auf Windows, achten Sie auf Probleme im Zusammenhang mit der automatischen Pfadübersetzung von MinGW. Es wandelt zum Beispiel einen AWS CLI Befehl wie `aws logs tail /aws/deadline/...` in einen Befehl um, der einem Protokoll ähnlich ist `aws logs tail "C:/Program Files/Git/aws/deadline/..."` und nicht korrekt weiterleitet. Stellen Sie die Variable `MSYS_NO_PATHCONV=1` ein, um dieses Verhalten auszuschalten.
    - In den meisten Fällen funktioniert derselbe Code auf allen Betriebssystemen. Wenn der Code anders sein muss, verwenden Sie ein `if/else` Konstrukt, um die Fälle zu behandeln.

      ```
      if [[ "$(uname)" == MINGW* || "$(uname -s)" == MSYS_NT* ]]; then
      ```

```
    # Code for Windows
elif [[ "$(uname)" == Darwin ]]; then
    # Code for MacOS
else
    # Code for Linux and other operating systems
fi
```

  - Sie können portable Python-Skripte schreiben, `pathlib` um Pfadunterschiede im Dateisystem zu behandeln und betriebsspezifische Funktionen zu vermeiden. Die Python-Dokumentation enthält Anmerkungen dazu, beispielsweise in der Dokumentation zur Signalbibliothek. LinuxDie Unterstützung spezifischer Funktionen ist als „Verfügbarkeit: Linux“ gekennzeichnet.
- Verwenden Sie die Jobparameter, um die Anwendungsanforderungen zu spezifizieren. Verwenden Sie konsistente Konventionen, die der Farmadministrator in Warteschlangenumgebungen anwenden kann.
  - Sie können beispielsweise die `RezPackages` Parameter `CondaPackages` und/oder in Ihrem Job mit einem Standardparameterwert verwenden, der die Namen und Versionen der Anwendungspakete auflistet, die der Job benötigt. Anschließend können Sie eine der Beispiel-Warteschlangenumgebungen Conda oder Rez verwenden, um eine virtuelle Umgebung für den Job bereitzustellen.

Erste Schritte mit Deadline Cloud-Ressourcen

Um mit der Erstellung benutzerdefinierter Lösungen für AWS Deadline Cloud zu beginnen, müssen Sie Ihre Ressourcen einrichten. Dazu gehören eine Farm, mindestens eine Warteschlange für die Farm und mindestens eine Arbeiterflotte zur Bedienung der Warteschlange. Sie können Ihre Ressourcen mit der Deadline Cloud-Konsole erstellen, oder Sie können die verwenden AWS Command Line Interface.

In diesem Tutorial werden Sie verwenden, AWS CloudShell um eine einfache Entwicklerfarm zu erstellen und den Worker-Agent auszuführen. Anschließend können Sie einen einfachen Job mit Parametern und Anhängen einreichen und ausführen, eine vom Service verwaltete Flotte hinzufügen und Ihre Farmressourcen bereinigen, wenn Sie fertig sind.

In den folgenden Abschnitten lernen Sie die verschiedenen Funktionen von Deadline Cloud kennen und erfahren, wie sie funktionieren und zusammenarbeiten. Das Befolgen dieser Schritte ist nützlich, um neue Workloads und Anpassungen zu entwickeln und zu testen.

Anweisungen zum Einrichten Ihrer Farm mithilfe der Konsole finden Sie unter Erste Schritte im Deadline Cloud-Benutzerhandbuch.

Themen

Erstellen Sie eine Deadline Cloud-Farm

Verwenden Sie die AWS Command Line Interface (AWS CLI), wie im folgenden Verfahren gezeigt, um Ihre Entwicklerfarm und Warteschlangenressourcen in AWS Deadline Cloud zu erstellen. Außerdem erstellen Sie eine AWS Identity and Access Management (IAM) -Rolle und eine vom Kunden verwaltete Flotte (CMF) und ordnen die Flotte Ihrer Warteschlange zu. Anschließend können Sie das konfigurieren AWS CLI und sicherstellen, dass Ihre Farm wie angegeben eingerichtet ist und funktioniert.

Sie können diese Farm verwenden, um die Funktionen von Deadline Cloud zu erkunden und anschließend neue Workloads, Anpassungen und Pipeline-Integrationen zu entwickeln und zu testen.

Um eine Farm zu erstellen

1. Öffnen Sie eine AWS CloudShell Sitzung. Sie verwenden das CloudShell Fenster, um Befehle AWS Command Line Interface (AWS CLI) einzugeben, um die Beispiele in diesem Tutorial auszuführen. Lassen Sie das CloudShell Fenster geöffnet, während Sie fortfahren.
2. Erstellen Sie einen Namen für Ihre Farm und fügen Sie diesen Farmnamen hinzu`~/.bashrc`. Dadurch wird es für andere Terminalsitzungen verfügbar.

```
echo "DEV_FARM_NAME=DeveloperFarm" >> ~/.bashrc
source ~/.bashrc
```

3. Erstellen Sie die Farmressource und fügen Sie ihre Farm-ID hinzu`~/.bashrc`.

```
aws deadline create-farm \
    --display-name "$DEV_FARM_NAME"

echo "DEV_FARM_ID=\$(aws deadline list-farms \
        --query \"farms[?displayName=='\$DEV_FARM_NAME'].farmId \
        | [0]\" --output text)" >> ~/.bashrc
source ~/.bashrc
```

4. Erstellen Sie die Warteschlangenressource und fügen Sie ihre Warteschlangen-ID hinzu `~/.bashrc`.

```
aws deadline create-queue \
    --farm-id $DEV_FARM_ID \
    --display-name "$DEV_FARM_NAME Queue" \
    --job-run-as-user '{"posix": {"user": "job-user", "group": "job-group"},
 "runAs":"QUEUE_CONFIGURED_USER"}'

echo "DEV_QUEUE_ID=\$(aws deadline list-queues \
        --farm-id \$DEV_FARM_ID \
        --query \"queues[?displayName=='\$DEV_FARM_NAME Queue'].queueId \
        | [0]\" --output text)" >> ~/.bashrc
source ~/.bashrc
```

5. Erstellen Sie eine IAM-Rolle für die Flotte. Diese Rolle bietet Worker-Hosts in Ihrer Flotte die erforderlichen Sicherheitsanmeldedaten, um Jobs aus Ihrer Warteschlange auszuführen.

```
aws iam create-role \
    --role-name "${DEV_FARM_NAME}FleetRole" \
    --assume-role-policy-document \
        '{
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "credentials.deadline.amazonaws.com"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }'
aws iam put-role-policy \
    --role-name "${DEV_FARM_NAME}FleetRole" \
    --policy-name WorkerPermissions \
    --policy-document \
        '{
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Action": [
                        "deadline:AssumeFleetRoleForWorker",
                        "deadline:UpdateWorker",
                        "deadline:DeleteWorker",
                        "deadline:UpdateWorkerSchedule",
                        "deadline:BatchGetJobEntity",
                        "deadline:AssumeQueueRoleForWorker"
                    ],
                    "Resource": "*",
                    "Condition": {
                        "StringEquals": {
                            "aws:PrincipalAccount": "${aws:ResourceAccount}"
                        }
                    }
                },
                {
                    "Effect": "Allow",
                    "Action": [
                        "logs:CreateLogStream"
```

```
                ],
                "Resource": "arn:aws:logs:*:*:*:/aws/deadline/*",
                "Condition": {
                    "StringEquals": {
                        "aws:PrincipalAccount": "${aws:ResourceAccount}"
                    }
                }
            },
            {
                "Effect": "Allow",
                "Action": [
                    "logs:PutLogEvents",
                    "logs:GetLogEvents"
                ],
                "Resource": "arn:aws:logs:*:*:*:/aws/deadline/*",
                "Condition": {
                    "StringEquals": {
                        "aws:PrincipalAccount": "${aws:ResourceAccount}"
                    }
                }
            }
        ]
    }'
```

6. Erstellen Sie die vom Kunden verwaltete Flotte (CMF) und fügen Sie deren Flotten-ID hinzu. `~/.bashrc`

```
FLEET_ROLE_ARN="arn:aws:iam::$(aws sts get-caller-identity \
        --query "Account" --output text):role/${DEV_FARM_NAME}FleetRole"
aws deadline create-fleet \
    --farm-id $DEV_FARM_ID \
    --display-name "$DEV_FARM_NAME CMF" \
    --role-arn $FLEET_ROLE_ARN \
    --max-worker-count 5 \
    --configuration \
        '{
            "customerManaged": {
                "mode": "NO_SCALING",
                "workerCapabilities": {
                    "vCpuCount": {"min": 1},
                    "memoryMiB": {"min": 512},
                    "osFamily": "linux",
                    "cpuArchitectureType": "x86_64"
```

```
                }
            }
        }'

echo "DEV_CMF_ID=\$(aws deadline list-fleets \
        --farm-id \$DEV_FARM_ID \
        --query \"fleets[?displayName=='\$DEV_FARM_NAME CMF'].fleetId \
        | [0]\" --output text)" >> ~/.bashrc
source ~/.bashrc
```

7. Ordnen Sie das CMF Ihrer Warteschlange zu.

```
aws deadline create-queue-fleet-association \
    --farm-id $DEV_FARM_ID \
    --queue-id $DEV_QUEUE_ID \
    --fleet-id $DEV_CMF_ID
```

8. Installieren Sie die Deadline Cloud-Befehlszeilenschnittstelle.

```
pip install deadline
```

9. Verwenden Sie den folgenden Befehl, um die Standardfarm auf die Farm-ID und die Warteschlange auf die Warteschlangen-ID festzulegen, die Sie zuvor erstellt haben.

```
deadline config set defaults.farm_id $DEV_FARM_ID
deadline config set defaults.queue_id $DEV_QUEUE_ID
```

10. (Optional) Verwenden Sie die folgenden Befehle, um zu überprüfen, ob Ihre Farm gemäß Ihren Spezifikationen eingerichtet wurde:

    - Alle Farmen auflisten — **`deadline farm list`**
    - Alle Warteschlangen in der Standardfarm auflisten — **`deadline queue list`**
    - Alle Flotten in der Standardfarm auflisten — **`deadline fleet list`**
    - Holen Sie sich die Standardfarm — **`deadline farm get`**
    - Holen Sie sich die Standardwarteschlange — **`deadline queue get`**
    - Ruft alle Flotten ab, die der Standardwarteschlange zugeordnet sind — **`deadline fleet get`**

Nächste Schritte

Nachdem Sie Ihre Farm erstellt haben, können Sie den Deadline Cloud-Worker-Agent auf den Hosts in Ihrer Flotte ausführen, um Jobs zu verarbeiten. Siehe Führen Sie den Deadline Cloud Worker Agent aus.

Führen Sie den Deadline Cloud Worker Agent aus

Bevor Sie die Jobs, die Sie an die Warteschlange auf Ihrer Entwicklerfarm einreichen, ausführen können, müssen Sie den AWS Deadline Cloud-Worker-Agent im Entwicklermodus auf einem Worker-Host ausführen.

Im weiteren Verlauf dieses Tutorials führen Sie mithilfe von zwei AWS CloudShell Tabs AWS CLI Operationen auf Ihrer Entwicklerfarm durch. Auf der ersten Registerkarte können Sie Jobs einreichen. Auf der zweiten Registerkarte können Sie den Worker Agent ausführen.

> **Note**
>
> Wenn Sie Ihre CloudShell Sitzung länger als 20 Minuten inaktiv lassen, kommt es zu einem Timeout und der Worker-Agent wird gestoppt. Folgen Sie den Anweisungen im folgenden Verfahren, um den Worker-Agent neu zu starten.

Bevor Sie einen Worker Agent starten können, müssen Sie eine Deadline Cloud-Farm, eine Warteschlange und eine Flotte einrichten. Siehe Erstellen Sie eine Deadline Cloud-Farm.

Um den Worker Agent im Entwicklermodus auszuführen

1. Wenn Ihre Farm immer noch auf der ersten CloudShell Registerkarte geöffnet ist, öffnen Sie eine zweite CloudShell Registerkarte und erstellen Sie dann die `demoenv-persist` Verzeichnisse `demoenv-logs` und.

   ```
   mkdir ~/demoenv-logs
   mkdir ~/demoenv-persist
   ```

2. Laden Sie die Deadline Cloud Worker Agent-Pakete von PyPI herunter und installieren Sie sie:

> **Note**
>
> Ein Windows, es ist erforderlich, dass die Agentendateien im globalen Site-Packages-Verzeichnis von Python installiert werden. Virtuelle Python-Umgebungen werden derzeit nicht unterstützt.

```
python -m pip install deadline-cloud-worker-agent
```

3. Damit der Worker-Agent die temporären Verzeichnisse für die Ausführung von Jobs erstellen kann, erstellen Sie ein Verzeichnis:

```
sudo mkdir /sessions
sudo chmod 750 /sessions
sudo chown cloudshell-user /sessions
```

4. Führen Sie den Deadline Cloud-Worker-Agent im Entwicklermodus mit den Variablen `DEV_FARM_ID` aus`DEV_CMF_ID`, die Sie dem hinzugefügt haben`~/.bashrc`.

```
deadline-worker-agent \
    --farm-id $DEV_FARM_ID \
    --fleet-id $DEV_CMF_ID \
    --run-jobs-as-agent-user \
    --logs-dir ~/demoenv-logs \
    --persistence-dir ~/demoenv-persist
```

Während der Worker-Agent den `UpdateWorkerSchedule` API-Vorgang initialisiert und dann abfragt, wird die folgende Ausgabe angezeigt:

```
INFO    Worker Agent starting
[2024-03-27 15:51:01,292][INFO    ] # Worker Agent starting
[2024-03-27 15:51:01,292][INFO    ] AgentInfo
Python Interpreter: /usr/bin/python3
Python Version: 3.9.16 (main, Sep  8 2023, 00:00:00)  - [GCC 11.4.1 20230605 (Red
 Hat 11.4.1-2)]
Platform: linux
...
```

```
[2024-03-27 15:51:02,528][INFO    ] # API.Resp # [deadline:UpdateWorkerSchedule]
(200) params={'assignedSessions': {}, 'cancelSessionActions': {},
 'updateIntervalSeconds': 15} ...
[2024-03-27 15:51:17,635][INFO    ] # API.Resp # [deadline:UpdateWorkerSchedule]
(200) params=(Duplicate removed, see previous response) ...
[2024-03-27 15:51:32,756][INFO    ] # API.Resp # [deadline:UpdateWorkerSchedule]
(200) params=(Duplicate removed, see previous response) ...
...
```

5. Wählen Sie Ihre erste CloudShell Registerkarte aus und listen Sie dann die Mitarbeiter in der Flotte auf.

   ```
   deadline worker list --fleet-id $DEV_CMF_ID
   ```

   Es wird eine Ausgabe wie die folgende angezeigt:

   ```
   Displaying 1 of 1 workers starting at 0

   - workerId: worker-8c9af877c8734e89914047111f
     status: STARTED
     createdAt: 2023-12-13 20:43:06+00:00
   ```

In einer Produktionskonfiguration erfordert der Deadline Cloud-Worker-Agent die Einrichtung mehrerer Benutzer und Konfigurationsverzeichnisse als Administratorbenutzer auf dem Host-Computer. Sie können diese Einstellungen überschreiben, da Sie Jobs in Ihrer eigenen Entwicklungsfarm ausführen, auf die nur Sie zugreifen können.

Nächste Schritte

Jetzt, da ein Worker-Agent auf Ihren Worker-Hosts ausgeführt wird, können Sie Jobs an Ihre Mitarbeiter senden. Sie haben folgende Möglichkeiten:

- Mit Deadline Cloud einreichenmit einem einfachen OpenJD-Jobpaket.
- Jobs mit Stellenanhängen in Deadline Cloud einreichendie Dateien zwischen Workstations teilen, die unterschiedliche Betriebssysteme verwenden.

Mit Deadline Cloud einreichen

Um Deadline Cloud-Jobs auf Ihren Worker-Hosts auszuführen, erstellen und verwenden Sie ein Open Job Description (OpenJD) -Jobpaket, um einen Job zu konfigurieren. Das Bundle konfiguriert den Job, indem es beispielsweise Eingabedateien für einen Job angibt und wo die Ausgabe des Jobs geschrieben werden soll. Dieses Thema enthält Beispiele dafür, wie Sie ein Job-Bundle konfigurieren können.

Bevor Sie die Verfahren in diesem Abschnitt ausführen können, müssen Sie die folgenden Schritte ausführen:

- Erstellen Sie eine Deadline Cloud-Farm
- Führen Sie den Deadline Cloud Worker Agent aus

Gehen Sie wie folgt vor, um AWS Deadline Cloud zum Ausführen von Jobs zu verwenden. Verwenden Sie die erste AWS CloudShell Registerkarte, um Jobs an Ihre Entwicklerfarm zu senden. Verwenden Sie die zweite CloudShell Registerkarte, um die Ergebnisse des Worker-Agents anzuzeigen.

Themen

Reichen Sie das ein simple_job Probe

Nachdem Sie eine Farm erstellt und den Worker-Agent ausgeführt haben, können Sie Folgendes einreichen simple_job Beispiel an Deadline Cloud.

Um das einzureichen simple_job Beispiel an Deadline Cloud

1. Wählen Sie Ihren ersten CloudShell Tab.
2. Laden Sie das Beispiel von herunter GitHub.

```
cd ~
```

```
git clone https://github.com/aws-deadline/deadline-cloud-samples.git
```

3. Navigieren Sie zum Verzeichnis mit den Beispielen für das Job-Bundle.

```
cd ~/deadline-cloud-samples/job_bundles/
```

4. Reichen Sie den simple_job Probe.

```
deadline bundle submit simple_job
```

5. Wählen Sie Ihre zweite CloudShell Registerkarte, um die Protokollausgabe zum Aufrufen`BatchGetJobEntities`, Aufrufen einer Sitzung und Ausführen einer Sitzungsaktion anzuzeigen.

```
...
[2024-03-27 16:00:21,846][INFO    ] # Session.Starting
 # [session-053d77cef82648fe2] Starting new Session.
 [queue-3ba4ff683ff54db09b851a2ed8327d7b/job-d34cc98a6e234b6f82577940ab4f76c6]
[2024-03-27 16:00:21,853][INFO    ] # API.Req # [deadline:BatchGetJobEntity]
 resource={'farm-id': 'farm-3e24cfc9bbcd423e9c1b6754bc1',
 'fleet-id': 'fleet-246ee60f46d44559b6cce010d05', 'worker-id':
 'worker-75e0fce9c3c344a69bff57fcd83'} params={'identifiers': [{'jobDetails':
 {'jobId': 'job-d34cc98a6e234b6f82577940ab4'}}]} request_url=https://
scheduling.deadline.us-west-2.amazonaws.com/2023-10-12/farms/
farm-3e24cfc9bbcd423e /fleets/fleet-246ee60f46d44559b1 /workers/worker-
 75e0fce9c3c344a69b /batchGetJobEntity
[2024-03-27 16:00:22,013][INFO    ] # API.Resp # [deadline:BatchGetJobEntity](200)
 params={'entities': [{'jobDetails': {'jobId': 'job-d34cc98a6e234b6f82577940ab6',
 'jobRunAsUser': {'posix': {'user': 'job-user', 'group': 'job-group'},
 'runAs': 'QUEUE_CONFIGURED_USER'}, 'logGroupName': '/aws/deadline/
farm-3e24cfc9bbcd423e9c1b6754bc1/queue-3ba4ff683ff54db09b851a2ed83', 'parameters':
 '*REDACTED*', 'schemaVersion': 'jobtemplate-2023-09'}}], 'errors': []}
 request_id=a3f55914-6470-439e-89e5-313f0c6
[2024-03-27 16:00:22,013][INFO    ] # Session.Add #
 [session-053d77cef82648fea9c69827182] Appended new SessionActions.
 (ActionIds: ['sessionaction-053d77cef82648fea9c69827182-0'])
 [queue-3ba4ff683ff54db09b851a2ed8b/job-d34cc98a6e234b6f82577940ab6]
[2024-03-27 16:00:22,014][WARNING ] # Session.User #
 [session-053d77cef82648fea9c69827182] Running as the Worker Agent's
 user. (User: cloudshell-user) [queue-3ba4ff683ff54db09b851a2ed8b/job-
d34cc98a6e234b6f82577940ac6]
```

```
[2024-03-27 16:00:22,015][WARNING ] # Session.AWSCreds #
 [session-053d77cef82648fea9c69827182] AWS Credentials are not available: Queue has
 no IAM Role. [queue-3ba4ff683ff54db09b851a2ed8b/job-d34cc98a6e234b6f82577940ab6]
[2024-03-27 16:00:22,026][INFO    ] # Session.Logs #
 [session-053d77cef82648fea9c69827182] Logs streamed to: AWS CloudWatch
 Logs. (LogDestination: /aws/deadline/farm-3e24cfc9bbcd423e9c1b6754bc1/
queue-3ba4ff683ff54db09b851a2ed83/session-053d77cef82648fea9c69827181)
 [queue-3ba4ff683ff54db09b851a2ed83/job-d34cc98a6e234b6f82577940ab4]
[2024-03-27 16:00:22,026][INFO    ] # Session.Logs #
 [session-053d77cef82648fea9c69827182] Logs streamed to: local
 file. (LogDestination: /home/cloudshell-user/demoenv-logs/
queue-3ba4ff683ff54db09b851a2ed8b/session-053d77cef82648fea9c69827182.log)
 [queue-3ba4ff683ff54db09b851a2ed83/job-d34cc98a6e234b6f82577940ab4]
...
```

> **Note**
>
> Es werden nur die Protokollausgaben des Worker-Agenten angezeigt. Es gibt ein separates Protokoll für die Sitzung, in der der Job ausgeführt wird.

6. Wählen Sie Ihre erste Registerkarte und überprüfen Sie dann die Protokolldateien, die der Worker-Agent schreibt.

   a. Navigieren Sie zum Protokollverzeichnis des Worker-Agents und sehen Sie sich dessen Inhalt an.

   ```
   cd ~/demoenv-logs
   ls
   ```

   b. Drucken Sie die erste Protokolldatei, die der Worker-Agent erstellt.

   ```
   cat worker-agent-bootstrap.log
   ```

   Diese Datei enthält die Ergebnisse des Worker-Agents darüber, wie er die Deadline Cloud-API aufgerufen hat, um eine Worker-Ressource in Ihrer Flotte zu erstellen, und dann die Flottenrolle übernommen hat.

   c. Druckt die Protokolldatei aus, die ausgegeben wird, wenn der Worker Agent der Flotte beitritt.

```
cat worker-agent.log
```

Dieses Protokoll enthält Ausgaben über alle Aktionen, die der Worker-Agent ausführt, enthält jedoch keine Ausgaben über die Warteschlangen, in denen er Jobs ausführt, mit Ausnahme IDs der Ressourcen.

d. Druckt die Protokolldateien für jede Sitzung in einem Verzeichnis, das den gleichen Namen wie die Ressourcen-ID der Warteschlange hat.

```
cat $DEV_QUEUE_ID/session-*.log
```

Wenn der Auftrag erfolgreich ist, sieht die Ausgabe der Protokolldatei wie folgt aus:

```
cat $DEV_QUEUE_ID/$(ls -t $DEV_QUEUE_ID | head -1)

2024-03-27 16:00:22,026 WARNING Session running with no AWS Credentials.
2024-03-27 16:00:22,404 INFO
2024-03-27 16:00:22,405 INFO ==============================================
2024-03-27 16:00:22,405 INFO --------- Running Task
2024-03-27 16:00:22,405 INFO ==============================================
2024-03-27 16:00:22,406 INFO ----------------------------------------------
2024-03-27 16:00:22,406 INFO Phase: Setup
2024-03-27 16:00:22,406 INFO ----------------------------------------------
2024-03-27 16:00:22,406 INFO Writing embedded files for Task to disk.
2024-03-27 16:00:22,406 INFO Mapping: Task.File.runScript -> /sessions/
session-053d77cef82648fea9c698271812a/embedded_fileswa_gj55_/tmp2u9yqtsz
2024-03-27 16:00:22,406 INFO Wrote: runScript -> /sessions/
session-053d77cef82648fea9c698271812a/embedded_fileswa_gj55_/tmp2u9yqtsz
2024-03-27 16:00:22,407 INFO ----------------------------------------------
2024-03-27 16:00:22,407 INFO Phase: Running action
2024-03-27 16:00:22,407 INFO ----------------------------------------------
2024-03-27 16:00:22,407 INFO Running command /sessions/
session-053d77cef82648fea9c698271812a/tmpzuzxpslm.sh
2024-03-27 16:00:22,414 INFO Command started as pid: 471
2024-03-27 16:00:22,415 INFO Output:
2024-03-27 16:00:22,420 INFO Welcome to AWS Deadline Cloud!
2024-03-27 16:00:22,571 INFO
2024-03-27 16:00:22,572 INFO ==============================================
2024-03-27 16:00:22,572 INFO --------- Session Cleanup
2024-03-27 16:00:22,572 INFO ==============================================
```

```
2024-03-27 16:00:22,572 INFO Deleting working directory: /sessions/
session-053d77cef82648fea9c698271812a
```

7. Druckt Informationen über den Job.

```
deadline job get
```

Wenn Sie den Job weiterleiten, speichert das System ihn als Standard, sodass Sie die Job-ID nicht eingeben müssen.

Reichen Sie eine ein simple_job mit einem Parameter

Sie können Jobs mit Parametern einreichen. Im folgenden Verfahren bearbeiten Sie simple_job Vorlage, um eine benutzerdefinierte Nachricht einzufügen, senden Sie die simple_job, drucken Sie dann die Sitzungsprotokolldatei aus, um die Nachricht anzuzeigen.

Um das einzureichen simple_job Beispiel mit einem Parameter

1. Wählen Sie Ihre erste CloudShell Registerkarte aus und navigieren Sie dann zum Verzeichnis mit den Job-Bundle-Beispielen.

```
cd ~/deadline-cloud-samples/job_bundles/
```

2. Drucken Sie den Inhalt des simple_job Schablone.

```
cat simple_job/template.yaml
```

Der `parameterDefinitions` Abschnitt mit dem `Message` Parameter sollte wie folgt aussehen:

```
parameterDefinitions:
- name: Message
  type: STRING
  default: Welcome to AWS Deadline Cloud!
```

3. Reichen Sie das ein simple_job Beispiel mit einem Parameterwert und warten Sie dann, bis die Ausführung des Jobs abgeschlossen ist.

```
deadline bundle submit simple_job \
    -p "Message=Greetings from the developer getting started guide."
```

4. Um die benutzerdefinierte Nachricht zu sehen, sehen Sie sich die letzte Sitzungsprotokolldatei an.

```
cd ~/demoenv-logs
cat $DEV_QUEUE_ID/$(ls -t $DEV_QUEUE_ID | head -1)
```

Erstellen Sie ein simple_file_job-Job-Bundle mit Datei-I/O

Ein Renderjob muss die Szenendefinition lesen, daraus ein Bild rendern und dieses Bild dann in einer Ausgabedatei speichern. Sie können diese Aktion simulieren, indem Sie den Job den Hash der Eingabe berechnen lassen, anstatt ein Bild zu rendern.

Um ein simple_file_job-Job-Paket mit Datei-I/O zu erstellen

1. Wählen Sie Ihre erste CloudShell Registerkarte aus und navigieren Sie dann zum Verzeichnis mit den Job-Bundle-Beispielen.

```
cd ~/deadline-cloud-samples/job_bundles/
```

2. Erstellen Sie eine Kopie von `simple_job` mit dem neuen Namen`simple_file_job`.

```
cp -r simple_job simple_file_job
```

3. Bearbeiten Sie die Jobvorlage wie folgt:

> **Note**
>
> Wir empfehlen Ihnen, Folgendes zu verwenden nano für diese Schritte. Wenn Sie lieber verwenden Vim, müssen Sie den Einfügemodus mit einstellen`:set paste`.

   a. Öffnen Sie die Vorlage in einem Texteditor.

```
nano simple_file_job/template.yaml
```

   b. Fügen Sie die folgenden `type`, `objectType`, und hinzu `dataFlow`, `parameterDefinitions`.

```
- name: InFile
```

```
  type: PATH
  objectType: FILE
  dataFlow: IN
- name: OutFile
  type: PATH
  objectType: FILE
  dataFlow: OUT
```

c. Fügen Sie den folgenden `bash` Skriptbefehl am Ende der Datei hinzu, die aus der Eingabedatei liest und in die Ausgabedatei schreibt.

```
        # hash the input file, and write that to the output
        sha256sum "{{Param.InFile}}" > "{{Param.OutFile}}"
```

Die aktualisierte `template.yaml` Version sollte genau dem Folgenden entsprechen:

```
specificationVersion: 'jobtemplate-2023-09'
name: Simple File Job Bundle Example
parameterDefinitions:
- name: Message
  type: STRING
  default: Welcome to AWS Deadline Cloud!
- name: InFile
  type: PATH
  objectType: FILE
  dataFlow: IN
- name: OutFile
  type: PATH
  objectType: FILE
  dataFlow: OUT
steps:
- name: WelcomeToDeadlineCloud
  script:
    actions:
      onRun:
        command: '{{Task.File.Run}}'
    embeddedFiles:
    - name: Run
      type: TEXT
      runnable: true
      data: |
        #!/usr/bin/env bash
        echo "{{Param.Message}}"
```

```
        # hash the input file, and write that to the output
        sha256sum "{{Param.InFile}}" > "{{Param.OutFile}}"
```

> **Note**
>
> Wenn Sie den Abstand in der anpassen möchten, stellen Sie sicher`template.yaml`, dass Sie Leerzeichen anstelle von Einzügen verwenden.

d. Speichern Sie die Datei und beenden Sie den Texteditor.

4. Geben Sie Parameterwerte für die Eingabe- und Ausgabedateien an, um den simple_file_job zu senden.

```
deadline bundle submit simple_file_job \
    -p "InFile=simple_job/template.yaml" \
    -p "OutFile=hash.txt"
```

5. Druckt Informationen über den Job.

```
deadline job get
```

- Sie werden eine Ausgabe wie die folgende sehen:

```
parameters:
  Message:
    string: Welcome to AWS Deadline Cloud!
  InFile:
    path: /local/home/cloudshell-user/BundleFiles/JobBundle-Examples/simple_job/
template.yaml
  OutFile:
    path: /local/home/cloudshell-user/BundleFiles/JobBundle-Examples/hash.txt
```

- Sie haben zwar nur relative Pfade angegeben, für die Parameter ist jedoch der vollständige Pfadsatz festgelegt. Der AWS CLI verknüpft das aktuelle Arbeitsverzeichnis mit allen Pfaden, die als Parameter bereitgestellt werden, wenn die Pfade den folgenden Typ habenPATH.
- Der Worker-Agent, der im anderen Terminalfenster ausgeführt wird, nimmt den Job auf und führt ihn aus. Diese Aktion erstellt die `hash.txt` Datei, die Sie mit dem folgenden Befehl anzeigen können.

```
cat hash.txt
```

Dieser Befehl druckt eine Ausgabe, die der folgenden ähnelt.

```
eaa2df5d34b54be5ac34c56a24a8c237b8487231a607eaf530a04d76b89c9cd3 /local/home/
cloudshell-user/BundleFiles/JobBundle-Examples/simple_job/template.yaml
```

Nächste Schritte

Nachdem Sie gelernt haben, wie Sie einfache Jobs mit der Deadline Cloud CLI einreichen, können Sie Folgendes erkunden:

- Jobs mit Stellenanhängen in Deadline Cloud einreichenum zu erfahren, wie man Jobs auf Hosts mit unterschiedlichen Betriebssystemen ausführt.
- Fügen Sie Ihrer Entwicklerfarm in Deadline Cloud eine vom Service verwaltete Flotte hinzuum Ihre Jobs auf Hosts auszuführen, die von Deadline Cloud verwaltet werden.
- Bereinigen Sie Ihre Farmressourcen in Deadline Cloudum die Ressourcen herunterzufahren, die Sie für dieses Tutorial verwendet haben.

Jobs mit Stellenanhängen in Deadline Cloud einreichen

Viele Farmen verwenden gemeinsam genutzte Dateisysteme, um Dateien zwischen den Hosts, die Jobs einreichen, und denen, die Jobs ausführen, gemeinsam zu nutzen. Im vorherigen Beispiel wird das lokale Dateisystem `simple_file_job` beispielsweise von den AWS CloudShell Terminalfenstern gemeinsam genutzt, die auf Registerkarte eins, wo Sie den Job einreichen, und Registerkarte zwei, wo Sie den Worker-Agent ausführen, ausgeführt werden.

Ein gemeinsam genutztes Dateisystem ist vorteilhaft, wenn sich die Worker-Hosts und die Worker-Hosts im selben lokalen Netzwerk befinden. Wenn Sie Ihre Daten vor Ort in der Nähe der Workstations speichern, die darauf zugreifen, bedeutet die Verwendung einer cloudbasierten Farm, dass Sie Ihre Dateisysteme über ein VPN mit hoher Latenz gemeinsam nutzen oder Ihre Dateisysteme in der Cloud synchronisieren müssen. Keine dieser Optionen ist einfach einzurichten oder zu bedienen.

AWS Deadline Cloud bietet eine einfache Lösung mit Job-Anhängen, die E-Mail-Anhängen ähneln. Mit Job-Anhängen hängen Sie Daten an Ihren Job an. Anschließend kümmert sich Deadline Cloud

um die Details der Übertragung und Speicherung Ihrer Auftragsdaten in Amazon Simple Storage Service (Amazon S3) -Buckets.

Workflows zur Erstellung von Inhalten sind oft iterativ, was bedeutet, dass ein Benutzer Jobs mit einer kleinen Teilmenge modifizierter Dateien einreicht. Da Amazon S3 S3-Buckets Auftragsanhänge in einem inhaltsadressierbaren Speicher speichern, basiert der Name jedes Objekts auf dem Hash der Objektdaten, und der Inhalt eines Verzeichnisbaums wird in einem Manifest-Dateiformat gespeichert, das an einen Auftrag angehängt ist.

Bevor Sie die Verfahren in diesem Abschnitt ausführen können, müssen Sie die folgenden Schritte ausführen:

- Erstellen Sie eine Deadline Cloud-Farm
- Führen Sie den Deadline Cloud Worker Agent aus

Gehen Sie wie folgt vor, um Jobs mit Auftragsanhängen auszuführen.

Themen

Fügen Sie Ihrer Warteschlange eine Konfiguration für Jobanhänge hinzu

Um Jobanhänge in Ihrer Warteschlange zu aktivieren, fügen Sie der Warteschlangenressource in Ihrem Konto eine Konfiguration für Jobanhänge hinzu.

Um Ihrer Warteschlange eine Konfiguration für Jobanhänge hinzuzufügen

1. Wählen Sie Ihre erste CloudShell Registerkarte und geben Sie dann einen der folgenden Befehle ein, um einen Amazon S3 S3-Bucket für Jobanhänge zu verwenden.
   - Wenn Sie noch keinen privaten Amazon S3 S3-Bucket haben, können Sie einen neuen S3-Bucket erstellen und verwenden.

```
DEV_FARM_BUCKET=$(echo $DEV_FARM_NAME \
    | tr '[:upper:]' '[:lower:]')-$(xxd -l 16 -p /dev/urandom)
```

```
if [ "$AWS_REGION" == "us-east-1" ]; then LOCATION_CONSTRAINT=
else LOCATION_CONSTRAINT="--create-bucket-configuration \
    LocationConstraint=${AWS_REGION}"
fi
aws s3api create-bucket \
    $LOCATION_CONSTRAINT \
    --acl private \
    --bucket ${DEV_FARM_BUCKET}
```

- Wenn Sie bereits einen privaten Amazon S3 S3-Bucket haben, können Sie ihn verwenden, indem Sie ihn *MY_BUCKET_NAME* durch den Namen Ihres Buckets ersetzen.

```
DEV_FARM_BUCKET=MY_BUCKET_NAME
```

2. Nachdem Sie Ihren Amazon S3 S3-Bucket erstellt oder ausgewählt haben, fügen Sie den Bucket-Namen hinzu, `~/.bashrc` um den Bucket für andere Terminalsitzungen verfügbar zu machen.

```
echo "DEV_FARM_BUCKET=$DEV_FARM_BUCKET" >> ~/.bashrc
 source ~/.bashrc
```

3. Erstellen Sie eine AWS Identity and Access Management (IAM-) Rolle für die Warteschlange.

```
aws iam create-role --role-name "${DEV_FARM_NAME}QueueRole" \
    --assume-role-policy-document \
        '{
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "credentials.deadline.amazonaws.com"
                    },
                    "Action": "sts:AssumeRole"
                }
            ]
        }'
aws iam put-role-policy \
    --role-name "${DEV_FARM_NAME}QueueRole" \
    --policy-name S3BucketsAccess \
    --policy-document \
            '{
                "Version": "2012-10-17",
```

```
                "Statement": [
                {
                    "Action": [
                        "s3:GetObject*",
                        "s3:GetBucket*",
                        "s3:List*",
                        "s3:DeleteObject*",
                        "s3:PutObject",
                        "s3:PutObjectLegalHold",
                        "s3:PutObjectRetention",
                        "s3:PutObjectTagging",
                        "s3:PutObjectVersionTagging",
                        "s3:Abort*"
                    ],
                    "Resource": [
                        "arn:aws:s3:::'$DEV_FARM_BUCKET'",
                        "arn:aws:s3:::'$DEV_FARM_BUCKET'/*"
                    ],
                    "Effect": "Allow"
                }
            ]
            }'
```

4. Aktualisieren Sie Ihre Warteschlange so, dass sie die Einstellungen für Jobanhänge und die IAM-Rolle enthält.

```
QUEUE_ROLE_ARN="arn:aws:iam::$(aws sts get-caller-identity \
        --query "Account" --output text):role/${DEV_FARM_NAME}QueueRole"
aws deadline update-queue \
    --farm-id $DEV_FARM_ID \
    --queue-id $DEV_QUEUE_ID \
    --role-arn $QUEUE_ROLE_ARN \
    --job-attachment-settings \
        '{
            "s3BucketName": "'$DEV_FARM_BUCKET'",
            "rootPrefix": "JobAttachments"
        }'
```

5. Vergewissern Sie sich, dass Sie Ihre Warteschlange aktualisiert haben.

```
deadline queue get
```

Es wird eine Ausgabe wie die folgende angezeigt:

```
...
jobAttachmentSettings:
  s3BucketName: DEV_FARM_BUCKET
  rootPrefix: JobAttachments
roleArn: arn:aws:iam::ACCOUNT_NUMBER:role/DeveloperFarmQueueRole
...
```

Einreichen simple_file_job mit Stellenanhängen

Wenn Sie Job-Anhänge verwenden, müssen Job-Bundles Deadline Cloud genügend Informationen liefern, um den Datenfluss des Jobs zu bestimmen, z. B. anhand von PATH Parametern. Im Fall der simple_file_job, Sie haben die `template.yaml` Datei bearbeitet, um Deadline Cloud mitzuteilen, dass sich der Datenfluss in der Eingabedatei und der Ausgabedatei befindet.

Nachdem Sie die Konfiguration für Jobanhänge zu Ihrer Warteschlange hinzugefügt haben, können Sie das simple_file_job-Beispiel mit Stellenanhängen einreichen. Nachdem Sie dies getan haben, können Sie sich die Protokollierung und die Jobausgabe ansehen, um zu überprüfen, ob simple_file_job mit Job-Anhängen funktioniert.

Um das simple_file_job-Job-Paket mit Job-Anhängen einzureichen

1. Wählen Sie Ihre erste CloudShell Registerkarte und öffnen Sie dann das Verzeichnis. `JobBundle-Samples`
2.
```
cd ~/deadline-cloud-samples/job_bundles/
```
3. Reichen Sie simple_file_job in die Warteschlange ein. Wenn Sie aufgefordert werden, den Upload zu bestätigen, geben Sie ein. **y**

```
deadline bundle submit simple_file_job \
    -p InFile=simple_job/template.yaml \
    -p OutFile=hash-jobattachments.txt
```
4. Führen Sie den folgenden Befehl aus, um die Ausgabe des Sitzungsprotokolls der Jobanhänge zur Datenübertragung anzuzeigen.

```
JOB_ID=$(deadline config get defaults.job_id)
SESSION_ID=$(aws deadline list-sessions \
        --farm-id $DEV_FARM_ID \
```

```
        --queue-id $DEV_QUEUE_ID \
        --job-id $JOB_ID \
        --query "sessions[0].sessionId" \
        --output text)
cat ~/demoenv-logs/$DEV_QUEUE_ID/$SESSION_ID.log
```

5. Listet die Sitzungsaktionen auf, die innerhalb der Sitzung ausgeführt wurden.

```
aws deadline list-session-actions \
    --farm-id $DEV_FARM_ID \
    --queue-id $DEV_QUEUE_ID \
    --job-id $JOB_ID \
    --session-id $SESSION_ID
```

Es wird eine Ausgabe wie die folgende angezeigt:

```
{
    "sessionactions": [
        {
            "sessionActionId": "sessionaction-123-0",
            "status": "SUCCEEDED",
            "startedAt": "<timestamp>",
            "endedAt": "<timestamp>",
            "progressPercent": 100.0,
            "definition": {
                "syncInputJobAttachments": {}
            }
        },
        {
            "sessionActionId": "sessionaction-123-1",
            "status": "SUCCEEDED",
            "startedAt": "<timestamp>",
            "endedAt": "<timestamp>",
            "progressPercent": 100.0,
            "definition": {
                "taskRun": {
                    "taskId": "task-abc-0",
                    "stepId": "step-def"
                }
            }
        }
    ]
```

```
}
```

Bei der ersten Sitzungsaktion wurden die Eingabeauftragsanhänge heruntergeladen, während die zweite Aktion die Aufgabe wie in den vorherigen Schritten ausführt und dann die Anlagen für den Ausgabeauftrag hochgeladen hat.

6. Listet das Ausgabeverzeichnis auf.

```
ls *.txt
```

Die Ausgabe `hash.txt` ist beispielsweise im Verzeichnis vorhanden, aber `hash-jobattachments.txt` nicht vorhanden, da die Ausgabedatei des Jobs noch nicht heruntergeladen wurde.

7. Laden Sie die Ausgabe des letzten Jobs herunter.

```
deadline job download-output
```

8. Sehen Sie sich die Ausgabe der heruntergeladenen Datei an.

```
cat hash-jobattachments.txt
```

Es wird eine Ausgabe wie die folgende angezeigt:

```
eaa2df5d34b54be5ac34c56a24a8c237b8487231a607eaf530a04d76b89c9cd3  /tmp/openjd/
session-123/assetroot-abc/simple_job/template.yaml
```

Verstehen, wie Jobanhänge in Amazon S3 gespeichert werden

Sie können die AWS Command Line Interface (AWS CLI) verwenden, um Daten für Jobanhänge hoch- oder herunterzuladen, die in Amazon S3 S3-Buckets gespeichert sind. Wenn Sie wissen, wie Deadline Cloud Jobanhänge auf Amazon S3 speichert, hilft Ihnen das bei der Entwicklung von Workloads und Pipeline-Integrationen.

Um zu überprüfen, wie Deadline Cloud-Jobanhänge in Amazon S3 gespeichert werden

1. Wählen Sie Ihren ersten CloudShell Tab und öffnen Sie dann das Verzeichnis mit den Job-Bundle-Beispielen.

```
cd ~/deadline-cloud-samples/job_bundles/
```

2. Untersuchen Sie die Jobeigenschaften.

```
deadline job get
```

Es wird eine Ausgabe wie die folgende angezeigt:

```
parameters:
  Message:
    string: Welcome to AWS Deadline Cloud!
  InFile:
    path: /home/cloudshell-user/deadline-cloud-samples/job_bundles/simple_job/
template.yaml
  OutFile:
    path: /home/cloudshell-user/deadline-cloud-samples/job_bundles/hash-
jobattachments.txt
attachments:
  manifests:
  - rootPath: /home/cloudshell-user/deadline-cloud-samples/job_bundles/
    rootPathFormat: posix
    outputRelativeDirectories:
    - .
    inputManifestPath: farm-3040c59a5b9943d58052c29d907a645d/queue-
cde9977c9f4d4018a1d85f3e6c1a4e6e/Inputs/
f46af01ca8904cd8b514586671c79303/0d69cd94523ba617c731f29c019d16e8_input.xxh128
    inputManifestHash: f95ef91b5dab1fc1341b75637fe987ee
  fileSystem: COPIED
```

Das Feld „Anlagen“ enthält eine Liste von Manifeststrukturen, die Eingabe- und Ausgabedatenpfade beschreiben, die der Job bei seiner Ausführung verwendet. Sehen Sie `rootPath` sich den lokalen Verzeichnispfad auf dem Computer an, der den Job eingereicht hat. Um das Amazon S3 S3-Objektsuffix zu sehen, das eine Manifestdatei enthält, lesen Sie den`inputManifestFile`. Die Manifestdatei enthält Metadaten für einen Verzeichnisstruktur-Snapshot der Eingabedaten des Jobs.

3. Drucken Sie das Amazon S3 S3-Manifest-Objekt hübsch aus, um die Eingabeverzeichnisstruktur für den Job zu sehen.

```
MANIFEST_SUFFIX=$(aws deadline get-job \
```

```
    --farm-id $DEV_FARM_ID \
    --queue-id $DEV_QUEUE_ID \
    --job-id $JOB_ID \
    --query "attachments.manifests[0].inputManifestPath" \
    --output text)
aws s3 cp s3://$DEV_FARM_BUCKET/JobAttachments/Manifests/$MANIFEST_SUFFIX - | jq .
```

Es wird eine Ausgabe wie die folgende angezeigt:

```
{
    "hashAlg": "xxh128",
    "manifestVersion": "2023-03-03",
    "paths": [
    {
        "hash": "2ec297b04c59c4741ed97ac8fb83080c",
        "mtime": 1698186190000000,
        "path": "simple_job/template.yaml",
        "size": 445
    }
    ],
    "totalSize": 445
}
```

4. Konstruieren Sie das Amazon S3 S3-Präfix, das die Manifeste für die Anlagen des Ausgabeauftrags enthält, und listen Sie das Objekt darunter auf.

```
SESSION_ACTION=$(aws deadline list-session-actions \
    --farm-id $DEV_FARM_ID \
    --queue-id $DEV_QUEUE_ID \
    --job-id $JOB_ID \
    --session-id $SESSION_ID \
    --query "sessionActions[?definition.taskRun != null] | [0]")
STEP_ID=$(echo $SESSION_ACTION | jq -r .definition.taskRun.stepId)
TASK_ID=$(echo $SESSION_ACTION | jq -r .definition.taskRun.taskId)
TASK_OUTPUT_PREFIX=JobAttachments/Manifests/$DEV_FARM_ID/$DEV_QUEUE_ID/$JOB_ID/
$STEP_ID/$TASK_ID/
aws s3api list-objects-v2 --bucket $DEV_FARM_BUCKET --prefix $TASK_OUTPUT_PREFIX
```

Die angehängten Ausgabeaufträge werden nicht direkt von der Jobressource referenziert, sondern stattdessen in einem Amazon S3 S3-Bucket platziert, der auf der Farmressource basiert IDs.

5. Rufen Sie den neuesten Manifestobjektschlüssel für die spezifische Sitzungsaktions-ID ab und drucken Sie dann die Manifestobjekte hübsch aus.

```
SESSION_ACTION_ID=$(echo $SESSION_ACTION | jq -r .sessionActionId)
 MANIFEST_KEY=$(aws s3api list-objects-v2 \
     --bucket $DEV_FARM_BUCKET \
     --prefix $TASK_OUTPUT_PREFIX \
     --query "Contents[*].Key" --output text \
     | grep $SESSION_ACTION_ID \
     | sort | tail -1)
 MANIFEST_OBJECT=$(aws s3 cp s3://$DEV_FARM_BUCKET/$MANIFEST_KEY -)
 echo $MANIFEST_OBJECT | jq .
```

In der Ausgabe werden Eigenschaften der Datei `hash-jobattachments.txt` wie die folgenden angezeigt:

```
{
     "hashAlg": "xxh128",
     "manifestVersion": "2023-03-03",
     "paths": [
     {
         "hash": "f60b8e7d0fabf7214ba0b6822e82e08b",
         "mtime": 1698785252554950,
         "path": "hash-jobattachments.txt",
         "size": 182
     }
     ],
     "totalSize": 182
 }
```

Ihr Job wird nur ein einziges Manifest-Objekt pro Aufgabenausführung haben, aber im Allgemeinen ist es möglich, mehr Objekte pro Aufgabenausführung zu haben.

6. Zeigen Sie die für den Inhalt adressierbare Amazon S3 S3-Speicherausgabe unter dem Präfix an. `Data`

```
 FILE_HASH=$(echo $MANIFEST_OBJECT | jq -r .paths[0].hash)
 FILE_PATH=$(echo $MANIFEST_OBJECT | jq -r .paths[0].path)
 aws s3 cp s3://$DEV_FARM_BUCKET/JobAttachments/Data/$FILE_HASH -
```

Es wird eine Ausgabe wie die folgende angezeigt:

```
eaa2df5d34b54be5ac34c56a24a8c237b8487231a607eaf530a04d76b89c9cd3  /tmp/openjd/
session-123/assetroot-abc/simple_job/template.yaml
```

Nächste Schritte

Nachdem Sie gelernt haben, wie Sie Jobs mit Anhängen mithilfe der Deadline Cloud-CLI einreichen, können Sie Folgendes erkunden:

- Mit Deadline Cloud einreichenum zu erfahren, wie Sie Jobs mit einem OpenJD-Bundle auf Ihren Worker-Hosts ausführen.
- Fügen Sie Ihrer Entwicklerfarm in Deadline Cloud eine vom Service verwaltete Flotte hinzuum Ihre Jobs auf Hosts auszuführen, die von Deadline Cloud verwaltet werden.
- Bereinigen Sie Ihre Farmressourcen in Deadline Cloudum die Ressourcen herunterzufahren, die Sie für dieses Tutorial verwendet haben.

Fügen Sie Ihrer Entwicklerfarm in Deadline Cloud eine vom Service verwaltete Flotte hinzu

AWS CloudShell bietet nicht genügend Rechenkapazität, um größere Workloads zu testen. Es ist auch nicht für Jobs konfiguriert, die Aufgaben auf mehrere Worker-Hosts verteilen.

Anstatt zu verwenden CloudShell, können Sie Ihrer Entwicklerfarm eine Auto Scaling Service Managed Fleet (SMF) hinzufügen. Ein SMF bietet ausreichend Rechenkapazität für größere Workloads und kann Jobs bewältigen, bei denen Jobaufgaben auf mehrere Worker-Hosts verteilt werden müssen.

Bevor Sie ein SMF hinzufügen, müssen Sie eine Deadline Cloud-Farm, eine Warteschlange und eine Flotte einrichten. Siehe Erstellen Sie eine Deadline Cloud-Farm.

Um Ihrer Entwicklerfarm eine vom Service verwaltete Flotte hinzuzufügen

1. Wählen Sie Ihre erste AWS CloudShell Registerkarte aus, erstellen Sie dann die vom Service verwaltete Flotte und fügen Sie deren Flotten-ID hinzu. `.bashrc` Diese Aktion macht es für andere Terminalsitzungen verfügbar.

```
FLEET_ROLE_ARN="arn:aws:iam::$(aws sts get-caller-identity \
        --query "Account" --output text):role/${DEV_FARM_NAME}FleetRole"
 aws deadline create-fleet \
     --farm-id $DEV_FARM_ID \
     --display-name "$DEV_FARM_NAME SMF" \
     --role-arn $FLEET_ROLE_ARN \
     --max-worker-count 5 \
     --configuration \
         '{
             "serviceManagedEc2": {
                 "instanceCapabilities": {
                     "vCpuCount": {
                         "min": 2,
                         "max": 4
                     },
                     "memoryMiB": {
                         "min": 512
                     },
                     "osFamily": "linux",
                     "cpuArchitectureType": "x86_64"
                 },
                 "instanceMarketOptions": {
                     "type": "spot"
                 }
             }
         }'

 echo "DEV_SMF_ID=$(aws deadline list-fleets \
         --farm-id $DEV_FARM_ID \
         --query "fleets[?displayName=='$DEV_FARM_NAME SMF'].fleetId \
         | [0]" --output text)" >> ~/.bashrc
 source ~/.bashrc
```

2. Ordnen Sie das SMF Ihrer Warteschlange zu.

```
aws deadline create-queue-fleet-association \
     --farm-id $DEV_FARM_ID \
     --queue-id $DEV_QUEUE_ID \
     --fleet-id $DEV_SMF_ID
```

3. Einreichen simple_file_job in die Warteschlange. Wenn Sie aufgefordert werden, den Upload zu bestätigen, geben Sie ein**y**.

```
deadline bundle submit simple_file_job \
    -p InFile=simple_job/template.yaml \
    -p OutFile=hash-jobattachments.txt
```

4. Vergewissern Sie sich, dass das SMF ordnungsgemäß funktioniert.

```
deadline fleet get
```

   - Es kann einige Minuten dauern, bis der Mitarbeiter anfängt. Wiederholen Sie den `deadline fleet get` Befehl, bis Sie sehen, dass die Flotte läuft.
   - Die `queueFleetAssociationsStatus` für den Service verwaltete Flotte wird es sein. `ACTIVE`
   - Die SMF `autoScalingStatus` wird von `GROWING` zu wechseln. `STEADY`

   Ihr Status wird in etwa wie folgt aussehen:

```
fleetId: fleet-2cc78e0dd3f04d1db427e7dc1d51ea44
farmId: farm-63ee8d77cdab4a578b685be8c5561c4a
displayName: DeveloperFarm SMF
description: ''
status: ACTIVE
autoScalingStatus: STEADY
targetWorkerCount: 0
workerCount: 0
minWorkerCount: 0
maxWorkerCount: 5
```

5. Sehen Sie sich das Protokoll für den Job an, den Sie eingereicht haben. Dieses Protokoll wird in einem Protokoll in Amazon CloudWatch Logs gespeichert, nicht im CloudShell Dateisystem.

```
 JOB_ID=$(deadline config get defaults.job_id)
 SESSION_ID=$(aws deadline list-sessions \
         --farm-id $DEV_FARM_ID \
         --queue-id $DEV_QUEUE_ID \
         --job-id $JOB_ID \
         --query "sessions[0].sessionId" \
         --output text)
 aws logs tail /aws/deadline/$DEV_FARM_ID/$DEV_QUEUE_ID \
     --log-stream-names $SESSION_ID
```

Nächste Schritte

Nachdem Sie eine Flotte mit Servicemanagement erstellt und getestet haben, sollten Sie die Ressourcen, die Sie erstellt haben, entfernen, um unnötige Kosten zu vermeiden.

- Bereinigen Sie Ihre Farmressourcen in Deadline Cloudum die Ressourcen herunterzufahren, die Sie für dieses Tutorial verwendet haben.

Bereinigen Sie Ihre Farmressourcen in Deadline Cloud

Um neue Workloads und Pipeline-Integrationen zu entwickeln und zu testen, können Sie weiterhin die Deadline Cloud-Entwicklerfarm verwenden, die Sie für dieses Tutorial erstellt haben. Wenn Sie Ihre Entwicklerfarm nicht mehr benötigen, können Sie ihre Ressourcen, einschließlich Farm-, Flotten-, Warteschlangen-, AWS Identity and Access Management (IAM-) Rollen und Logs, in Amazon CloudWatch Logs löschen. Nachdem Sie diese Ressourcen gelöscht haben, müssen Sie das Tutorial erneut beginnen, um die Ressourcen verwenden zu können. Weitere Informationen finden Sie unter Erste Schritte mit Deadline Cloud-Ressourcen.

Um die Ressourcen der Entwicklerfarm zu bereinigen

1. Wählen Sie Ihren ersten CloudShell Tab und beenden Sie dann alle Verbindungen zwischen Warteschlangen und Flotten für Ihre Warteschlange.

```
FLEETS=$(aws deadline list-queue-fleet-associations \
        --farm-id $DEV_FARM_ID \
        --queue-id $DEV_QUEUE_ID \
        --query "queueFleetAssociations[].fleetId" \
        --output text)
for FLEET_ID in $FLEETS; do
    aws deadline update-queue-fleet-association \
        --farm-id $DEV_FARM_ID \
        --queue-id $DEV_QUEUE_ID \
        --fleet-id $FLEET_ID \
        --status STOP_SCHEDULING_AND_CANCEL_TASKS
done
```

2. Listet die Flottenzuordnungen der Warteschlange auf.

```
aws deadline list-queue-fleet-associations \
     --farm-id $DEV_FARM_ID \
```

```
     --queue-id $DEV_QUEUE_ID
```

Möglicherweise müssen Sie den Befehl erneut ausführen, bis die Ausgabe meldet`"status": "STOPPED"`, dann können Sie mit dem nächsten Schritt fortfahren. Dieser Vorgang kann mehrere Minuten in Anspruch nehmen.

```
{
    "queueFleetAssociations": [
        {
            "queueId": "queue-abcdefgh01234567890123456789012id",
            "fleetId": "fleet-abcdefgh01234567890123456789012id",
            "status": "STOPPED",
            "createdAt": "2023-11-21T20:49:19+00:00",
            "createdBy": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/
MySessionName",
            "updatedAt": "2023-11-21T20:49:38+00:00",
            "updatedBy": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/
MySessionName"
        },
        {
            "queueId": "queue-abcdefgh01234567890123456789012id",
            "fleetId": "fleet-abcdefgh01234567890123456789012id",
            "status": "STOPPED",
            "createdAt": "2023-11-21T20:32:06+00:00",
            "createdBy": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/
MySessionName",
            "updatedAt": "2023-11-21T20:49:39+00:00",
            "updatedBy": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/
MySessionName"
        }
    ]
}
```

3. Löschen Sie alle Verknüpfungen zwischen Warteschlange und Flotte für Ihre Warteschlange.

```
for FLEET_ID in $FLEETS; do
     aws deadline delete-queue-fleet-association \
         --farm-id $DEV_FARM_ID \
         --queue-id $DEV_QUEUE_ID \
         --fleet-id $FLEET_ID
 done
```

4. Löschen Sie alle Flotten, die Ihrer Warteschlange zugeordnet sind.

```
for FLEET_ID in $FLEETS; do
     aws deadline delete-fleet \
         --farm-id $DEV_FARM_ID \
         --fleet-id $FLEET_ID
 done
```

5. Löscht die Warteschlange.

```
aws deadline delete-queue \
     --farm-id $DEV_FARM_ID \
     --queue-id $DEV_QUEUE_ID
```

6. Löschen Sie die Farm.

```
aws deadline delete-farm \
     --farm-id $DEV_FARM_ID
```

7. Löschen Sie andere AWS Ressourcen für Ihre Farm.

   a. Löschen Sie die Flottenrolle AWS Identity and Access Management (IAM).

```
aws iam delete-role-policy \
     --role-name "${DEV_FARM_NAME}FleetRole" \
     --policy-name WorkerPermissions
aws iam delete-role \
     --role-name "${DEV_FARM_NAME}FleetRole"
```

   b. Löschen Sie die Warteschlangen-IAM-Rolle.

```
aws iam delete-role-policy \
     --role-name "${DEV_FARM_NAME}QueueRole" \
     --policy-name S3BucketsAccess
aws iam delete-role \
     --role-name "${DEV_FARM_NAME}QueueRole"
```

   c. Löschen Sie die Amazon CloudWatch Logs-Protokollgruppen. Jede Warteschlange und Flotte hat ihre eigene Protokollgruppe.

```
aws logs delete-log-group \
     --log-group-name "/aws/deadline/$DEV_FARM_ID/$DEV_QUEUE_ID"
```

```
aws logs delete-log-group \
     --log-group-name "/aws/deadline/$DEV_FARM_ID/$DEV_CMF_ID"
aws logs delete-log-group \
     --log-group-name "/aws/deadline/$DEV_FARM_ID/$DEV_SMF_ID"
```

Jobs mithilfe von Warteschlangenumgebungen konfigurieren

AWS Deadline Cloud verwendet Warteschlangenumgebungen, um die Software auf Ihren Mitarbeitern zu konfigurieren. In einer Umgebung können Sie zeitaufwändige Aufgaben wie Einrichtung und Abbau einmal für alle Aufgaben in einer Sitzung ausführen. Sie definiert die Aktionen, die auf einem Worker ausgeführt werden, wenn eine Sitzung gestartet oder beendet wird. Sie können eine Umgebung für eine Warteschlange, Jobs, die in der Warteschlange ausgeführt werden, und die einzelnen Schritte für einen Job konfigurieren.

Sie definieren Umgebungen als Warteschlangenumgebungen oder Jobumgebungen. Erstellen Sie Warteschlangenumgebungen mit der Deadline Cloud-Konsole oder mit dem Deadline: CreateQueueEnvironment -Betrieb und definieren Sie Jobumgebungen in den Jobvorlagen der Jobs, die Sie einreichen. Sie folgen der Open Job Description (OpenJD) -Spezifikation für Umgebungen. Einzelheiten finden Siehttps://github.com/OpenJobDescription/openjd-specifications/wiki/2023-09-Template-Schemas#4-environment <Environment>in der OpenJD-Spezifikation unter. GitHub

Zusätzlich zu einem `name` und enthält jede Umgebung zwei Felder`description`, die die Umgebung auf dem Host definieren. Diese sind:

- `script`— Die Aktion, die ergriffen wird, wenn diese Umgebung auf einem Worker ausgeführt wird.
- `variables`— Eine Reihe von Name/Wert-Paaren für Umgebungsvariablen, die beim Betreten der Umgebung festgelegt werden.

Sie müssen mindestens einen Wert von `script` oder angeben. `variables`

Sie können in Ihrer Jobvorlage mehr als eine Umgebung definieren. Jede Umgebung wird in der Reihenfolge angewendet, in der sie in der Vorlage aufgeführt ist. Sie können dies verwenden, um die Komplexität Ihrer Umgebungen zu bewältigen.

Die Standard-Warteschlangenumgebung für Deadline Cloud verwendet den Conda-Paketmanager, um Software in die Umgebung zu laden, aber Sie können auch andere Paketmanager verwenden. Die Standardumgebung definiert zwei Parameter, um die Software anzugeben, die geladen werden soll. Diese Variablen werden von den von Deadline Cloud bereitgestellten Einsendern festgelegt. Sie können sie jedoch auch in Ihren eigenen Skripten und Anwendungen festlegen, die die Standardumgebung verwenden. Diese sind:

- `CondaPackages`— Eine durch Leerzeichen getrennte Liste von Conda-Paketen, die den Spezifikationen entsprechen, die für den Job installiert werden sollen. Zum Beispiel würde der Blender-Absender in Blender 3.6 zusätzliche Bilder `blender=3.6` zum Rendern hinzufügen.
- `CondaChannels`— Eine durch Leerzeichen getrennte Liste von Conda-Kanälen, aus denen Pakete installiert werden sollen. Für vom Service verwaltete Flotten werden Pakete vom Channel aus installiert. `deadline-cloud` Sie können weitere Kanäle hinzufügen.

Themen

Steuern Sie die Jobumgebung mit OpenJD-Warteschlangenumgebungen

Mithilfe von Warteschlangenumgebungen können Sie benutzerdefinierte Umgebungen für Ihre Renderaufträge definieren. Eine Warteschlangenumgebung ist eine Vorlage, die die Umgebungsvariablen, Dateizuordnungen und andere Einstellungen für Jobs steuert, die in einer bestimmten Warteschlange ausgeführt werden. Sie ermöglicht es Ihnen, die Ausführungsumgebung für die an eine Warteschlange eingereichten Jobs an die Anforderungen Ihrer Workloads anzupassen. AWS Deadline Cloud bietet drei verschachtelte Ebenen, auf die Sie Open Job Description (OpenJD) -Umgebungen anwenden können: Queue, Job und Step. Durch die Definition von Warteschlangenumgebungen können Sie eine konsistente und optimierte Leistung für verschiedene Arten von Jobs sicherstellen, die Ressourcenzuweisung optimieren und die Warteschlangenverwaltung vereinfachen.

Die Warteschlangenumgebung ist eine Vorlage, die Sie über die AWS Verwaltungskonsole oder mithilfe der an eine Warteschlange in Ihrem AWS Konto anhängen. AWS CLI Sie können eine Umgebung für eine Warteschlange erstellen, oder Sie können mehrere Warteschlangenumgebungen erstellen, die angewendet wurden, um die Ausführungsumgebung zu erstellen. Auf diese Weise können Sie eine Umgebung schrittweise erstellen und testen, um sicherzustellen, dass sie für Ihre Jobs ordnungsgemäß funktioniert.

Job- und Step-Umgebungen sind in der Jobvorlage definiert, mit der Sie einen Job in Ihrer Warteschlange erstellen. Die OpenJD-Syntax ist in diesen verschiedenen Formen von Umgebungen dieselbe. In diesem Abschnitt werden wir sie innerhalb von Jobvorlagen zeigen.

Themen

Legen Sie Umgebungsvariablen in einer Warteschlangenumgebung fest

Open Job Description (OpenJD) -Umgebungen können Umgebungsvariablen festlegen, die jeder Taskbefehl in ihrem Geltungsbereich verwendet. Viele Anwendungen und Frameworks suchen nach Umgebungsvariablen, um die Funktionseinstellungen, den Protokollierungsgrad und mehr zu steuern.

Das Qt Framework bietet beispielsweise GUI-Funktionen für viele Desktop-Anwendungen. Wenn Sie diese Anwendungen auf einem Worker-Host ohne interaktive Anzeige ausführen, müssen Sie die Umgebungsvariable möglicherweise auf setzen`QT_QPA_PLATFORM`, `offscreen` damit der Worker nicht nach einer Anzeige sucht.

In diesem Beispiel verwenden Sie ein Beispiel-Auftragspaket aus dem Deadline Cloud-Beispielverzeichnis, um die Umgebungsvariablen für einen Job festzulegen und anzuzeigen.

Voraussetzungen

Führen Sie die folgenden Schritte aus, um das Beispiel-Job-Bundle mit Umgebungsvariablen aus dem Github-Repository für Beispiele von Deadline Cloud auszuführen.

1. Wenn Sie keine Deadline Cloud-Farm mit einer Warteschlange und der zugehörigen Linux-Flotte haben, folgen Sie der Anleitung zum Onboarding in der Deadline Cloud-Konsole, um eine Farm mit Standardeinstellungen zu erstellen.
2. Wenn Sie die Deadline Cloud-CLI und den Deadline Cloud-Monitor nicht auf Ihrer Workstation haben, folgen Sie den Schritten unter Deadline Cloud-Einreicher einrichten im Benutzerhandbuch.
3. Wird verwendet`git`, um das Deadline GitHub Cloud-Beispiel-Repository zu klonen.

```
git clone https://github.com/aws-deadline/deadline-cloud-samples.git
 Cloning into 'deadline-cloud-samples'...
 ...
cd deadline-cloud-samples/job_bundles
```

Führen Sie das Beispiel für die Umgebungsvariable aus

1. Verwenden Sie die Deadline Cloud-CLI, um das `job_env_vars` Beispiel einzureichen.

```
deadline bundle submit job_env_vars
 Submitting to Queue: MySampleQueue
 ...
```

2. Im Deadline Cloud-Monitor können Sie den neuen Job sehen und seinen Fortschritt überwachen. Nach dem Linux Die der Warteschlange zugeordnete Flotte verfügt über einen Mitarbeiter, der die Aufgabe des Auftrags ausführen kann. Der Auftrag ist in wenigen Sekunden abgeschlossen. Wählen Sie die Aufgabe aus und wählen Sie dann im Menü oben rechts im Aufgabenbereich die Option Protokolle anzeigen.

   Auf der rechten Seite befinden sich die drei Sitzungsaktionen „Starten“ JobEnv, „Starten StepEnv“ und „Aufgabe ausführen“. Die Protokollansicht in der Mitte des Fensters entspricht der ausgewählten Sitzungsaktion auf der rechten Seite.

Vergleichen Sie die Sitzungsaktionen mit ihren Definitionen

In diesem Abschnitt verwenden Sie den Deadline Cloud-Monitor, um die Sitzungsaktionen mit der Position zu vergleichen, in der sie in der Jobvorlage definiert sind. Es geht weiter mit dem vorherigen Abschnitt.

Öffnen Sie die Datei job_env_vars/template.yaml in einem Texteditor. Dies ist die Jobvorlage, die die Sitzungsaktionen definiert.

1. Wählen Sie im Deadline Cloud-Monitor die Aktion JobEnv Sitzung starten aus. Sie werden die folgende Protokollausgabe sehen.

```
 024/07/16 16:18:27-07:00
 2024/07/16 16:18:27-07:00 ==============================================
 2024/07/16 16:18:27-07:00 --------- Entering Environment: JobEnv
 2024/07/16 16:18:27-07:00 ==============================================
 2024/07/16 16:18:27-07:00 Setting: JOB_VERBOSITY=MEDIUM
 2024/07/16 16:18:27-07:00 Setting: JOB_EXAMPLE_PARAM=An example parameter value
 2024/07/16 16:18:27-07:00 Setting: JOB_PROJECT_ID=project-12
 2024/07/16 16:18:27-07:00 Setting: JOB_ENDPOINT_URL=https://internal-host-name/some/
path
 2024/07/16 16:18:27-07:00 Setting: QT_QPA_PLATFORM=offscreen
```

In den folgenden Zeilen aus der Jobvorlage wurde diese Aktion angegeben.

```
jobEnvironments:
 - name: JobEnv
   description: Job environments apply to everything in the job.
   variables:
     # When applications have options as environment variables, you can set them
 here.
     JOB_VERBOSITY: MEDIUM
     # You can use the value of job parameters when setting environment variables.
     JOB_EXAMPLE_PARAM: "{{Param.ExampleParam}}"
     # Some more ideas.
     JOB_PROJECT_ID: project-12
     JOB_ENDPOINT_URL: https://internal-host-name/some/path
     # This variable lets applications using the Qt Framework run without a display
     QT_QPA_PLATFORM: offscreen
```

2. Wählen Sie im Deadline Cloud-Monitor die Aktion StepEnv Sitzung starten aus. Sie werden die folgende Protokollausgabe sehen.

```
2024/07/16 16:18:27-07:00
2024/07/16 16:18:27-07:00 ================================================
2024/07/16 16:18:27-07:00 --------- Entering Environment: StepEnv
2024/07/16 16:18:27-07:00 ================================================
2024/07/16 16:18:27-07:00 Setting: STEP_VERBOSITY=HIGH
2024/07/16 16:18:27-07:00 Setting: JOB_PROJECT_ID=step-project-12
```

In den folgenden Zeilen aus der Jobvorlage wurde diese Aktion angegeben.

```
  stepEnvironments:
  - name: StepEnv
    description: Step environments apply to all the tasks in the step.
    variables:
      # These environment variables are only set within this step, not other steps.
      STEP_VERBOSITY: HIGH
      # Replace a variable value defined at the job level.
      JOB_PROJECT_ID: step-project-12
```

3. Wählen Sie im Deadline Cloud-Monitor die Aktion Sitzung ausführen aus. Sie werden die folgende Ausgabe sehen.

```
 2024/07/16 16:18:27-07:00
 2024/07/16 16:18:27-07:00 ==============================================
 2024/07/16 16:18:27-07:00 --------- Running Task
 2024/07/16 16:18:27-07:00 ==============================================
 2024/07/16 16:18:27-07:00 ----------------------------------------------
 2024/07/16 16:18:27-07:00 Phase: Setup
 2024/07/16 16:18:27-07:00 ----------------------------------------------
 2024/07/16 16:18:27-07:00 Writing embedded files for Task to disk.
 2024/07/16 16:18:27-07:00 Mapping: Task.File.Run -> /sessions/session-
b4bd451784674c0987be82c5f7d5642deupf6tk9/embedded_files08cdnuyt/tmpmdiajwvh
 2024/07/16 16:18:27-07:00 Wrote: Run -> /sessions/session-
b4bd451784674c0987be82c5f7d5642deupf6tk9/embedded_files08cdnuyt/tmpmdiajwvh
 2024/07/16 16:18:27-07:00 ----------------------------------------------
 2024/07/16 16:18:27-07:00 Phase: Running action
 2024/07/16 16:18:27-07:00 ----------------------------------------------
 2024/07/16 16:18:27-07:00 Running command sudo -u job-user -i setsid -w /sessions/
session-b4bd451784674c0987be82c5f7d5642deupf6tk9/tmpiqbrsby4.sh
 2024/07/16 16:18:27-07:00 Command started as pid: 2176
 2024/07/16 16:18:27-07:00 Output:
 2024/07/16 16:18:28-07:00 Running the task
 2024/07/16 16:18:28-07:00
 2024/07/16 16:18:28-07:00 Environment variables starting with JOB_*:
 2024/07/16 16:18:28-07:00 JOB_ENDPOINT_URL=https://internal-host-name/some/path
 2024/07/16 16:18:28-07:00 JOB_EXAMPLE_PARAM='An example parameter value'
 2024/07/16 16:18:28-07:00 JOB_PROJECT_ID=step-project-12
 2024/07/16 16:18:28-07:00 JOB_VERBOSITY=MEDIUM
 2024/07/16 16:18:28-07:00
 2024/07/16 16:18:28-07:00 Environment variables starting with STEP_*:
 2024/07/16 16:18:28-07:00 STEP_VERBOSITY=HIGH
 2024/07/16 16:18:28-07:00
 2024/07/16 16:18:28-07:00 Done running the task
 2024/07/16 16:18:28-07:00 ----------------------------------------------
 2024/07/16 16:18:28-07:00 Uploading output files to Job Attachments
 2024/07/16 16:18:28-07:00 ----------------------------------------------
```

In den folgenden Zeilen aus der Jobvorlage wurde diese Aktion angegeben.

```
  script:
    actions:
      onRun:
        command: bash
        args:
```

```
        - '{{Task.File.Run}}'
    embeddedFiles:
    - name: Run
      type: TEXT
      data: |
        echo Running the task
        echo ""

        echo Environment variables starting with JOB_*:
        set | grep ^JOB_
        echo ""

        echo Environment variables starting with STEP_*:
        set | grep ^STEP_
        echo ""

        echo Done running the task
```

Legen Sie den Pfad in einer Warteschlangenumgebung fest

Verwenden Sie OpenJD-Umgebungen, um neue Befehle in einer Umgebung bereitzustellen. Zuerst erstellen Sie ein Verzeichnis mit Skriptdateien und fügen dieses Verzeichnis dann zu den `PATH` Umgebungsvariablen hinzu, sodass die ausführbaren Dateien in Ihrem Skript sie ausführen können, ohne jedes Mal den Verzeichnispfad angeben zu müssen. Die Liste der Variablen in einer Umgebungsdefinition bietet keine Möglichkeit, die Variable zu ändern. Sie tun dies also, indem Sie stattdessen ein Skript ausführen. Nachdem das Skript die Dinge eingerichtet und geändert hat`PATH`, exportiert es die Variable mit dem Befehl in die OpenJD-Laufzeit. `echo "openjd_env: PATH=$PATH"`

Voraussetzungen

Führen Sie die folgenden Schritte aus, um das Beispiel-Job-Bundle mit Umgebungsvariablen aus dem Github-Repository für Beispiele von Deadline Cloud auszuführen.

1. Wenn Sie keine Deadline Cloud-Farm mit einer Warteschlange und der zugehörigen Linux-Flotte haben, folgen Sie der Anleitung zum Onboarding in der Deadline Cloud-Konsole, um eine Farm mit Standardeinstellungen zu erstellen.
2. Wenn Sie die Deadline Cloud-CLI und den Deadline Cloud-Monitor nicht auf Ihrer Workstation haben, folgen Sie den Schritten unter Deadline Cloud-Einreicher einrichten im Benutzerhandbuch.
3. Wird verwendet`git`, um das Deadline GitHub Cloud-Beispiel-Repository zu klonen.

```
git clone https://github.com/aws-deadline/deadline-cloud-samples.git
 Cloning into 'deadline-cloud-samples'...
 ...
cd deadline-cloud-samples/job_bundles
```

Führen Sie das Pfadbeispiel aus

1. Verwenden Sie die Deadline Cloud-CLI, um das `job_env_with_new_command` Beispiel einzureichen.

   ```
   $ deadline bundle submit job_env_with_new_command
   Submitting to Queue: MySampleQueue
   ...
   ```

2. Im Deadline Cloud-Monitor sehen Sie den neuen Job und können seinen Fortschritt überwachen. Sobald der Linux Die der Warteschlange zugeordnete Flotte verfügt über einen Mitarbeiter, der die Aufgabe des Auftrags ausführen kann. Der Auftrag ist in wenigen Sekunden abgeschlossen. Wählen Sie die Aufgabe aus und wählen Sie dann im Menü oben rechts im Aufgabenbereich die Option Protokolle anzeigen.

   Auf der rechten Seite befinden sich zwei Sitzungsaktionen: Starten RandomSleepCommand und Ausführen von Aufgaben. Die Protokollanzeige in der Mitte des Fensters entspricht der ausgewählten Sitzungsaktion auf der rechten Seite.

Vergleichen Sie die Sitzungsaktionen mit ihren Definitionen

In diesem Abschnitt verwenden Sie den Deadline Cloud-Monitor, um die Sitzungsaktionen mit der Position zu vergleichen, in der sie in der Jobvorlage definiert sind. Es geht weiter mit dem vorherigen Abschnitt.

Öffnen Sie die Datei job_env_with_new_command/template.yaml in einem Texteditor. Vergleichen Sie die Sitzungsaktionen mit den in der Jobvorlage definierten Aktionen.

1. Wählen Sie im Deadline Cloud-Monitor die Aktion RandomSleepCommand Sitzung starten aus. Sie werden die Protokollausgabe wie folgt sehen.

   ```
   2024/07/16 17:25:32-07:00
   2024/07/16 17:25:32-07:00 ================================================
   ```

```
 2024/07/16 17:25:32-07:00 --------- Entering Environment: RandomSleepCommand
 2024/07/16 17:25:32-07:00 ==============================================
 2024/07/16 17:25:32-07:00 ----------------------------------------------
 2024/07/16 17:25:32-07:00 Phase: Setup
 2024/07/16 17:25:32-07:00 ----------------------------------------------
 2024/07/16 17:25:32-07:00 Writing embedded files for Environment to disk.
 2024/07/16 17:25:32-07:00 Mapping: Env.File.Enter -> /sessions/session-
ab132a51b9b54d5da22cbe839dd946baaw1c8hk5/embedded_filesf3tq_1os/tmpbt8j_c3f
 2024/07/16 17:25:32-07:00 Mapping: Env.File.SleepScript -> /sessions/session-
ab132a51b9b54d5da22cbe839dd946baaw1c8hk5/embedded_filesf3tq_1os/tmperastlp4
 2024/07/16 17:25:32-07:00 Wrote: Enter -> /sessions/session-
ab132a51b9b54d5da22cbe839dd946baaw1c8hk5/embedded_filesf3tq_1os/tmpbt8j_c3f
 2024/07/16 17:25:32-07:00 Wrote: SleepScript -> /sessions/session-
ab132a51b9b54d5da22cbe839dd946baaw1c8hk5/embedded_filesf3tq_1os/tmperastlp4
 2024/07/16 17:25:32-07:00 ----------------------------------------------
 2024/07/16 17:25:32-07:00 Phase: Running action
 2024/07/16 17:25:32-07:00 ----------------------------------------------
 2024/07/16 17:25:32-07:00 Running command sudo -u job-user -i setsid -w /sessions/
session-ab132a51b9b54d5da22cbe839dd946baaw1c8hk5/tmpbwrquq5u.sh
 2024/07/16 17:25:32-07:00 Command started as pid: 2205
 2024/07/16 17:25:32-07:00 Output:
 2024/07/16 17:25:33-07:00 openjd_env: PATH=/sessions/session-
ab132a51b9b54d5da22cbe839dd946baaw1c8hk5/bin:/opt/conda/condabin:/home/job-
user/.local/bin:/home/job-user/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/
bin:/sbin:/bin:/var/lib/snapd/snap/bin
 No newer logs at this moment.
```

In den folgenden Zeilen aus der Jobvorlage wurde diese Aktion angegeben.

```
jobEnvironments:
- name: RandomSleepCommand
  description: Adds a command 'random-sleep' to the environment.
  script:
    actions:
      onEnter:
        command: bash
        args:
        - "{{Env.File.Enter}}"
    embeddedFiles:
    - name: Enter
      type: TEXT
      data: |
        #!/bin/env bash
```

```
        set -euo pipefail

        # Make a bin directory inside the session's working directory for providing
 new commands
        mkdir -p '{{Session.WorkingDirectory}}/bin'

        # If this bin directory is not already in the PATH, then add it
        if ! [[ ":$PATH:" == *':{{Session.WorkingDirectory}}/bin:'* ]]; then
          export "PATH={{Session.WorkingDirectory}}/bin:$PATH"

          # This message to Open Job Description exports the new PATH value to the
 environment
          echo "openjd_env: PATH=$PATH"
        fi

        # Copy the SleepScript embedded file into the bin directory
        cp '{{Env.File.SleepScript}}' '{{Session.WorkingDirectory}}/bin/random-
sleep'
        chmod u+x '{{Session.WorkingDirectory}}/bin/random-sleep'
    - name: SleepScript
      type: TEXT
      runnable: true
      data: |
        ...
```

2. Wählen Sie im Deadline Cloud-Monitor die Aktion StepEnv Sitzung starten aus. Sie sehen die Protokollausgabe wie folgt.

```
 2024/07/16 17:25:33-07:00
 2024/07/16 17:25:33-07:00 ==============================================
 2024/07/16 17:25:33-07:00 --------- Running Task
 2024/07/16 17:25:33-07:00 ==============================================
 2024/07/16 17:25:33-07:00 ----------------------------------------------
 2024/07/16 17:25:33-07:00 Phase: Setup
 2024/07/16 17:25:33-07:00 ----------------------------------------------
 2024/07/16 17:25:33-07:00 Writing embedded files for Task to disk.
 2024/07/16 17:25:33-07:00 Mapping: Task.File.Run -> /sessions/session-
ab132a51b9b54d5da22cbe839dd946baaw1c8hk5/embedded_filesf3tq_1os/tmpdrwuehjf
 2024/07/16 17:25:33-07:00 Wrote: Run -> /sessions/session-
ab132a51b9b54d5da22cbe839dd946baaw1c8hk5/embedded_filesf3tq_1os/tmpdrwuehjf
 2024/07/16 17:25:33-07:00 ----------------------------------------------
 2024/07/16 17:25:33-07:00 Phase: Running action
 2024/07/16 17:25:33-07:00 ----------------------------------------------
```

```
 2024/07/16 17:25:33-07:00 Running command sudo -u job-user -i setsid -w /sessions/
session-ab132a51b9b54d5da22cbe839dd946baaw1c8hk5/tmpz81iaqfw.sh
 2024/07/16 17:25:33-07:00 Command started as pid: 2256
 2024/07/16 17:25:33-07:00 Output:
 2024/07/16 17:25:34-07:00 + random-sleep 12.5 27.5
 2024/07/16 17:26:00-07:00 Sleeping for duration 26.90
 2024/07/16 17:26:00-07:00 ----------------------------------------------
 2024/07/16 17:26:00-07:00 Uploading output files to Job Attachments
 2024/07/16 17:26:00-07:00 ----------------------------------------------
```

3. In den folgenden Zeilen aus der Jobvorlage wurde diese Aktion angegeben.

```
steps:
- name: EnvWithCommand
  script:
    actions:
      onRun:
        command: bash
        args:
        - '{{Task.File.Run}}'
    embeddedFiles:
    - name: Run
      type: TEXT
      data: |
        set -xeuo pipefail

        # Run the script installed into PATH by the job environment
        random-sleep 12.5 27.5
  hostRequirements:
    attributes:
    - name: attr.worker.os.family
      anyOf:
      - linux
```

Führen Sie einen Hintergrund-Daemon-Prozess in der Warteschlangenumgebung aus

In vielen Anwendungsfällen beim Rendern kann das Laden der Anwendungs- und Szenendaten viel Zeit in Anspruch nehmen. Wenn ein Job sie für jeden Frame neu lädt, verbringt er die meiste Zeit mit Overhead. Es ist oft möglich, die Anwendung einmal als Hintergrund-Daemon-Prozess zu laden, sie

die Szenendaten laden zu lassen und ihr dann Befehle über Interprozesskommunikation (IPC) zu senden, um die Renderings durchzuführen.

Viele der Open-Source-Integrationen von Deadline Cloud verwenden dieses Muster. Das Projekt Open Job Description stellt eine Adapter-Laufzeitbibliothek mit robusten IPC-Mustern auf allen unterstützten Betriebssystemen bereit.

Um dieses Muster zu demonstrieren, gibt es ein eigenständiges Beispiel-Job-Paket, das Python- und Bash-Code verwendet, um einen Hintergrund-Daemon und den IPC für Aufgaben zur Kommunikation mit ihm zu implementieren. Der Daemon ist in Python implementiert und wartet auf ein SIGUSR1 POSIX-Signal, das angibt, wann eine Aufgabe bearbeitet werden muss. Die Aufgabendetails werden in einer bestimmten JSON-Datei an den Daemon übergeben, und die Ergebnisse der Ausführung der Aufgabe werden als weitere JSON-Datei zurückgegeben.

Voraussetzungen

Führen Sie die folgenden Schritte aus, um das Beispiel-Auftragspaket mit einem Daemon-Prozess aus dem Github-Repository für Beispiele von Deadline Cloud auszuführen.

1. Wenn Sie keine Deadline Cloud-Farm mit einer Warteschlange und der zugehörigen Linux-Flotte haben, folgen Sie der Anleitung zum Onboarding in der Deadline Cloud-Konsole, um eine Farm mit Standardeinstellungen zu erstellen.
2. Wenn Sie die Deadline Cloud-CLI und den Deadline Cloud-Monitor nicht auf Ihrer Workstation haben, folgen Sie den Schritten unter Deadline Cloud-Einreicher einrichten im Benutzerhandbuch.
3. Wird verwendet`git`, um das Deadline GitHub Cloud-Beispiel-Repository zu klonen.

```
git clone https://github.com/aws-deadline/deadline-cloud-samples.git
 Cloning into 'deadline-cloud-samples'...
 ...
cd deadline-cloud-samples/job_bundles
```

Führen Sie das Daemon-Beispiel aus

1. Verwenden Sie die Deadline Cloud-CLI, um das `job_env_daemon_process` Beispiel einzureichen.

```
 git clone https://github.com/aws-deadline/deadline-cloud-samples.git
Cloning into 'deadline-cloud-samples'...
```

```
 ...
cd deadline-cloud-samples/job_bundles
```

2. In der Deadline Cloud-Monitoranwendung sehen Sie den neuen Job und können seinen Fortschritt überwachen. Sobald der Linux In der Flotte, die der Warteschlange zugeordnet ist, steht ein Mitarbeiter zur Verfügung, der die Aufgabe ausführen kann. Der Auftrag wird in etwa einer Minute abgeschlossen. Wenn Sie eine der Aufgaben ausgewählt haben, wählen Sie im Menü oben rechts im Aufgabenbereich die Option Protokolle anzeigen.

   Auf der rechten Seite befinden sich zwei Sitzungsaktionen: Starten DaemonProcess und Ausführen von Aufgaben. Die Protokollanzeige in der Mitte des Fensters entspricht der ausgewählten Sitzungsaktion auf der rechten Seite.

   Wählen Sie die Option Protokolle für alle Aufgaben anzeigen. In der Zeitleiste werden die restlichen Aufgaben angezeigt, die im Rahmen der Sitzung ausgeführt wurden, sowie die `Shut down DaemonProcess` Aktion, die die Umgebung verlassen hat.

Sehen Sie sich die Daemon-Protokolle an

1. In diesem Abschnitt verwenden Sie den Deadline Cloud-Monitor, um die Sitzungsaktionen mit denen zu vergleichen, in denen sie in der Jobvorlage definiert sind. Es geht weiter mit dem vorherigen Abschnitt.

   Öffnen Sie die Datei job_env_daemon_process/template.yaml in einem Texteditor. Vergleichen Sie die Sitzungsaktionen mit den Aktionen, in denen sie in der Jobvorlage definiert sind.

2. Wählen Sie die `Launch DaemonProcess` Sitzungsaktion im Deadline Cloud-Monitor aus. Sie werden die Protokollausgabe wie folgt sehen.

```
 2024/07/17 16:27:20-07:00
 2024/07/17 16:27:20-07:00 ================================================
 2024/07/17 16:27:20-07:00 --------- Entering Environment: DaemonProcess
 2024/07/17 16:27:20-07:00 ================================================
 2024/07/17 16:27:20-07:00 ------------------------------------------------
 2024/07/17 16:27:20-07:00 Phase: Setup
 2024/07/17 16:27:20-07:00 ------------------------------------------------
 2024/07/17 16:27:20-07:00 Writing embedded files for Environment to disk.
 2024/07/17 16:27:20-07:00 Mapping: Env.File.Enter -> /sessions/
session-972e21d98dde45e59c7153bd9258a64dohwg4yg1/embedded_fileswy00x5ra/enter-daemon-
process-env.sh
```

```
 2024/07/17 16:27:20-07:00 Mapping: Env.File.Exit -> /sessions/
session-972e21d98dde45e59c7153bd9258a64dohwg4yg1/embedded_fileswy00x5ra/exit-daemon-
process-env.sh
 2024/07/17 16:27:20-07:00 Mapping: Env.File.DaemonScript -> /sessions/
session-972e21d98dde45e59c7153bd9258a64dohwg4yg1/embedded_fileswy00x5ra/daemon-
script.py
 2024/07/17 16:27:20-07:00 Mapping: Env.File.DaemonHelperFunctions -> /sessions/
session-972e21d98dde45e59c7153bd9258a64dohwg4yg1/embedded_fileswy00x5ra/daemon-
helper-functions.sh
 2024/07/17 16:27:20-07:00 Wrote: Enter -> /sessions/
session-972e21d98dde45e59c7153bd9258a64dohwg4yg1/embedded_fileswy00x5ra/enter-daemon-
process-env.sh
 2024/07/17 16:27:20-07:00 Wrote: Exit -> /sessions/
session-972e21d98dde45e59c7153bd9258a64dohwg4yg1/embedded_fileswy00x5ra/exit-daemon-
process-env.sh
 2024/07/17 16:27:20-07:00 Wrote: DaemonScript -> /sessions/
session-972e21d98dde45e59c7153bd9258a64dohwg4yg1/embedded_fileswy00x5ra/daemon-
script.py
 2024/07/17 16:27:20-07:00 Wrote: DaemonHelperFunctions -> /sessions/
session-972e21d98dde45e59c7153bd9258a64dohwg4yg1/embedded_fileswy00x5ra/daemon-
helper-functions.sh
 2024/07/17 16:27:20-07:00 ------------------------------------------------
 2024/07/17 16:27:20-07:00 Phase: Running action
 2024/07/17 16:27:20-07:00 ------------------------------------------------
 2024/07/17 16:27:20-07:00 Running command sudo -u job-user -i setsid -w /sessions/
session-972e21d98dde45e59c7153bd9258a64dohwg4yg1/tmp_u8slys3.sh
 2024/07/17 16:27:20-07:00 Command started as pid: 2187
 2024/07/17 16:27:20-07:00 Output:
 2024/07/17 16:27:21-07:00 openjd_env: DAEMON_LOG=/sessions/
session-972e21d98dde45e59c7153bd9258a64dohwg4yg1/daemon.log
 2024/07/17 16:27:21-07:00 openjd_env: DAEMON_PID=2223
 2024/07/17 16:27:21-07:00 openjd_env: DAEMON_BASH_HELPER_SCRIPT=/sessions/
session-972e21d98dde45e59c7153bd9258a64dohwg4yg1/embedded_fileswy00x5ra/daemon-
helper-functions.sh
```

In den folgenden Zeilen aus der Jobvorlage wurde diese Aktion angegeben.

```
  stepEnvironments:
  - name: DaemonProcess
    description: Runs a daemon process for the step's tasks to share.
    script:
      actions:
        onEnter:
```

```
          command: bash
          args:
          - "{{Env.File.Enter}}"
        onExit:
          command: bash
          args:
          - "{{Env.File.Exit}}"
      embeddedFiles:
      - name: Enter
        filename: enter-daemon-process-env.sh
        type: TEXT
        data: |
          #!/bin/env bash
          set -euo pipefail

          DAEMON_LOG='{{Session.WorkingDirectory}}/daemon.log'
          echo "openjd_env: DAEMON_LOG=$DAEMON_LOG"
          nohup python {{Env.File.DaemonScript}} > $DAEMON_LOG 2>&1 &
          echo "openjd_env: DAEMON_PID=$!"
          echo "openjd_env:
 DAEMON_BASH_HELPER_SCRIPT={{Env.File.DaemonHelperFunctions}}"

          echo 0 > 'daemon_log_cursor.txt'
    ...
```

3. Wählen Sie im Deadline Cloud-Monitor eine der Aktionen Task run: N session aus. Sie werden die Protokollausgabe wie folgt sehen.

```
2024/07/17 16:27:22-07:00
 2024/07/17 16:27:22-07:00 ============================================
 2024/07/17 16:27:22-07:00 --------- Running Task
 2024/07/17 16:27:22-07:00 ============================================
 2024/07/17 16:27:22-07:00 Parameter values:
 2024/07/17 16:27:22-07:00 Frame(INT) = 2
 2024/07/17 16:27:22-07:00 ------------------------------------------
 2024/07/17 16:27:22-07:00 Phase: Setup
 2024/07/17 16:27:22-07:00 ------------------------------------------
 2024/07/17 16:27:22-07:00 Writing embedded files for Task to disk.
 2024/07/17 16:27:22-07:00 Mapping: Task.File.Run -> /sessions/
session-972e21d98dde45e59c7153bd9258a64dohwg4yg1/embedded_fileswy00x5ra/run-task.sh
 2024/07/17 16:27:22-07:00 Wrote: Run -> /sessions/
session-972e21d98dde45e59c7153bd9258a64dohwg4yg1/embedded_fileswy00x5ra/run-task.sh
 2024/07/17 16:27:22-07:00 ------------------------------------------
```

```
 2024/07/17 16:27:22-07:00 Phase: Running action
 2024/07/17 16:27:22-07:00 ------------------------------------------
 2024/07/17 16:27:22-07:00 Running command sudo -u job-user -i setsid -w /sessions/
session-972e21d98dde45e59c7153bd9258a64dohwg4yg1/tmpv4obfkhn.sh
 2024/07/17 16:27:22-07:00 Command started as pid: 2301
 2024/07/17 16:27:22-07:00 Output:
 2024/07/17 16:27:23-07:00 Daemon PID is 2223
 2024/07/17 16:27:23-07:00 Daemon log file is /sessions/
session-972e21d98dde45e59c7153bd9258a64dohwg4yg1/daemon.log
 2024/07/17 16:27:23-07:00
 2024/07/17 16:27:23-07:00 === Previous output from daemon
 2024/07/17 16:27:23-07:00 ===
 2024/07/17 16:27:23-07:00
 2024/07/17 16:27:23-07:00 Sending command to daemon
 2024/07/17 16:27:23-07:00 Received task result:
 2024/07/17 16:27:23-07:00 {
 2024/07/17 16:27:23-07:00   "result": "SUCCESS",
 2024/07/17 16:27:23-07:00   "processedTaskCount": 1,
 2024/07/17 16:27:23-07:00   "randomValue": 0.2578537967668988,
 2024/07/17 16:27:23-07:00   "failureRate": 0.1
 2024/07/17 16:27:23-07:00 }
 2024/07/17 16:27:23-07:00
 2024/07/17 16:27:23-07:00 === Daemon log from running the task
 2024/07/17 16:27:23-07:00 Loading the task details file
 2024/07/17 16:27:23-07:00 Received task details:
 2024/07/17 16:27:23-07:00 {
 2024/07/17 16:27:23-07:00  "pid": 2329,
 2024/07/17 16:27:23-07:00  "frame": 2
 2024/07/17 16:27:23-07:00 }
 2024/07/17 16:27:23-07:00 Processing frame number 2
 2024/07/17 16:27:23-07:00 Writing result
 2024/07/17 16:27:23-07:00 Waiting until a USR1 signal is sent...
 2024/07/17 16:27:23-07:00 ===
 2024/07/17 16:27:23-07:00
 2024/07/17 16:27:23-07:00 ------------------------------------------
 2024/07/17 16:27:23-07:00 Uploading output files to Job Attachments
 2024/07/17 16:27:23-07:00 ------------------------------------------
```

Die folgenden Zeilen aus der Jobvorlage spezifizieren diese Aktion. ```Schritte:

```
 steps:
 - name: EnvWithDaemonProcess
   parameterSpace:
```

```
    taskParameterDefinitions:
    - name: Frame
      type: INT
      range: "{{Param.Frames}}"

  stepEnvironments:
    ...

  script:
    actions:
      onRun:
        timeout: 60
        command: bash
        args:
        - '{{Task.File.Run}}'
    embeddedFiles:
    - name: Run
      filename: run-task.sh
      type: TEXT
      data: |
        # This bash script sends a task to the background daemon process,
        # then waits for it to respond with the output result.

        set -euo pipefail

        source "$DAEMON_BASH_HELPER_SCRIPT"

        echo "Daemon PID is $DAEMON_PID"
        echo "Daemon log file is $DAEMON_LOG"

        print_daemon_log "Previous output from daemon"

        send_task_to_daemon "{\"pid\": $$, \"frame\": {{Task.Param.Frame}} }"
        wait_for_daemon_task_result

        echo Received task result:
        echo "$TASK_RESULT" | jq .

        print_daemon_log "Daemon log from running the task"

  hostRequirements:
    attributes:
    - name: attr.worker.os.family
      anyOf:
```

```
        - linux
```

Bewerben Sie sich für Ihre Jobs

Sie können eine Warteschlangenumgebung verwenden, um Anwendungen zur Verarbeitung Ihrer Jobs zu laden. Wenn Sie mithilfe der Deadline Cloud-Konsole eine vom Service verwaltete Flotte erstellen, haben Sie die Möglichkeit, eine Warteschlangenumgebung zu erstellen, die den Conda-Paketmanager zum Laden von Anwendungen verwendet.

Wenn Sie einen anderen Paketmanager verwenden möchten, können Sie eine Warteschlangenumgebung für diesen Manager erstellen. Ein Beispiel für die Verwendung von Rez finden Sie unterVerwenden Sie einen anderen Paketmanager.

Deadline Cloud bietet einen Conda-Kanal, über den Sie eine Auswahl von Rendering-Anwendungen in Ihre Umgebung laden können. Sie unterstützen die Einreicher, die Deadline Cloud für Anwendungen zur Erstellung digitaler Inhalte bereitstellt.

Sie können auch Software für Conda-Forge laden, um sie in Ihren Jobs zu verwenden. Die folgenden Beispiele zeigen Jobvorlagen, die die von Deadline Cloud bereitgestellte Warteschlangenumgebung verwenden, um Anwendungen vor der Ausführung des Jobs zu laden.

Themen

Eine Anwendung von einem Conda-Kanal abrufen

Sie können eine benutzerdefinierte Warteschlangenumgebung für Ihre Deadline Cloud-Mitarbeiter erstellen, die die Software Ihrer Wahl installiert. Diese Beispiel-Warteschlangenumgebung hat dasselbe Verhalten wie die Umgebung, die von der Konsole für vom Service verwaltete Flotten verwendet wird. Sie führt Conda direkt aus, um die Umgebung zu erstellen.

Die Umgebung erstellt für jede Deadline Cloud-Sitzung, die auf einem Worker ausgeführt wird, eine neue virtuelle Conda-Umgebung und löscht die Umgebung, wenn sie fertig ist.

Conda speichert die heruntergeladenen Pakete im Cache, sodass sie nicht erneut heruntergeladen werden müssen. In jeder Sitzung müssen jedoch alle Pakete mit der Umgebung verknüpft werden.

Die Umgebung definiert drei Skripte, die ausgeführt werden, wenn Deadline Cloud eine Sitzung auf einem Worker startet. Das erste Skript wird ausgeführt, wenn die `onEnter` Aktion aufgerufen wird. Es ruft die anderen beiden auf, um Umgebungsvariablen einzurichten. Wenn die Ausführung des Skripts abgeschlossen ist, ist die Conda-Umgebung verfügbar, in der alle angegebenen Umgebungsvariablen gesetzt sind.

Die neueste Version des Beispiels finden Sie unter conda_queue_env_console_equivalent.yaml im Repository unter. deadline-cloud-samples GitHub

Wenn Sie eine Anwendung verwenden möchten, die im Conda-Channel nicht verfügbar ist, können Sie einen Conda-Channel in Amazon S3 erstellen und dann Ihre eigenen Pakete für diese Anwendung erstellen. Weitere Informationen hierzu finden Sie unter Erstellen Sie einen Conda-Kanal mit S3.

Holen Sie sich Open-Source-Bibliotheken von Conda-Forge

In diesem Abschnitt wird beschrieben, wie Sie Open-Source-Bibliotheken aus dem `conda-forge` Kanal verwenden. Das folgende Beispiel ist eine Jobvorlage, die das `polars` Python-Paket verwendet.

Der Job legt die in der Warteschlangenumgebung definierten `CondaChannels` Parameter `CondaPackages` und fest, die Deadline Cloud mitteilen, wo das Paket abgerufen werden soll.

Der Abschnitt der Jobvorlage, der die Parameter festlegt, lautet:

```
- name: CondaPackages
  description: A list of conda packages to install. The job expects a Queue Environment
 to handle this.
  type: STRING
  default: polars
- name: CondaChannels
  description: A list of conda channels to get packages from. The job expects a Queue
 Environment to handle this.
  type: STRING
  default: conda-forge
```

Die neueste Version der vollständigen Beispiel-Jobvorlage finden Sie unter stage_1_self_contained_template/template.yaml. Die neueste Version der Warteschlangenumgebung, die die Conda-Pakete lädt, finden Sie unter conda_queue_env_console_equivalent.yaml im Repository unter. deadline-cloud-samples GitHub

Get Blender aus dem Deadline-Cloud-Kanal

Das folgende Beispiel zeigt eine Jobvorlage, die Blender aus dem `deadline-cloud` Conda-Kanal. Dieser Kanal unterstützt die Einreicher, die Deadline Cloud für Software zur Erstellung digitaler Inhalte bereitstellt. Sie können jedoch denselben Kanal verwenden, um Software für Ihren eigenen Gebrauch zu laden.

Eine Liste der vom `deadline-cloud` Kanal bereitgestellten Software finden Sie unter Standard-Warteschlangenumgebung im AWS Deadline Cloud-Benutzerhandbuch.

Dieser Job legt den in der Warteschlangenumgebung definierten `CondaPackages` Parameter fest, um Deadline Cloud anzuweisen, zu laden Blender in die Umgebung.

Der Abschnitt der Jobvorlage, der den Parameter festlegt, lautet:

```
- name: CondaPackages
  type: STRING
  userInterface:
    control: LINE_EDIT
    label: Conda Packages
    groupLabel: Software Environment
  default: blender
  description: >
    Tells the queue environment to install Blender from the deadline-cloud conda
 channel.
```

Die neueste Version der vollständigen Beispiel-Jobvorlage finden Sie unter blender_render/template.yaml. Die neueste Version der Warteschlangenumgebung, die die Conda-Pakete lädt, finden Sie unter conda_queue_env_console_equivalent.yaml im Repository unter deadline-cloud-samples GitHub.

Verwenden Sie einen anderen Paketmanager

Der Standard-Paketmanager für Deadline Cloud ist conda. Wenn Sie einen anderen Paketmanager verwenden müssen, z. B. Rez, können Sie eine benutzerdefinierte Warteschlangenumgebung erstellen, die Skripts enthält, die stattdessen Ihren Paketmanager verwenden.

Diese Beispiel-Warteschlangenumgebung bietet dasselbe Verhalten wie die Umgebung, die von der Konsole für vom Service verwaltete Flotten verwendet wird. Sie ersetzt den Conda-Paketmanager durch Rez.

Die Umgebung definiert drei Skripte, die ausgeführt werden, wenn Deadline Cloud eine Sitzung auf einem Worker startet. Das erste Skript wird ausgeführt, wenn die `onEnter` Aktion aufgerufen wird. Es ruft die anderen beiden auf, um Umgebungsvariablen einzurichten. Wenn die Ausführung des Skripts beendet ist, Rez Die Umgebung ist verfügbar, wenn alle angegebenen Umgebungsvariablen gesetzt sind.

Das Beispiel geht davon aus, dass Sie über eine vom Kunden verwaltete Flotte verfügen, die ein gemeinsam genutztes Dateisystem für die Rez-Pakete verwendet.

Die neueste Version des Beispiels finden Sie unter rez_queue_env.yaml im Repository unter deadline-cloud-samples GitHub.

Erstellen Sie einen Conda-Kanal mit S3

Wenn Sie benutzerdefinierte Pakete für Anwendungen haben, die auf den `conda-forge` Kanälen `deadline-cloud` oder nicht verfügbar sind, können Sie einen Conda-Channel erstellen, der die Pakete enthält, die Ihre Umgebungen verwenden. Sie können die Pakete in einem Amazon S3 S3-Bucket speichern und mithilfe von AWS Identity and Access Management Berechtigungen den Zugriff auf den Channel kontrollieren.

Sie können eine Deadline Cloud-Warteschlange verwenden, um die Pakete für Ihren Conda-Kanal zu erstellen, um die Aktualisierung und Wartung der Anwendungspakete zu vereinfachen.

Ein wesentlicher Vorteil dieses Ansatzes besteht darin, dass Ihre Warteschlange zur Paketerstellung Pakete für mehrere verschiedene Betriebssysteme mit oder ohne CUDA-Unterstützung erstellen kann. Im Vergleich dazu müssen Sie, wenn Sie Pakete auf Ihrer Workstation erstellen, für diese Fälle verschiedene Arbeitsstationen erstellen und verwalten.

Die folgenden Beispiele zeigen, wie Sie einen Conda-Channel erstellen, der eine Anwendung für Ihre Umgebungen bereitstellt. Die Anwendung in den Beispielen ist Blender 4.2, aber jede der in Deadline Cloud integrierten Anwendungen kann verwendet werden.

Sie können eine AWS CloudFormation Vorlage verwenden, um eine Deadline Cloud-Farm zu erstellen, die eine Warteschlange zur Paketerstellung enthält, oder Sie können den nachstehenden Anweisungen folgen, um die Beispielfarm selbst zu erstellen. Die AWS CloudFormation Vorlage finden Sie unter Eine AWS Deadline Cloud-Starter-Farm im Deadline Cloud-Beispiel-Repository auf GitHub.

Themen

Erstellen Sie eine Warteschlange zur Paketerstellung

In diesem Beispiel erstellen Sie eine Deadline Cloud-Warteschlange zum Erstellen der Blender 4.2 Anwendung. Dies vereinfacht die Lieferung der fertigen Pakete an den Amazon S3 S3-Bucket, der als Conda-Kanal verwendet wird, und Sie können Ihre bestehende Flotte verwenden, um das Paket zu erstellen. Dadurch wird die Anzahl der zu verwaltenden Infrastrukturkomponenten reduziert.

Folgen Sie den Anweisungen unter Eine Warteschlange erstellen im Deadline Cloud-Benutzerhandbuch. Nehmen Sie die folgenden Änderungen vor:

- Wählen Sie in Schritt 5 einen vorhandenen S3-Bucket aus. Geben Sie beispielsweise einen Namen für den Stammordner an, **`DeadlineCloudPackageBuild`** damit Build-Artefakte von Ihren normalen Deadline Cloud-Anhängen getrennt bleiben.
- In Schritt 6 können Sie die Warteschlange zur Paketerstellung einer vorhandenen Flotte zuordnen oder eine völlig neue Flotte erstellen, falls Ihre aktuelle Flotte nicht geeignet ist.
- Erstellen Sie in Schritt 9 eine neue Servicerolle für Ihre Paketbau-Warteschlange. Sie werden die Berechtigungen ändern, um der Warteschlange die Berechtigungen zu geben, die für das Hochladen von Paketen und die Neuindizierung eines Conda-Kanals erforderlich sind.

Konfigurieren Sie die Berechtigungen für die Warteschlange zur Paketerstellung

Damit die Warteschlange für die Paketerstellung auf das `/Conda` Präfix im S3-Bucket der Warteschlange zugreifen kann, müssen Sie die Rolle der Warteschlange ändern, um ihr Lese-/Schreibzugriff zu gewähren. Die Rolle benötigt die folgenden Berechtigungen, damit Paketerstellungsaufträge neue Pakete hochladen und den Channel neu indizieren können.

- `s3:GetObject`
- `s3:PutObject`
- `s3:ListBucket`
- `s3:GetBucketLocation`
- `s3:DeleteObject`

1. Öffnen Sie die Deadline Cloud-Konsole und navigieren Sie zur Seite mit den Warteschlangendetails für die Warteschlange zur Paketerstellung.

2. Wählen Sie die Warteschlangendienst-Rolle und anschließend Warteschlange bearbeiten aus.
3. Scrollen Sie zum Abschnitt Warteschlangendienstrolle und wählen Sie dann Diese Rolle in der IAM-Konsole anzeigen aus.
4. Wählen Sie aus der Liste der Berechtigungsrichtlinien die AmazonDeadlineCloudQueuePolicyfür Ihre Warteschlange aus.
5. Wählen Sie auf der Registerkarte „Berechtigungen“ die Option Bearbeiten aus.
6. Aktualisieren Sie die Warteschlangendienst-Rolle wie folgt. Ersetzen Sie *amzn-s3-demo-bucket* und *111122223333* durch Ihren eigenen Bucket und Ihr eigenes Konto.

```
{
   "Effect": "Allow",
   "Sid": "CustomCondaChannelReadWrite",
   "Action": [
    "s3:GetObject",
    "s3:PutObject",
    "s3:DeleteObject",
    "s3:ListBucket",
    "s3:GetBucketLocation"
   ],
   "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket",
    "arn:aws:s3:::amzn-s3-demo-bucket/Conda/*"   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "111122223333"
    }
   }
  },
```

Konfigurieren Sie die Berechtigungen für die Produktionswarteschlange für benutzerdefinierte Conda-Pakete

Ihre Produktionswarteschlange benötigt nur Leseberechtigungen für das `/Conda` Präfix im S3-Bucket der Warteschlange. Öffnen Sie die Seite AWS Identity and Access Management (IAM) für die Rolle, die der Produktionswarteschlange zugeordnet ist, und ändern Sie die Richtlinie wie folgt:

1. Öffnen Sie die Deadline Cloud-Konsole und navigieren Sie zur Seite mit den Warteschlangendetails für die Warteschlange zur Paketerstellung.

2. Wählen Sie die Warteschlangendienst-Rolle und anschließend Warteschlange bearbeiten aus.
3. Scrollen Sie zum Abschnitt Warteschlangendienstrolle und wählen Sie dann Diese Rolle in der IAM-Konsole anzeigen aus.
4. Wählen Sie aus der Liste der Berechtigungsrichtlinien die AmazonDeadlineCloudQueuePolicyfür Ihre Warteschlange aus.
5. Wählen Sie auf der Registerkarte „Berechtigungen“ die Option Bearbeiten aus.
6. Fügen Sie der Warteschlangendienst-Rolle einen neuen Abschnitt wie den folgenden hinzu. Ersetzen Sie *amzn-s3-demo-bucket* und *111122223333* durch Ihren eigenen Bucket und Ihr eigenes Konto.

```
{
   "Effect": "Allow",
   "Sid": "CustomCondaChannelReadOnly",
   "Action": [
    "s3:GetObject",
    "s3:ListBucket"
   ],
   "Resource": [
    "arn:aws:s3:::amzn-s3-demo-bucket",
    "arn:aws:s3:::amzn-s3-demo-bucket/Conda/*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "111122223333"
    }
   }
  },
```

Fügen Sie einer Warteschlangenumgebung einen Conda-Kanal hinzu

Um den S3-Conda-Kanal zu verwenden, müssen Sie den `s3://amzn-s3-demo-bucket/Conda/Default` Kanalstandort zum `CondaChannels` Parameter von Jobs hinzufügen, die Sie an Deadline Cloud senden. Die mit Deadline Cloud bereitgestellten Einreicher stellen Felder zur Verfügung, um benutzerdefinierte Conda-Kanäle und -Pakete anzugeben.

Sie können vermeiden, jeden Job zu ändern, indem Sie die Conda-Warteschlangenumgebung für Ihre Produktionswarteschlange bearbeiten. Gehen Sie für eine vom Service verwaltete Warteschlange wie folgt vor:

1. Öffnen Sie die Deadline Cloud-Konsole und navigieren Sie zur Seite mit den Warteschlangendetails für die Produktionswarteschlange.
2. Wählen Sie den Tab Umgebungen.
3. Wählen Sie die Conda-Warteschlangenumgebung und dann Bearbeiten aus.
4. Wählen Sie den JSON-Editor und suchen Sie dann im Skript nach der Parameterdefinition für`CondaChannels`.
5. Bearbeiten Sie die Zeile `default: "deadline-cloud"` so, dass sie mit dem neu erstellten S3-Conda-Kanal beginnt:

   ```
   default: "s3://amzn-s3-demo-bucket/Conda/Default deadline-cloud"
   ```

Serviceverwaltete Flotten aktivieren standardmäßig die strikte Kanalpriorität für Conda. Wenn Sie den neuen S3-Kanal verwenden, kann Conda den Kanal nicht verwenden. `deadline-cloud` Jeder Job, der die Verwendung über `blender=3.6` den `deadline-cloud` Kanal erfolgreich abgeschlossen hat, schlägt jetzt fehl, da Sie Blender 4.2.

Für vom Kunden verwaltete Flotten können Sie die Verwendung von Conda-Paketen aktivieren, indem Sie eines der Beispiele für die Conda-Warteschlangenumgebung in den Deadline Cloud-Beispielen verwenden GitHub Repository.

Erstellen Sie ein Conda-Paket für eine Anwendung

Sie können eine gesamte Anwendung, einschließlich Abhängigkeiten, zu einem Conda-Paket zusammenfassen. Die Pakete, die Deadline Cloud im Deadline-Cloud-Channel für serviceverwaltete Flotten bereitstellt, verwenden diesen binären Repacking-Ansatz. Dadurch werden dieselben Dateien wie bei einer Installation so organisiert, dass sie zur virtuellen Conda-Umgebung passen.

Beim Neupaketieren einer Anwendung für Conda gibt es zwei Ziele:

- Die meisten Dateien für die Anwendung sollten von der primären Struktur der virtuellen Conda-Umgebung getrennt sein. Umgebungen können die Anwendung dann mit Paketen aus anderen Quellen wie Conda-Forge mischen.

- Wenn eine virtuelle Conda-Umgebung aktiviert ist, sollte die Anwendung über die Umgebungsvariable PATH verfügbar sein.

Um eine Anwendung für Conda neu zu verpacken

1. Um eine Anwendung für Conda neu zu packen, schreiben Sie Conda-Build-Rezepte, die die Anwendung in einem Unterverzeichnis wie installieren. `$CONDA_PREFIX/opt/<application-name>` Dies unterscheidet es von den Standardpräfixverzeichnissen wie und. `bin` `lib`
2. Fügen Sie dann Symlinks oder Startskripte hinzu, `$CONDA_PREFIX/bin` um die Anwendungsbinärdateien auszuführen.

   Alternativ können Sie activate.d-Skripten erstellen, die der `conda activate` Befehl ausführt, um die Binärverzeichnisse der Anwendung zum PATH hinzuzufügen. Ein Windows, wo Symlinks nicht überall unterstützt werden, wo Umgebungen erstellt werden können, verwenden Sie stattdessen die Skripten application launch oder activate.d.
3. Manche Anwendungen sind auf Bibliotheken angewiesen, die nicht standardmäßig auf den vom Service verwalteten Flotten von Deadline Cloud installiert sind. Beispielsweise ist das X11-Fenstersystem für nicht interaktive Jobs normalerweise nicht erforderlich, aber für einige Anwendungen muss es immer noch ohne grafische Oberfläche ausgeführt werden. Sie müssen diese Abhängigkeiten in dem Paket angeben, das Sie erstellen.
4. Stellen Sie sicher, dass Sie die Urheber- und Lizenzvereinbarungen für die von Ihnen verpackten Anwendungen einhalten. Wir empfehlen, einen privaten Amazon S3 S3-Bucket für Ihren Conda-Kanal zu verwenden, um die Verteilung zu kontrollieren und den Paketzugriff auf Ihre Farm einzuschränken.

Erstellen Sie ein Conda-Build-Rezept für Blender

Sie können verschiedene Anwendungen verwenden, um ein Conda-Build-Rezept zu erstellen. Blender ist kostenlos zu verwenden und lässt sich einfach mit Conda verpacken. Das Tool Blender Foundation stellt Anwendungsarchive für mehrere Betriebssysteme bereit. Wir haben ein Beispiel für ein Conda-Build-Rezept erstellt, das die Windows-Dateien .zip und .tar.xz für Linux verwendet. In diesem Abschnitt erfahren Sie, wie Sie Blender 4.2 Conda-Build-Rezept.

Die Datei deadline-cloud.yaml spezifiziert die Conda-Plattformen und andere Metadaten für die Übermittlung von Paketaufträgen an Deadline Cloud. Dieses Rezept enthält Informationen zum

lokalen Quellarchiv, um zu demonstrieren, wie das funktioniert. Die Linux-64-Conda-Plattform ist so eingestellt, dass sie eine Standardkonfiguration für die Einreichung von Jobs einbaut, die der gängigsten Konfiguration entspricht. Die Datei deadline-cloud.yaml sieht etwa wie folgt aus:

```
condaPlatforms:
  - platform: linux-64
    defaultSubmit: true
    sourceArchiveFilename: blender-4.2.1-linux-x64.tar.xz
    sourceDownloadInstructions: 'Run "curl -LO https://download.blender.org/release/
Blender4.2/blender-4.2.1-linux-x64.tar.xz"'
  - platform: win-64
    defaultSubmit: false
    sourceArchiveFilename: blender-4.2.1-windows-x64.zip
    sourceDownloadInstructions: 'Run "curl -LO https://download.blender.org/release/
Blender4.2/blender-4.2.1-windows-x64.zip"'
```

Überprüfen Sie die Dateien im Verzeichnis. `recipe` Die Metadaten für das Rezept befinden sich in recipe/meta.yaml. Sie können auch die Dokumentation zu conda build meta.yaml lesen, um mehr zu erfahren, z. B. darüber, wie die Datei eine Vorlage zur Generierung von YAML ist. Die Vorlage wird verwendet, um die Versionsnummer nur einmal anzugeben und je nach Betriebssystem unterschiedliche Werte bereitzustellen.

Sie können die unter ausgewählten Build-Optionen überprüfen`meta.yaml`, um verschiedene Prüfungen für die binäre Verlagerung und das Verknüpfen von dynamischen gemeinsamen Objekten (DSO) zu deaktivieren. Diese Optionen steuern, wie das Paket funktioniert, wenn es in einer virtuellen Conda-Umgebung unter einem beliebigen Verzeichnispräfix installiert wird. Die Standardwerte vereinfachen das Verpacken jeder Abhängigkeitsbibliothek in ein separates Paket, aber wenn Sie eine Anwendung binär neu verpacken, müssen Sie sie ändern.

Wenn für die Anwendung, die Sie verpacken, zusätzliche Abhängigkeitsbibliotheken erforderlich sind oder Sie Plugins für eine Anwendung separat verpacken, können DSO-Fehler auftreten. Diese Fehler treten auf, wenn sich die Abhängigkeit nicht im Bibliothekssuchpfad für die ausführbare Datei oder Bibliothek befindet, die sie benötigt. Anwendungen sind darauf angewiesen, dass sich Bibliotheken in global definierten Pfaden wie `/lib` oder befinden`/usr/lib`, wenn sie auf einem System installiert sind. Da virtuelle Conda-Umgebungen jedoch überall platziert werden können, gibt es keinen absoluten Pfad, der verwendet werden kann. Conda verwendet relative RPATH-Funktionen, die beide Linux and macOS Unterstützung, um damit umzugehen. Weitere Informationen finden Sie in der Conda-Build-Dokumentation unter Pakete verschiebbar machen.

Blender erfordert keine RPATH-Anpassung, da die Anwendungsarchive unter Berücksichtigung dieser Tatsache erstellt wurden. Für Anwendungen, die dies benötigen, können Sie dieselben Tools verwenden wie Conda Build: unter Linux und `patchelf` unter `install_name_tool` macOS.

Während der Paketerstellung wird das Skript build.sh oder build_win.sh (aufgerufen von`bld.bat`) ausgeführt, um Dateien in einer Umgebung zu installieren, die mit den Paketabhängigkeiten vorbereitet ist. Diese Skripten kopieren die Installationsdateien, erstellen Symlinks von `$PREFIX/bin` ihnen und richten die Aktivierungsskripten ein. Ein Windows, es erstellt keine Symlinks, sondern fügt stattdessen das Blender-Verzeichnis zum PATH im Aktivierungsskript hinzu.

Wir verwenden `bash` statt `cmd.exe` einer.bat-Datei für Windows Teil des Conda-Build-Rezepts, da dies für mehr Konsistenz zwischen den Build-Skripten sorgt. Tipps zur Verwendung `bash` von finden Sie in der Empfehlung des Deadline Cloud-Entwicklerhandbuchs zur Workload-Portabilität Windows. Wenn du Git installiert hast für Windowsum das deadline-cloud-samplesGit-Repository zu klonen, auf das du bereits Zugriff hast`bash`.

In der Dokumentation zu den Conda-Build-Umgebungsvariablen sind die Werte aufgeführt, die für die Verwendung im Build-Skript verfügbar sind. Zu diesen Werten gehören `$SRC_DIR` für die Quellarchivdaten, `$PREFIX` für das Installationsverzeichnis, für den `$RECIPE_DIR` Zugriff auf andere Dateien aus dem Rezept, `$PKG_NAME` `$PKG_VERSION` für den Paketnamen und die Version sowie `$target_platform` für die Ziel-Conda-Plattform.

Reichen Sie das ein Blender 4.2 Paket-Job

Sie können Ihr eigenes bauen Blender 4.2 Conda-Paket zum Rendern von Jobs, indem Sie das herunterladen Blender archivieren und dann einen Job an die Paketbau-Warteschlange senden. Die Warteschlange sendet den Job an die zugehörige Flotte, um das Paket zu erstellen und den Conda-Channel neu zu indizieren.

Diese Anweisungen verwenden Git aus einer Bash-kompatiblen Shell, um einen OpenJD-Paketbaujob und einige Conda-Rezepte aus den Deadline Cloud-Beispielen abzurufen GitHub Repositorium. Sie benötigen außerdem Folgendes:

- Wenn du verwendest Windows, eine Version von bash, git BASH, wird installiert, wenn Sie Git installieren.
- Sie müssen die Deadline Cloud CLI installiert haben.
- Sie müssen beim Deadline Cloud-Monitor angemeldet sein.

1. Öffnen Sie die Deadline Cloud-Konfigurations-GUI mit dem folgenden Befehl und legen Sie die Standardfarm und -warteschlange auf Ihre Paketerstellungswarteschlange fest.

```
deadline config gui
```

2. Verwenden Sie den folgenden Befehl, um die Deadline Cloud-Beispiele zu klonen GitHUb Repository.

```
git clone https://github.com/aws-deadline/deadline-cloud-samples.git
```

3. Wechseln Sie in das `conda_recipes` Verzeichnis im `deadline-cloud-samples` Verzeichnis.

```
cd deadline-cloud-samples/conda_recipes
```

4. Führen Sie das aufgerufene Skript aus`submit-package-job`. Das Skript enthält Anweisungen zum Herunterladen Blender wenn Sie das Skript zum ersten Mal ausführen.

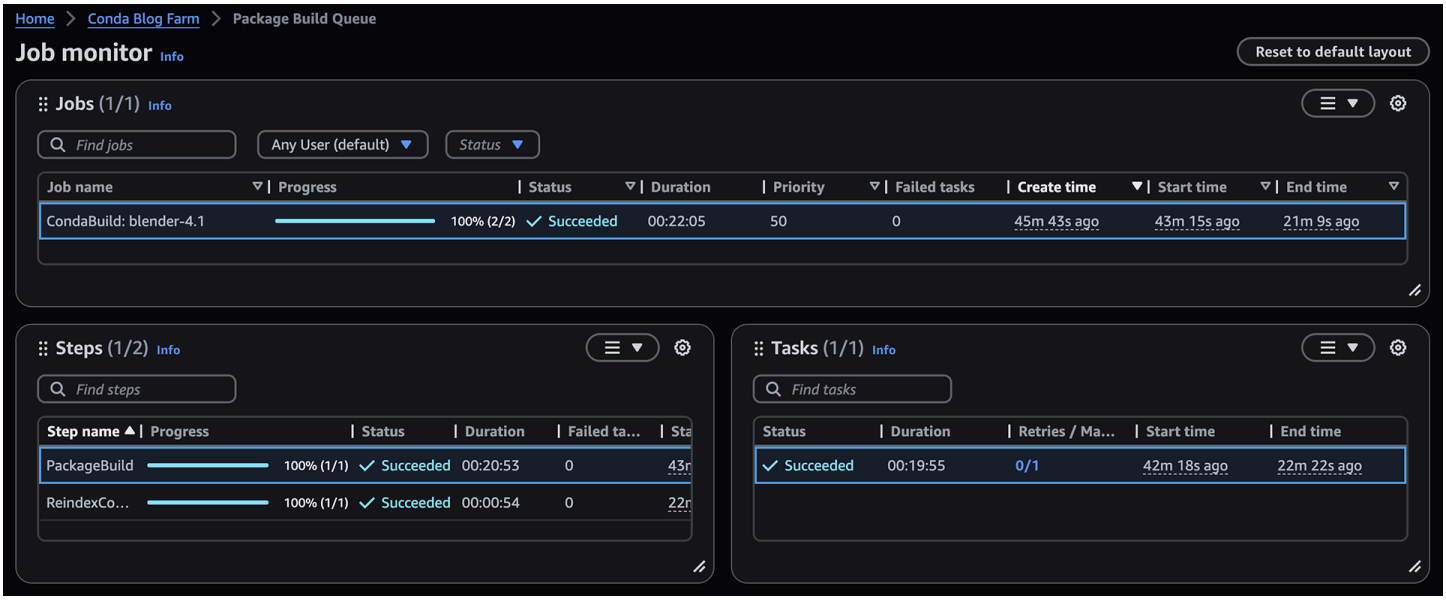
```
./submit-package-job blender-4.2/
```

5. Folgen Sie den Anweisungen zum Herunterladen Blender. Wenn Sie das Archiv haben, führen Sie das `submit-package-job` Skript erneut aus.

```
./submit-package-job blender-4.2/
```

Nachdem Sie den Job eingereicht haben, können Sie den Deadline Cloud-Monitor verwenden, um den Fortschritt und Status des Jobs während der Ausführung zu verfolgen.

In der unteren linken Ecke des Monitors werden die beiden Schritte des Jobs angezeigt: das Erstellen des Pakets und die anschließende Neuindizierung. Unten rechts werden die einzelnen Schritte für jede Aufgabe angezeigt. In diesem Beispiel gibt es für jede Aufgabe einen Schritt.



In der unteren linken Ecke des Monitors befinden sich die beiden Schritte des Jobs: das Erstellen des Pakets und das anschließende Neuindizieren des Conda-Kanals. Unten rechts befinden sich die einzelnen Aufgaben für jeden Schritt. In diesem Beispiel gibt es für jeden Schritt nur eine Aufgabe.

Wenn Sie mit der rechten Maustaste auf die Aufgabe für den Schritt zur Paketerstellung klicken und Protokolle anzeigen auswählen, zeigt der Monitor eine Liste von Sitzungsaktionen an, die zeigen, wie die Aufgabe für den Worker geplant ist. Die Aktionen sind:

- Anlagen synchronisieren — Diese Aktion kopiert die Eingabe-Job-Anhänge oder mountet ein virtuelles Dateisystem, je nachdem, welche Einstellung für das Dateisystem mit den Job-Anhängen verwendet wurde.
- Conda starten — Diese Aktion stammt aus der Warteschlangenumgebung, die standardmäßig hinzugefügt wurde, als Sie die Warteschlange erstellt haben. Der Job spezifiziert keine Conda-Pakete, sodass er schnell abgeschlossen wird und keine virtuelle Conda-Umgebung erstellt.
- CondaBuild Env starten — Diese Aktion erstellt eine benutzerdefinierte virtuelle Conda-Umgebung, die die Software enthält, die zum Erstellen eines Conda-Pakets und zur Neuindizierung eines Kanals erforderlich ist. Sie wird über den Conda-Forge-Kanal installiert.
- Task ausführen — Diese Aktion erstellt die Blender packt und lädt die Ergebnisse auf Amazon S3 hoch.

Während die Aktionen ausgeführt werden, senden sie Protokolle in einem strukturierten Format an Amazon CloudWatch. Wenn ein Job abgeschlossen ist, wählen Sie Protokolle für alle Aufgaben

anzeigen aus, um zusätzliche Protokolle über den Auf- und Abbau der Umgebung, in der der Job ausgeführt wird, einzusehen.

Testen Sie Ihr Paket mit einem Blender 4.2 Job rendern

Nachdem du die Blender 4.2 Das Paket erstellt und Ihre Produktionswarteschlange für die Verwendung des S3-Conda-Kanals konfiguriert, können Sie Jobs zum Rendern mit dem Paket einreichen. Wenn Sie keine haben Blender Szene, laden Sie die herunter Blender 3.5 - Gemütliche Küchenszene aus dem BlenderSeite mit Demo-Dateien.

Die Deadline Cloud-Beispiele GitHub Das Repository, das Sie zuvor heruntergeladen haben, enthält einen Beispieljob zum Rendern eines Blender Szene mit den folgenden Befehlen:

```
deadline bundle submit blender_render \
     -p CondaPackages=blender=4.2 \
     -p BlenderSceneFile=/path/to/downloaded/blender-3.5-splash.blend \
     -p Frames=1
```

Sie können den Deadline Cloud-Monitor verwenden, um den Fortschritt Ihres Jobs zu verfolgen:

1. Wählen Sie im Monitor die Aufgabe für den Job aus, den Sie eingereicht haben, und wählen Sie dann die Option, um das Protokoll anzuzeigen.
2. Wählen Sie auf der rechten Seite der Protokollansicht die Aktion Conda-Sitzung starten aus.

Sie können sehen, dass die Aktion in den beiden für die Warteschlangenumgebung konfigurierten Conda-Kanälen nach Blender 4.2 gesucht hat und dass sie das Paket im S3-Kanal gefunden hat.

Erstellen Sie ein Conda-Build-Rezept für Autodesk Maya

Sie können kommerzielle Anwendungen als Conda-Pakete verpacken. In Erstellen Sie ein Conda-Build-Rezept für Blenderhaben Sie gelernt, eine Anwendung zu verpacken, die als einfache, verschiebbare Archivdatei und unter Open-Source-Lizenzbedingungen verfügbar ist. Kommerzielle Anwendungen werden häufig über Installationsprogramme vertrieben und verfügen möglicherweise über ein Lizenzverwaltungssystem, mit dem sie arbeiten können.

Die folgende Liste baut auf den Grundlagen auf, die unter Erstellen eines Conda-Pakets für eine Anwendung behandelt werden, und zwar mit den Anforderungen, die üblicherweise mit der Paketierung kommerzieller Anwendungen verbunden sind. Die Einzelheiten in den Unteraufzählungen veranschaulichen, wie Sie die Richtlinien anwenden können Maya.

- Machen Sie sich mit den Lizenzrechten und Einschränkungen der Anwendung vertraut. Möglicherweise müssen Sie ein Lizenzverwaltungssystem konfigurieren. Wenn das Programm keine Durchsetzung vorsieht, müssen Sie Ihre Farm entsprechend Ihren Rechten konfigurieren.
  - Lesen Sie den Autodesk Häufig gestellte Fragen zu Abonnementvorteilen zu Cloud-Rechten, um mehr über Cloud-Rechte zu erfahren Maya das könnte auf Sie zutreffen. Konfigurieren Sie Ihre Deadline Cloud-Farm nach Bedarf.
  - Autodesk Produkte basieren auf einer Datei namens`ProductInformation.pit`. Für die meisten Konfigurationen dieser Datei ist Administratorzugriff auf das System erforderlich. Dieser Zugriff ist für vom Service verwaltete Flotten nicht verfügbar. Produktfunktionen für Thin Clients bieten eine Möglichkeit, dieses Problem an einem anderen Ort zu lösen. Weitere Informationen finden Sie unter Thin Client-Lizenzierung für Maya. MotionBuilder
- Manche Anwendungen hängen von Bibliotheken ab, die nicht auf den vom Service verwalteten Fleet Worker-Hosts installiert sind, weshalb das Paket sie bereitstellen muss. Dies kann direkt im Anwendungspaket oder in einem separaten Abhängigkeitspaket enthalten sein.
  - Maya hängt von einer Reihe solcher Bibliotheken ab, darunter freetype und fontconfig. Wenn diese Bibliotheken im Systempaketmanager verfügbar sind, z. B. in `dnf` für AL2 023, können Sie sie als Quelle für die Anwendung verwenden. Da diese RPM-Pakete nicht so konzipiert sind, dass sie verschiebbar sind, müssen Sie Tools verwenden, mit denen Sie sicherstellen können`patchelf`, dass Abhängigkeiten innerhalb der Maya Installationspräfix.
- Für die Installation ist möglicherweise Administratorzugriff erforderlich. Da vom Service verwaltete Flotten keinen Administratorzugriff bieten, müssen Sie eine Installation auf einem System mit diesem Zugriff durchführen. Erstellen Sie anschließend ein Archiv mit den Dateien, die für den Paketerstellungsauftrag benötigt werden.
  - Das Tool Windows Installationsprogramm für Maya erfordert Administratorzugriff, daher erfordert das Erstellen des Conda-Pakets dafür einen manuellen Prozess, um zuerst ein solches Archiv zu erstellen.
- Die Anwendungskonfiguration, einschließlich der Art und Weise, wie sich Plugins bei ihr registrieren, kann auf Betriebssystem- oder Benutzerebene definiert werden. Wenn Plugins in einer virtuellen Conda-Umgebung platziert werden, müssen sie so in die Anwendung integriert werden können, dass sie in sich geschlossen sind und niemals Dateien oder andere Daten außerhalb des Präfixes der virtuellen Umgebung schreiben. Wir empfehlen Ihnen, dies über das Conda-Paket der Anwendung einzurichten.
  - Die Probe Maya package definiert die Umgebungsvariable, `MAYA_NO_HOME=1` um sie von der Konfiguration auf Benutzerebene zu isolieren, und fügt Modulsuchpfade hinzu, `MAYA_MODULE_PATH` sodass separat verpackte Plugins aus der virtuellen Umgebung heraus

integriert werden können. Das Beispiel MtoA Das Paket platziert eine .mod-Datei in einem dieser Verzeichnisse, in die geladen werden kann Maya Start.

Schreiben Sie die Rezept-Metada

1. Öffnen Sie GitHub deadline-cloud-samplesVerzeichnis /conda_recipes/maya-2025 in Ihrem Browser oder in einem Texteditor in Ihrem lokalen Klon des Repositorys.

   Die Datei `deadline-cloud.yaml` beschreibt die Conda-Build-Plattformen, für die Pakete erstellt werden sollen, und wo die Anwendung herkommt. Das Rezeptbeispiel spezifiziert beide Linux and Windows baut, und nur das Linux wird standardmäßig übermittelt.

2. Laden Sie das vollständige Dokument herunter Maya Installateure von Ihrem Autodesk einloggen. Wählen Sie in der &Snowconsole; Ihren Auftrag aus der Tabelle. Linux, der Paket-Build kann das Archiv direkt verwenden, also platzieren Sie es direkt im `conda_recipes/archive_files` Verzeichnis. Wählen Sie in der &Snowconsole; Ihren Auftrag aus der Tabelle. Windows, das Installationsprogramm benötigt Administratorzugriff, um ausgeführt zu werden. Sie müssen das Installationsprogramm ausführen und die erforderlichen Dateien in einem Archiv für das Paketrezept sammeln, das Sie verwenden möchten. Die Datei README.md im Rezept dokumentiert ein wiederholbares Verfahren zur Erstellung dieses Artefakts. Das Verfahren verwendet eine neu gestartete EC2 Amazon-Instance, um eine saubere Umgebung für die Installation bereitzustellen, die Sie dann beenden können, nachdem Sie das Ergebnis gespeichert haben. Um andere Anwendungen zu verpacken, für die Administratorzugriff erforderlich ist, können Sie ein ähnliches Verfahren anwenden, sobald Sie den Satz von Dateien festgelegt haben, den die Anwendung benötigt.

3. Öffnen Sie die Dateien recipe/recipe.yaml und recipe/meta.yaml, um die Einstellungen für Rattler-Build und Conda-Build zu überprüfen oder zu bearbeiten. Sie können den Paketnamen und die Version für die Anwendung festlegen, die Sie verpacken.

   Der Quellbereich enthält einen Verweis auf die Archive, einschließlich des Sha256-Hashs der Dateien. Immer wenn Sie diese Dateien ändern, z. B. auf eine neue Version, müssen Sie diese Werte berechnen und aktualisieren.

   Der Build-Abschnitt enthält hauptsächlich Optionen zum Ausschalten der standardmäßigen Binärverschiebungsoptionen, da die automatischen Mechanismen für die speziellen Bibliotheks- und Binärverzeichnisse, die das Paket verwendet, nicht richtig funktionieren.

Schließlich können Sie im Abschnitt „Über“ einige Metadaten über die Anwendung eingeben, die beim Durchsuchen oder Verarbeiten des Inhalts eines Conda-Kanals verwendet werden können.

Schreiben Sie das Paketerstellungsskript

1. Die Skripte zum Erstellen von Paketen im Maya Die Beispiele für das Conda-Build-Rezept enthalten Kommentare, in denen die Schritte erläutert werden, die die Skripts ausführen. Lesen Sie sich die Kommentare und Befehle durch, um Folgendes herauszufinden:
   - Wie das Rezept mit der RPM-Datei umgeht von Autodesk
   - Die Änderungen, die das Rezept vornimmt, damit die Installation in die virtuellen Conda-Umgebungen verlagert werden kann, in denen das Rezept installiert ist
   - Wie das Rezept Hilfsvariablen festlegt, z. B. `MAYA_LOCATION` und `MAYA_VERSION` die Ihre Software verwenden kann, um zu verstehen Maya es läuft.
2. Wählen Sie in der &Snowconsole; Ihren Auftrag aus der Tabelle. Linux, öffnen Sie die Datei recipe/build.sh, um das Paketerstellungsskript zu überprüfen oder zu bearbeiten.

   Wählen Sie in der &Snowconsole; Ihren Auftrag aus der Tabelle. Windows, öffnen Sie die Datei recipe/build_win.sh, um das Paketerstellungsskript zu überprüfen oder zu bearbeiten.

Reichen Sie einen Job ein, der das erstellt Maya Pakete

1. Geben Sie das `conda_recipes` Verzeichnis in Ihrem Klon des GitHub deadline-cloud-samplesRepositorys ein.
2. Stellen Sie sicher, dass Ihre Deadline Cloud-Farm für Ihre Deadline Cloud-CLI konfiguriert ist. Wenn Sie die Schritte zum Erstellen eines Conda-Kanals mit Amazon S3 befolgt haben, sollte Ihre Farm für Ihre CLI konfiguriert sein.
3. Führen Sie den folgenden Befehl aus, um einen Job einzureichen, der beide erstellt Linux and Windows Pakete.

   ```
   ./submit-package-job maya-2025 --all-platforms
   ```

Erstellen Sie ein Conda-Build-Rezept für Autodesk Maya to Arnold (MtoA) Plugin

Sie können Plugins für kommerzielle Anwendungen als Conda-Pakete verpacken. Plugins sind dynamisch geladene Bibliotheken, die eine von einer Anwendung bereitgestellte Anwendungsbinärschnittstelle (ABI) verwenden, um die Funktionalität dieser Anwendung zu erweitern. Das Tool Maya to Arnold (MtoA) Das Plugin fügt das hinzu Arnold Renderer als Option innerhalb Maya.

Das Erstellen eines Pakets für ein Plugin ist wie das Verpacken einer Anwendung, aber das Paket wird in eine Hostanwendung integriert, die in einem anderen Paket enthalten ist. In der folgenden Liste werden die Voraussetzungen beschrieben, damit dies funktioniert.

- Nehmen Sie das Host-Anwendungspaket sowohl als Build- als auch als Ausführungsabhängigkeit in das Buildrezept auf `meta.yaml` und`recipe.yaml`. Verwenden Sie eine Versionsbeschränkung, sodass das Build-Rezept nur mit kompatiblen Paketen installiert wird.
  - Das Tool MtoA Das Beispiel-Buildrezept hängt ab von MayaPaket und verwendet eine == Einschränkung für die Version.
- Halten Sie sich bei der Registrierung des Plug-ins an die Konventionen für das Host-Anwendungspaket.
  - Das Tool Maya Paket konfiguriert ein Maya Modulpfad in der virtuellen Umgebung,`$PREFIX/usr/autodesk/maya$MAYA_VERSION/modules`, in dem das Plugin eine `.mod` Datei platzieren soll. Das Tool MtoA Ein Beispiel-Build-Rezept erstellt eine Datei `mtoa.mod` in diesem Verzeichnis.

Schreiben Sie die Rezept-Metadaten

1. Öffnen Sie GitHub deadline-cloud-samplesVerzeichnis /conda_recipes/maya-mtoa-2025 in Ihrem Browser oder in einem Texteditor in Ihrem lokalen Klon des Repositorys.

   Das Rezept folgt den gleichen Mustern wie das Maya Conda baut das Rezept und verwendet dieselben Quellarchive, um das Plugin zu installieren.
2. Öffnen Sie die Dateien recipe/recipe.yaml und recipe/meta.yaml, um die Einstellungen für Rattler-Build und für Conda-Build zu überprüfen oder zu bearbeiten. Diese Dateien spezifizieren eine Abhängigkeit, von der während der Paketerstellung und beim Erstellen einer virtuellen Umgebung zur Ausführung des Plugins abhängig ist. `maya`

Schreiben Sie das Paketerstellungsskript

- Die Skripte zum Erstellen von Paketen im MtoA Die Beispiele für das Conda-Build-Rezept enthalten Kommentare, in denen die Schritte erläutert werden, die die Skripts ausführen. Lesen Sie sich die Kommentare und Befehle durch, um zu erfahren, wie das Rezept installiert wird MtoA und erstellt eine Datei `mtoa.mod` in dem Verzeichnis, das durch den Maya Paket.

  Arnold and Maya dieselbe Lizenzierungstechnologie verwenden, also Maya Das Conda-Build-Rezept enthält bereits die Informationen, die benötigt werden von Arnold.

  Die Unterschiede zwischen den Linux and Windows Build-Skripte ähneln den Unterschieden für Maya Conda Build-Rezept.

Reichen Sie einen Job ein, der das erstellt Maya MtoA Plugin-Pakete

1. Geben Sie das `conda_recipes` Verzeichnis in Ihrem Klon des GitHub deadline-cloud-samplesRepositorys ein.
2. Stellen Sie sicher, dass Sie Pakete für erstellt haben Maya Host-Anwendung aus dem vorherigen Abschnitt.
3. Stellen Sie sicher, dass Ihre Deadline Cloud-Farm für Ihre Deadline Cloud-CLI konfiguriert ist. Wenn Sie die Schritte zum Erstellen eines Conda-Kanals mit Amazon S3 befolgt haben, sollte Ihre Farm für Ihre CLI konfiguriert sein.
4. Führen Sie den folgenden Befehl aus, um einen Job einzureichen, der beide erstellt Linux and Windows Pakete.

   ```
   ./submit-package-job maya-mtoa-2025 --all-platforms
   ```

Testen Sie Ihr Paket mit einem Maya Job rendern

Nachdem du die Maya 2025 und MtoA Wenn Pakete gebaut wurden, können Sie Jobs zum Rendern mit dem Paket einreichen. Der Plattenspieler mit Maya/ArnoldDas Job-Bundle-Beispiel rendert eine Animation mit Maya and Arnold. Dieses Beispiel wird auch FFmpeg zum Kodieren eines Videos verwendet. Sie können den Conda-Forge-Kanal zur Standardliste `CondaChannels` in Ihrer Conda-Warteschlangenumgebung hinzufügen, um eine Quelle für das Paket bereitzustellen. `ffmpeg`

Führen Sie im `job_bundles` Verzeichnis in Ihrem Git-Klon von den deadline-cloud-samplesfolgenden Befehl aus.

```
deadline bundle submit turntable_with_maya_arnold
```

Sie können den Deadline Cloud-Monitor verwenden, um den Fortschritt Ihres Jobs zu verfolgen:

1. Wählen Sie im Monitor die Aufgabe für den Job aus, den Sie eingereicht haben, und wählen Sie dann die Option, um das Protokoll anzuzeigen.
2. Wählen Sie auf der rechten Seite der Protokollansicht die Aktion Conda-Sitzung starten aus.

Sie können sehen, dass die Aktion gesucht hat maya and maya-mtoa in den Conda-Kanälen, die für die Warteschlangenumgebung konfiguriert sind, und dass die Pakete im S3-Kanal gefunden wurden.

Jobs erstellen, um sie an Deadline Cloud einzureichen

Sie reichen Jobs mithilfe von Jobpaketen an Deadline Cloud ein. Ein Job-Bundle ist eine Sammlung von Dateien, einschließlich einer Jobvorlage für Open Job Description (OpenJD) und aller zum Rendern des Jobs benötigten Asset-Dateien.

Die Jobvorlage beschreibt, wie Worker die Assets verarbeiten und darauf zugreifen, und stellt das Skript bereit, das der Worker ausführt. Job-Pakete ermöglichen es Künstlern, technischen Direktoren und Pipeline-Entwicklern, komplexe Jobs einfach von ihren lokalen Workstations oder der lokalen Renderfarm aus an Deadline Cloud zu senden. Dies ist besonders nützlich für Teams, die an groß angelegten Projekten mit visuellen Effekten, Animationen oder anderen Medienrendering-Projekten arbeiten und skalierbare Rechenressourcen auf Abruf benötigen.

Sie können das Auftragspaket mithilfe des lokalen Dateisystems zum Speichern von Dateien und eines Texteditors zum Erstellen der Auftragsvorlage erstellen. Nachdem Sie das Paket erstellt haben, reichen Sie den Job entweder mit der Deadline Cloud-CLI oder einem Tool wie einem Deadline Cloud-Submitter an Deadline Cloud ein

Sie können Ihre Ressourcen in einem Dateisystem speichern, das von Ihren Mitarbeitern gemeinsam genutzt wird, oder Sie können Deadline Cloud-Jobanhänge verwenden, um das Verschieben von Assets in S3-Buckets zu automatisieren, wo Ihre Mitarbeiter darauf zugreifen können. Jobanhänge helfen auch dabei, die Ergebnisse Ihrer Jobs zurück auf Ihre Workstations zu übertragen.

Die folgenden Abschnitte enthalten detaillierte Anweisungen zum Erstellen und Einreichen von Jobpaketen an Deadline Cloud.

Themen

Vorlagen für offene Stellenbeschreibungen (OpenJD) für Deadline Cloud

Ein Job-Bundle ist eines der Tools, mit denen Sie Jobs für AWS Deadline Cloud definieren. Sie gruppieren eine OpenJD-Vorlage (Open Job Description) mit zusätzlichen Informationen wie Dateien und Verzeichnissen, die Ihre Jobs mit Stellenanhängen verwenden. Sie verwenden die Deadline Cloud-Befehlszeilenschnittstelle (CLI), um ein Job-Bundle zu verwenden, um Jobs für die Ausführung in einer Warteschlange einzureichen.

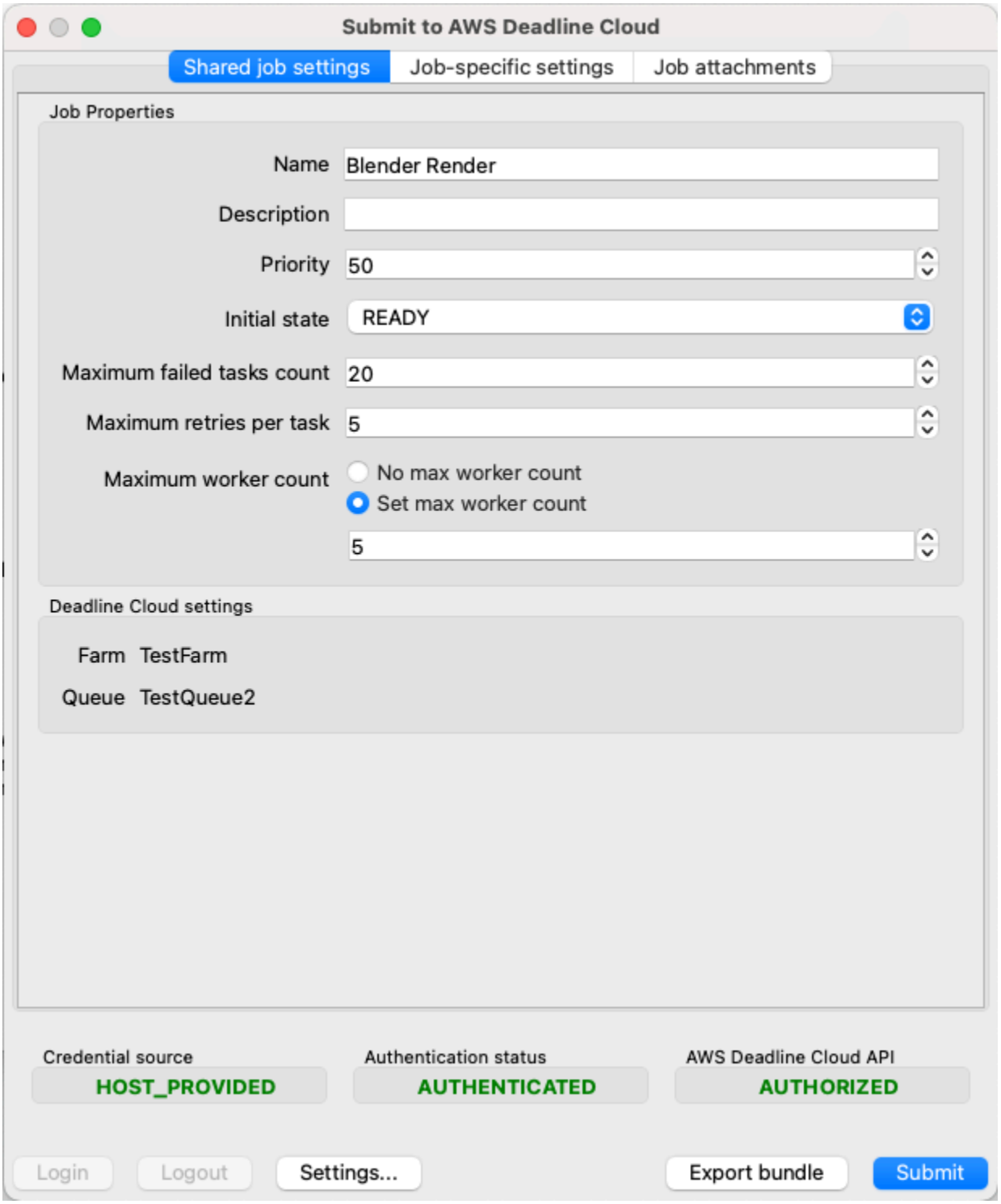
Ein Job-Bundle ist eine Verzeichnisstruktur, die eine OpenJD-Jobvorlage, andere Dateien, die den Job definieren, und jobspezifische Dateien enthält, die als Eingabe für Ihren Job benötigt werden. Sie können die Dateien, die Ihren Job definieren, entweder als YAML- oder JSON-Dateien angeben.

Die einzige erforderliche Datei ist entweder `template.yaml` oder`template.json`. Sie können auch die folgenden Dateien einschließen:

```
/template.yaml (or template.json)
/asset_references.yaml (or asset_references.json)
/parameter_values.yaml (or parameter_values.json)
/other job-specific files and directories
```

Verwenden Sie ein Job-Bundle für benutzerdefinierte Job-Übermittlungen mit der Deadline Cloud-CLI und einem Jobanhang, oder Sie können eine grafische Einreichungsoberfläche verwenden. Im Folgenden finden Sie beispielsweise das Blender-Beispiel von GitHub. Um das Beispiel mit dem folgenden Befehl im Blender-Beispielverzeichnis auszuführen:

```
deadline bundle gui-submit blender_render
```



Das Fenster mit den auftragsspezifischen Einstellungen wird aus den `userInterface` Eigenschaften der Jobparameter generiert, die in der Jobvorlage definiert sind.

Um einen Job über die Befehlszeile einzureichen, können Sie einen Befehl verwenden, der dem folgenden ähnelt

```
deadline bundle submit \
    --yes \
    --name Demo \
     -p BlenderSceneFile=location of scene file \
     -p OutputDir=file pathe for job output \
      blender_render/
```

Oder Sie können die `deadline.client.api.create_job_from_job_bundle` Funktion im `deadline` Python-Paket verwenden.

Alle in Deadline Cloud enthaltenen Plug-ins für Job-Einreicher, wie das Autodesk Maya-Plugin, generieren ein Job-Bundle für Ihre Einreichung und verwenden dann das Deadline Cloud-Python-Paket, um Ihren Job bei Deadline Cloud einzureichen. Sie können die eingereichten Job-Bundles im Job-Verlaufsverzeichnis Ihrer Workstation oder mithilfe eines Absenders einsehen. Sie können Ihr Job-Verlaufsverzeichnis mit dem folgenden Befehl finden:

```
deadline config get settings.job_history_dir
```

Wenn Ihr Job auf einem Deadline Cloud-Worker ausgeführt wird, hat er Zugriff auf Umgebungsvariablen, die ihm Informationen über den Job liefern. Die Umgebungsvariablen sind:

Variablenname	Verfügbar
DEADLINE_FARM_ID	Alle Aktionen
DEADLINE_FLOTTENNUMMER	Alle Aktionen
DEADLINE_WORKER-ID	Alle Aktionen
DEADLINE_WARTESCHLANGEN-ID	Alle Aktionen
DEADLINE_JOB-ID	Alle Aktionen
DEADLINE_SESSION_ID	Alle Aktionen
AKTIONS-ID FÜR DIE DEADLINE_SESSION_	Alle Aktionen
DEADLINE_TASK_ID	Aktionen der Aufgabe

Themen

Jobvorlagenelemente für Jobpakete

Die Jobvorlage definiert die Laufzeitumgebung und die Prozesse, die als Teil eines Deadline Cloud-Jobs ausgeführt werden. Sie können Parameter in einer Vorlage erstellen, sodass sie verwendet werden kann, um Jobs zu erstellen, die sich nur in den Eingabewerten unterscheiden, ähnlich wie bei einer Funktion in einer Programmiersprache.

Wenn Sie einen Job an Deadline Cloud senden, wird er in allen Warteschlangenumgebungen ausgeführt, die auf die Warteschlange angewendet wurden. Warteschlangenumgebungen werden mithilfe der Spezifikation für externe Umgebungen von Open Job Description (OpenJD) erstellt. Einzelheiten finden Sie in der Environment-Vorlage im OpenJD-Repository GitHub .

Eine Einführung in die Erstellung eines Jobs mit einer OpenJD-Jobvorlage finden Sie unter Einführung in die Erstellung eines Jobs im GitHub OpenJD-Repository. Zusätzliche Informationen finden Sie unter Wie Jobs ausgeführt werden. Es gibt Beispiele für Jobvorlagen im `samples` Verzeichnis des GitHub OpenJD-Repositorys.

Sie können die Jobvorlage entweder im YAML-Format (`template.yaml`) oder im JSON-Format (`template.json`) definieren. Die Beispiele in diesem Abschnitt werden im YAML-Format angezeigt.

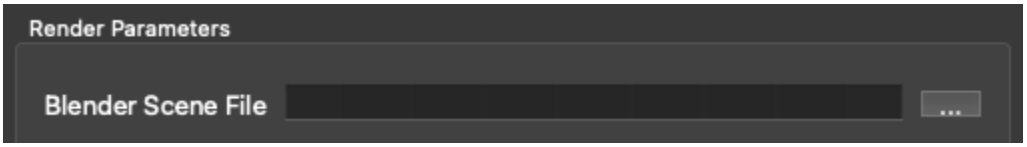
Die Jobvorlage für das `blender_render` Beispiel definiert beispielsweise einen Eingabeparameter `BlenderSceneFile` als Dateipfad:

```
- name: BlenderSceneFile
  type: PATH
  objectType: FILE
  dataFlow: IN
  userInterface:
    control: CHOOSE_INPUT_FILE
    label: Blender Scene File
    groupLabel: Render Parameters
    fileFilters:
    - label: Blender Scene Files
      patterns: ["*.blend"]
```

```
    - label: All Files
      patterns: ["*"]
  description: >
    Choose the Blender scene file to render. Use the 'Job Attachments' tab
    to add textures and other files that the job needs.
```

Die `userInterface` Eigenschaft definiert das Verhalten automatisch generierter Benutzeroberflächen sowohl in der Befehlszeile, die den Befehl verwendet, als auch in den Plug-ins für die Auftragsübermittlung für Anwendungen wie Autodesk Maya. `deadline bundle gui-submit`

In diesem Beispiel ist das UI-Widget zur Eingabe eines Werts für den `BlenderSceneFile` Parameter ein Dialogfeld zur Dateiauswahl, in dem nur Dateien angezeigt werden. `.blend`



Weitere Beispiele für die Verwendung des `userInteface` Elements finden Sie im Beispiel gui_control_showcase im Repository unter. deadline-cloud-samples GitHub

Die `dataFlow` Eigenschaften `objectType` und steuern das Verhalten von Job-Anhängen, wenn Sie einen Job aus einem Job-Bundle einreichen. In diesem Fall `dataFlow:IN` bedeuten `objectType: FILE` und, dass der Wert von eine Eingabedatei für Jobanhänge `BlenderSceneFile` ist.

Im Gegensatz dazu hat die Definition des `OutputDir` Parameters `objectType: DIRECTORY` und`dataFlow: OUT`:

```
- name: OutputDir
  type: PATH
  objectType: DIRECTORY
  dataFlow: OUT
  userInterface:
    control: CHOOSE_DIRECTORY
    label: Output Directory
    groupLabel: Render Parameters
  default: "./output"
  description: Choose the render output directory.
```

Der Wert des `OutputDir` Parameters wird von Job-Anhängen als Verzeichnis verwendet, in das der Job Ausgabedateien schreibt.

Weitere Informationen zu den `dataFlow` Eigenschaften `objectType` und finden Sie JobPathParameterDefinitionin der Spezifikation Open Job Description

Der Rest des Beispiels für eine `blender_render` Jobvorlage definiert den Arbeitsablauf des Jobs als einen einzelnen Schritt, wobei jedes Bild in der Animation als separate Aufgabe gerendert wird:

```
steps:
- name: RenderBlender
  parameterSpace:
    taskParameterDefinitions:
    - name: Frame
      type: INT
      range: "{{Param.Frames}}"
  script:
    actions:
      onRun:
        command: bash
        # Note: {{Task.File.Run}} is a variable that expands to the filename on the
 worker host's
        # disk where the contents of the 'Run' embedded file, below, is written.
        args: ['{{Task.File.Run}}']
    embeddedFiles:
      - name: Run
        type: TEXT
        data: |
          # Configure the task to fail if any individual command fails.
          set -xeuo pipefail

          mkdir -p '{{Param.OutputDir}}'

          blender --background '{{Param.BlenderSceneFile}}' \
                  --render-output '{{Param.OutputDir}}/{{Param.OutputPattern}}' \
                  --render-format {{Param.Format}} \
                  --use-extension 1 \
                  --render-frame {{Task.Param.Frame}}
```

Wenn der Wert des `Frames` Parameters beispielsweise lautet`1-10`, definiert er 10 Aufgaben. Jede Aufgabe hat einen anderen Wert für den `Frame` Parameter. Um eine Aufgabe auszuführen:

1. Alle Variablenverweise in der `data` Eigenschaft der eingebetteten Datei sind beispielsweise erweitert`--render-frame 1`.

2. Der Inhalt der `data` Eigenschaft wird in eine Datei im Arbeitsverzeichnis der Sitzung auf der Festplatte geschrieben.
3. Der onRun Befehl der Aufgabe wird in aufgelöst `bash` *`location of embedded file`* und dann ausgeführt.

Weitere Informationen zu eingebetteten Dateien, Sitzungen und Pfadzuordnungen finden Sie unter So werden Jobs ausgeführt in der Open Job Description-Spezifikation.

Es gibt weitere Beispiele für Jobvorlagen im Repository deadline-cloud-samples/job_bundles sowie die Vorlagenbeispiele, die in der Open Job Description-Spezifikation enthalten sind.

Parameterwerte, Elemente für Job-Bundles

Sie können die Parameterdatei verwenden, um die Werte einiger Jobparameter in der Jobvorlage oder der CreateJobOperationsanforderungsargumente im Job-Bundle festzulegen, sodass Sie beim Senden eines Jobs keine Werte festlegen müssen. Die Benutzeroberfläche für die Auftragsübermittlung ermöglicht es Ihnen, diese Werte zu ändern.

Sie können die Jobvorlage entweder im YAML-Format (`parameter_values.yaml`) oder im JSON-Format (`parameter_values.json`) definieren. Die Beispiele in diesem Abschnitt werden im YAML-Format angezeigt.

In YAML ist das Format der Datei:

```
parameterValues:
- name: <string>
  value: <integer>, <float>, or <string>
- name: <string>
  value: <integer>, <float>, or <string>ab
... repeating as necessary
```

Jedes Element der `parameterValues` Liste muss eines der folgenden sein:

- Ein in der Jobvorlage definierter Jobparameter.
- Ein Jobparameter, der in einer Warteschlangenumgebung für die Warteschlange definiert ist, an die Sie den Job senden.
- Ein spezieller Parameter, der beim Erstellen eines Jobs an den `CreateJob` Vorgang übergeben wird.

- `deadline:priority`— Der Wert muss eine Ganzzahl sein. Er wird als Prioritätsparameter an die `CreateJob` Operation übergeben.
- `deadline:targetTaskRunStatus`— Der Wert muss eine Zeichenfolge sein. Er wird als targetTaskRunStatus-Parameter an die `CreateJob` Operation übergeben.
- `deadline:maxFailedTasksCount`— Der Wert muss eine Ganzzahl sein. Er wird als maxFailedTasksCount-Parameter an die `CreateJob` Operation übergeben.
- `deadline:maxRetriesPerTask`— Der Wert muss eine Ganzzahl sein. Er wird als maxRetriesPerTask-Parameter an die `CreateJob` Operation übergeben.
- `deadline:maxWorkercount`— Der Wert muss eine Ganzzahl sein. Er wird als mazWorkerCountParameter an die `CreateJob` Operation übergeben.

Bei einer Jobvorlage handelt es sich immer um eine Vorlage und nicht um einen bestimmten Job, der ausgeführt werden soll. Eine Datei mit Parameterwerten ermöglicht es einem Job-Bundle, entweder als Vorlage zu dienen, wenn für einige Parameter in dieser Datei keine Werte definiert sind, oder als spezifische Jobübermittlung, wenn alle Parameter Werte haben.

Das Beispiel blender_render hat beispielsweise keine Parameterdatei und die zugehörige Jobvorlage definiert Parameter ohne Standardwerte. Diese Vorlage muss als Vorlage für die Erstellung von Jobs verwendet werden. Nachdem Sie mit diesem Job-Bundle einen Job erstellt haben, schreibt Deadline Cloud ein neues Job-Bundle in das Job-Verlaufsverzeichnis.

Zum Beispiel, wenn Sie einen Job mit dem folgenden Befehl einreichen:

```
deadline bundle gui-submit blender_render/
```

Das neue Job-Bundle enthält eine `parameter_values.yaml` Datei, die die angegebenen Parameter enthält:

```
% cat ~/.deadline/job_history/\(default\)/2024-06/2024-06-20-01-JobBundle-Demo/
parameter_values.yaml
parameterValues:
- name: deadline:targetTaskRunStatus
  value: READY
- name: deadline:maxFailedTasksCount
  value: 10
- name: deadline:maxRetriesPerTask
  value: 5
- name: deadline:priority
```

```
  value: 75
- name: BlenderSceneFile
  value: /private/tmp/bundle_demo/bmw27_cpu.blend
- name: Frames
  value: 1-10
- name: OutputDir
  value: /private/tmp/bundle_demo/output
- name: OutputPattern
  value: output_####
- name: Format
  value: PNG
- name: CondaPackages
  value: blender
- name: RezPackages
  value: blender
```

Sie können denselben Job mit dem folgenden Befehl erstellen:

```
deadline bundle submit ~/.deadline/job_history/\(default\)/2024-06/2024-06-20-01-
JobBundle-Demo/
```

> **Note**
>
> Das von Ihnen eingereichte Job-Bundle wird in Ihrem Job-Verlaufsverzeichnis gespeichert. Sie können den Speicherort dieses Verzeichnisses mit dem folgenden Befehl ermitteln:
>
> ```
> deadline config get settings.job_history_dir
> ```

Asset-Referenzen, Elemente für Job-Bundles

Sie können Deadline Cloud-Jobanhänge verwenden, um Dateien zwischen Ihrer Workstation und Deadline Cloud hin und her zu übertragen. Die Asset-Referenzdatei listet Eingabedateien und -verzeichnisse sowie Ausgabeverzeichnisse für Ihre Anhänge auf. Wenn Sie nicht alle Dateien und Verzeichnisse in dieser Datei auflisten, können Sie sie auswählen, wenn Sie einen Job mit dem `deadline bundle gui-submit` Befehl einreichen.

Diese Datei hat keine Auswirkung, wenn Sie keine Jobanhänge verwenden.

Sie können die Jobvorlage entweder im YAML-Format (`asset_references.yaml`) oder im JSON-Format (`asset_references.json`) definieren. Die Beispiele in diesem Abschnitt werden im YAML-Format angezeigt.

In YAML ist das Format der Datei:

```
assetReferences:
    inputs:
        # Filenames on the submitting workstation whose file contents are needed as
        # inputs to run the job.
        filenames:
        - list of file paths
        # Directories on the submitting workstation whose contents are needed as inputs
        # to run the job.
        directories:
        - list of directory paths

    outputs:
        # Directories on the submitting workstation where the job writes output files
        # if running locally.
        directories:
        - list of directory paths

    # Paths referenced by the job, but not necessarily input or output.
    # Use this if your job uses the name of a path in some way, but does not explicitly
 need
    # the contents of that path.
    referencedPaths:
    - list of directory paths
```

Bei der Auswahl der Eingabe- oder Ausgabedatei, die auf Amazon S3 hochgeladen werden soll, vergleicht Deadline Cloud den Dateipfad mit den Pfaden, die in Ihren Speicherprofilen aufgeführt sind. Jeder Dateisystemspeicherort `SHARED` vom Typ -type in einem Speicherprofil abstrahiert eine Netzwerk-Dateifreigabe, die auf Ihren Workstations und Worker-Hosts bereitgestellt wird. Deadline Cloud lädt nur Dateien hoch, die sich nicht auf einer dieser Dateifreigaben befinden.

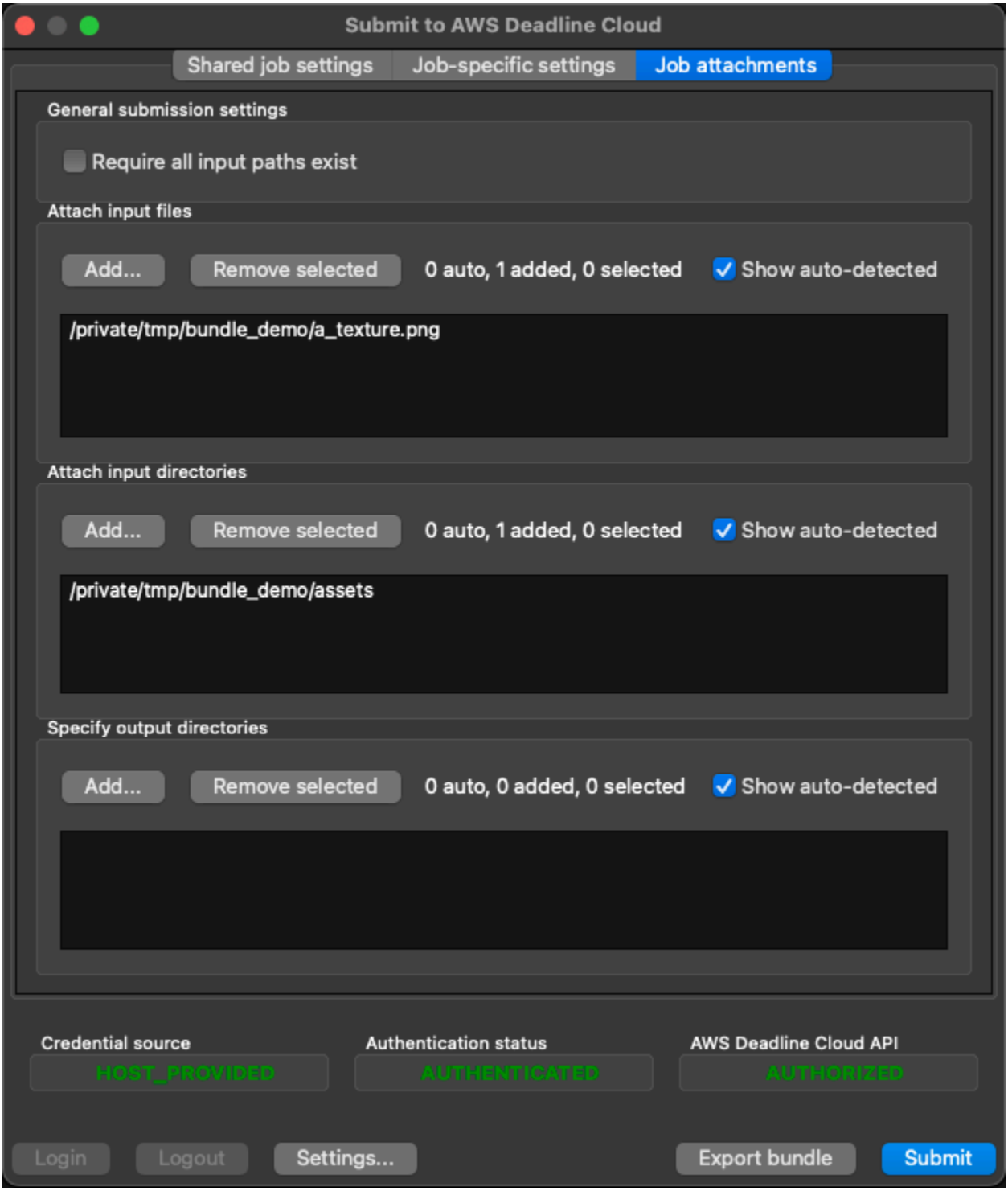
Weitere Informationen zum Erstellen und Verwenden von Speicherprofilen finden Sie unter Gemeinsamer Speicher in Deadline Cloud im AWS Deadline Cloud-Benutzerhandbuch.

Example - Die von der Deadline Cloud-GUI erstellte Asset-Referenzdatei

Verwenden Sie den folgenden Befehl, um einen Job mithilfe des Beispiels blender_render einzureichen.

```
deadline bundle gui-submit blender_render/
```

Fügen Sie dem Job auf der Registerkarte Jobanhänge einige zusätzliche Dateien hinzu:



Nachdem Sie den Job eingereicht haben, können Sie sich die `asset_references.yaml` Datei im Job-Bundle im Job-Verlaufsverzeichnis ansehen, um die Assets in der YAML-Datei zu sehen:

```
% cat ~/.deadline/job_history/\(default\)/2024-06/2024-06-20-01-JobBundle-Demo/
asset_references.yaml
```

```
assetReferences:
  inputs:
    filenames:
    - /private/tmp/bundle_demo/a_texture.png
    directories:
    - /private/tmp/bundle_demo/assets
  outputs:
    directories: []
  referencedPaths: []
```

Dateien in Ihren Jobs verwenden

Viele der Jobs, die Sie an AWS Deadline Cloud einreichen, enthalten Eingabe- und Ausgabedateien. Ihre Eingabedateien und Ausgabeverzeichnisse befinden sich möglicherweise auf einer Kombination aus gemeinsam genutzten Dateisystemen und lokalen Laufwerken. Jobs müssen den Inhalt an diesen Speicherorten lokalisieren. Deadline Cloud bietet zwei Funktionen: Jobanhänge und Speicherprofile, die zusammenarbeiten, damit Ihre Jobs die benötigten Dateien finden können.

Arbeitsanhänge bieten mehrere Vorteile

- Dateien mit Amazon S3 zwischen Hosts verschieben
- Übertragen Sie Dateien von Ihrer Workstation auf Worker-Hosts und umgekehrt
- Verfügbar für Jobs in Warteschlangen, in denen Sie die Funktion aktivieren
- Wird hauptsächlich für vom Service verwaltete Flotten verwendet, ist aber auch kompatibel mit vom Kunden verwalteten Flotten.

Verwenden Sie Speicherprofile, um das Layout gemeinsam genutzter Dateisystemspeicherorte auf Ihrer Workstation und Ihren Worker-Hosts zuzuordnen. Dies hilft Ihren Jobs dabei, gemeinsam genutzte Dateien und Verzeichnisse zu finden, wenn sich deren Speicherorte auf Ihrer Workstation und Ihren Worker-Hosts unterscheiden, z. B. bei plattformübergreifenden Konfigurationen mit Windows basierten Workstations und Linux basierten Worker-Hosts. Die Zuordnung Ihrer Dateisystemkonfiguration im Speicherprofil wird auch von Job-Anhängen verwendet, um die Dateien zu identifizieren, die für den Transfer zwischen Hosts über Amazon S3 benötigt werden.

Wenn Sie keine Jobanhänge verwenden und keine Datei- und Verzeichnisspeicherorte zwischen Workstations und Worker-Hosts neu zuordnen müssen, müssen Sie Ihre Fileshares nicht mit Speicherprofilen modellieren.

Themen

Beispiel für eine Projektinfrastruktur

Um die Verwendung von Job-Anhängen und Speicherprofilen zu demonstrieren, richten Sie eine Testumgebung mit zwei separaten Projekten ein. Sie können die Deadline Cloud-Konsole verwenden, um die Testressourcen zu erstellen.

1. Falls Sie dies noch nicht getan haben, erstellen Sie eine Testfarm. Gehen Sie wie unter Farm erstellen beschrieben vor, um eine Farm zu erstellen.
2. Erstellen Sie in jedem der beiden Projekte zwei Warteschlangen für Jobs. Gehen Sie wie unter Warteschlange erstellen beschrieben vor, um Warteschlangen zu erstellen.

    a. Erstellen Sie die erste **`Q1`** aufgerufene Warteschlange. Verwenden Sie die folgende Konfiguration und verwenden Sie die Standardeinstellungen für alle anderen Elemente.

    - Wählen Sie für Jobanhänge Create a new Amazon S3 S3-Bucket aus.
    - Wählen Sie Zuordnung zu kundenverwalteten Flotten aktivieren aus.
    - Geben Sie für die Ausführung als Benutzer sowohl **`jobuser`** für den POSIX-Benutzer als auch für die POSIX-Gruppe ein.
    - Erstellen Sie für die Warteschlangendienst-Rolle eine neue Rolle mit dem Namen **`AssetDemoFarm-Q1-Role`**
    - Deaktivieren Sie das standardmäßige Kontrollkästchen für die Conda-Warteschlangenumgebung.

    b. Erstellen Sie die zweite **`Q2`** aufgerufene Warteschlange. Verwenden Sie die folgende Konfiguration und verwenden Sie die Standardeinstellungen für alle anderen Elemente.

    - Wählen Sie für Jobanhänge Create a new Amazon S3 S3-Bucket aus.
    - Wählen Sie Zuordnung zu kundenverwalteten Flotten aktivieren aus.
    - Geben Sie für die Ausführung als Benutzer sowohl **`jobuser`** für den POSIX-Benutzer als auch für die POSIX-Gruppe ein.
    - Erstellen Sie für die Warteschlangendienst-Rolle eine neue Rolle mit dem Namen **`AssetDemoFarm-Q2-Role`**

    - Deaktivieren Sie das standardmäßige Kontrollkästchen für die Conda-Warteschlangenumgebung.

3. Erstellen Sie eine einzige, vom Kunden verwaltete Flotte, die die Jobs von beiden Warteschlangen aus ausführt. Um die Flotte zu erstellen, folgen Sie dem Verfahren unter Erstellen einer kundenverwalteten Flotte. Verwenden Sie die folgende Konfiguration:

    - Verwenden Sie als Name**`DemoFleet`**.
    - Wählen Sie als Flottenart die Option Vom Kunden verwaltet aus
    - Erstellen Sie für die Servicerolle Fleet eine neue Rolle mit dem Namen AssetDemoFarm-Fleet-Role.
    - Ordnen Sie die Flotte keinen Warteschlangen zu.

Die Testumgebung geht davon aus, dass es drei Dateisysteme gibt, die von Hosts gemeinsam genutzt werden, die Netzwerkdateifreigaben verwenden. In diesem Beispiel haben die Speicherorte die folgenden Namen:

- `FSCommon`- enthält Eingabe-Job-Assets, die beiden Projekten gemeinsam sind.
- `FS1`- enthält Eingabe- und Ausgabe-Auftragsressourcen für Projekt 1.
- `FS2`- enthält Eingabe- und Ausgabe-Auftragsressourcen für Projekt 2.

In der Testumgebung wird außerdem davon ausgegangen, dass es drei Arbeitsstationen gibt, und zwar wie folgt:

- `WSAll`- Eine Linux basierte Workstation, die von Entwicklern für alle Projekte verwendet wird. Die gemeinsam genutzten Speicherorte im Dateisystem sind:
    - `FSCommon`: `/shared/common`
    - `FS1`: `/shared/projects/project1`
    - `FS2`: `/shared/projects/project2`
- `WS1`- Eine Windows basierte Workstation, die für Projekt 1 verwendet wird. Die gemeinsam genutzten Speicherorte im Dateisystem sind:
    - `FSCommon`: `S:\`
    - `FS1`: `Z:\`
    - `FS2`: Nicht verfügbar

- `WS1`- Eine macOS basierte Workstation, die für Projekt 2 verwendet wird. Die Speicherorte des gemeinsam genutzten Dateisystems sind:
  - `FSCommon`: `/Volumes/common`
  - `FS1`: Nicht verfügbar
  - `FS2`: `/Volumes/projects/project2`

Definieren Sie abschließend die gemeinsam genutzten Dateisystemspeicherorte für die Mitarbeiter in Ihrer Flotte. Die folgenden Beispiele beziehen sich auf diese Konfiguration als`WorkerConfig`. Die gemeinsam genutzten Standorte sind:

- `FSCommon`: `/mnt/common`
- `FS1`: `/mnt/projects/project1`
- `FS2`: `/mnt/projects/project2`

Sie müssen keine gemeinsam genutzten Dateisysteme, Workstations oder Worker einrichten, die dieser Konfiguration entsprechen. Die gemeinsam genutzten Standorte müssen für die Demonstration nicht existieren.

Speicherprofile und Pfadzuweisung

Verwenden Sie Speicherprofile, um die Dateisysteme auf Ihrer Workstation und Ihren Worker-Hosts zu modellieren. Jedes Speicherprofil beschreibt das Betriebssystem und das Dateisystem-Layout einer Ihrer Systemkonfigurationen. In diesem Thema wird beschrieben, wie Sie Speicherprofile verwenden, um die Dateisystemkonfigurationen Ihrer Hosts zu modellieren, sodass Deadline Cloud Pfadzuordnungsregeln für Ihre Jobs generieren kann, und wie diese Pfadzuordnungsregeln aus Ihren Speicherprofilen generiert werden.

Wenn Sie einen Job an Deadline Cloud einreichen, können Sie eine optionale Speicherprofil-ID für den Job angeben. Dieses Speicherprofil beschreibt das Dateisystem der einreichenden Workstation. Es beschreibt die ursprüngliche Dateisystemkonfiguration, die von den Dateipfaden in der Jobvorlage verwendet wird.

Sie können einer Flotte auch ein Speicherprofil zuordnen. Das Speicherprofil beschreibt die Dateisystemkonfiguration aller Worker-Hosts in der Flotte. Wenn Sie über Mitarbeiter mit einer anderen Dateisystemkonfiguration verfügen, müssen diese Mitarbeiter einer anderen Flotte in Ihrer Farm zugewiesen werden.

Pfadzuordnungsregeln beschreiben, wie Pfade neu zugeordnet werden sollten, und zwar von der Art, wie sie im Job angegeben sind, bis zum tatsächlichen Speicherort des Pfads auf einem Worker-Host. Deadline Cloud vergleicht die im Speicherprofil eines Jobs beschriebene Dateisystemkonfiguration mit dem Speicherprofil der Flotte, die den Job ausführt, um diese Pfadzuordnungsregeln abzuleiten.

Themen

Modellieren Sie gemeinsam genutzte Dateisystemspeicherorte mit Speicherprofilen

Ein Speicherprofil modelliert die Dateisystemkonfiguration einer Ihrer Hostkonfigurationen. In der Beispielprojektinfrastruktur gibt es vier verschiedene Hostkonfigurationen. In diesem Beispiel erstellen Sie für jedes ein separates Speicherprofil. Sie können ein Speicherprofil mit einer der folgenden Methoden erstellen:

- CreateStorageProfile API
- AWS::Deadline::StorageProfile AWS CloudFormation Ressource
- AWS -Konsole

Ein Speicherprofil besteht aus einer Liste von Dateisystemspeicherorten, die Deadline Cloud jeweils den Speicherort und den Typ eines Dateisystemspeicherorts mitteilen, der für Jobs relevant ist, die von einem Host eingereicht oder auf einem Host ausgeführt werden. Ein Speicherprofil sollte nur die Standorte modellieren, die für Jobs relevant sind. Der gemeinsam genutzte `FSCommon` Speicherort befindet sich beispielsweise auf der Workstation `WS1` unter`S:\`, sodass der entsprechende Speicherort im Dateisystem wie folgt lautet:

```
{
    "name": "FSCommon",
    "path": "S:\\",
    "type": "SHARED"
}
```

Verwenden Sie die folgenden Befehle, um das Speicherprofil für Workstation-Konfigurationen `WS1` `WS3` und die Worker-Konfiguration `WorkerConfig` mithilfe von AWS CLIin zu erstellen AWS CloudShell: `WS2`

```
# Change the value of FARM_ID to your farm's identifier
FARM_ID=farm-00112233445566778899aabbccddeeff

aws deadline create-storage-profile --farm-id $FARM_ID \
  --display-name WSAll \
  --os-family LINUX \
  --file-system-locations \
  '[
      {"name": "FSCommon", "type":"SHARED", "path":"/shared/common"},
      {"name": "FS1", "type":"SHARED", "path":"/shared/projects/project1"},
      {"name": "FS2", "type":"SHARED", "path":"/shared/projects/project2"}
  ]'

aws deadline create-storage-profile --farm-id $FARM_ID \
  --display-name WS1 \
  --os-family WINDOWS \
  --file-system-locations \
  '[
      {"name": "FSCommon", "type":"SHARED", "path":"S:\\"},
      {"name": "FS1", "type":"SHARED", "path":"Z:\\"}
   ]'

aws deadline create-storage-profile --farm-id $FARM_ID \
  --display-name WS2 \
  --os-family MACOS \
  --file-system-locations \
  '[
      {"name": "FSCommon", "type":"SHARED", "path":"/Volumes/common"},
      {"name": "FS2", "type":"SHARED", "path":"/Volumes/projects/project2"}
  ]'

aws deadline create-storage-profile --farm-id $FARM_ID \
  --display-name WorkerCfg \
  --os-family LINUX \
  --file-system-locations \
  '[
      {"name": "FSCommon", "type":"SHARED", "path":"/mnt/common"},
      {"name": "FS1", "type":"SHARED", "path":"/mnt/projects/project1"},
      {"name": "FS2", "type":"SHARED", "path":"/mnt/projects/project2"}
```

```
  ]'
```

> **Note**
>
> Sie müssen auf die Dateisystemspeicherorte in Ihren Speicherprofilen verweisen und dabei dieselben Werte für die `name` Eigenschaft in allen Speicherprofilen in Ihrer Farm verwenden. Deadline Cloud vergleicht die Namen, um festzustellen, dass Dateisystemspeicherorte aus verschiedenen Speicherprofilen auf denselben Speicherort verweisen, wenn Pfadzuordnungsregeln generiert werden.

Konfigurieren Sie Speicherprofile für Flotten

Sie können eine Flotte so konfigurieren, dass sie ein Speicherprofil enthält, das die Dateisystemstandorte aller Mitarbeiter in der Flotte modelliert. Die Host-Dateisystemkonfiguration aller Mitarbeiter in einer Flotte muss dem Speicherprofil ihrer Flotte entsprechen. Mitarbeiter mit unterschiedlichen Dateisystemkonfigurationen müssen sich in separaten Flotten befinden.

Um die Konfiguration Ihrer Flotte für die Verwendung des `WorkerConfig` Speicherprofils festzulegen, verwenden Sie den folgenden Befehl AWS CLI: AWS CloudShell

```
# Change the value of FARM_ID to your farm's identifier
FARM_ID=farm-00112233445566778899aabbccddeeff
# Change the value of FLEET_ID to your fleet's identifier
FLEET_ID=fleet-00112233445566778899aabbccddeeff
# Change the value of WORKER_CFG_ID to your storage profile named WorkerConfig
WORKER_CFG_ID=sp-00112233445566778899aabbccddeeff

FLEET_WORKER_MODE=$( \
  aws deadline get-fleet --farm-id $FARM_ID --fleet-id $FLEET_ID \
   --query '.configuration.customerManaged.mode' \
)
FLEET_WORKER_CAPABILITIES=$( \
  aws deadline get-fleet --farm-id $FARM_ID --fleet-id $FLEET_ID \
   --query '.configuration.customerManaged.workerCapabilities' \
)

aws deadline update-fleet --farm-id $FARM_ID --fleet-id $FLEET_ID \
  --configuration \
  "{
    \"customerManaged\": {
```

```
      \"storageProfileId\": \"$WORKER_CFG_ID\",
      \"mode\": $FLEET_WORKER_MODE,
      \"workerCapabilities\": $FLEET_WORKER_CAPABILITIES
    }
  }"
```

Konfigurieren Sie Speicherprofile für Warteschlangen

Die Konfiguration einer Warteschlange umfasst eine Liste von Namen der gemeinsam genutzten Dateisystemspeicherorte, auf die an die Warteschlange übermittelte Jobs Zugriff benötigen, wobei Groß- und Kleinschreibung beachtet werden muss. Beispielsweise erfordern an die Warteschlange übermittelte Jobs `Q1` Dateisystemspeicherorte und. `FSCommon` `FS1` Für an die Warteschlange übermittelte Jobs `Q2` sind Dateisystemspeicherorte `FSCommon` und erforderlich. `FS2`

Verwenden Sie das folgende Skript, um die Konfigurationen der Warteschlange so einzustellen, dass diese Dateisystemspeicherorte erforderlich sind:

```
# Change the value of FARM_ID to your farm's identifier
FARM_ID=farm-00112233445566778899aabbccddeeff
# Change the value of QUEUE1_ID to queue Q1's identifier
QUEUE1_ID=queue-00112233445566778899aabbccddeeff
# Change the value of QUEUE2_ID to queue Q2's identifier
QUEUE2_ID=queue-00112233445566778899aabbccddeeff

aws deadline update-queue --farm-id $FARM_ID --queue-id $QUEUE1_ID \
  --required-file-system-location-names-to-add FSComm FS1

aws deadline update-queue --farm-id $FARM_ID --queue-id $QUEUE2_ID \
  --required-file-system-location-names-to-add FSComm FS2
```

Die Konfiguration einer Warteschlange umfasst auch eine Liste der zulässigen Speicherprofile, die für Aufträge gilt, die an diese Warteschlange weitergeleitet wurden, und für Flotten, die dieser Warteschlange zugeordnet sind. In der Liste der zulässigen Speicherprofile der Warteschlange sind nur Speicherprofile zulässig, die Dateisystemspeicherorte für alle erforderlichen Dateisystemspeicherorte für die Warteschlange definieren.

Ein Job schlägt fehl, wenn Sie ihn mit einem Speicherprofil einreichen, das nicht in der Liste der zulässigen Speicherprofile für die Warteschlange enthalten ist. Sie können einen Job ohne Speicherprofil jederzeit an eine Warteschlange senden. Die Workstation-Konfigurationen sind beschriftet `WSAll` und `WS1` beide verfügen über die erforderlichen Dateisystemspeicherorte

(FSCommonundFS1) für die WarteschlangeQ1. Sie müssen berechtigt sein, Jobs an die Warteschlange weiterzuleiten. Ebenso müssen die WSAll Workstation-Konfigurationen die WS2 Anforderungen für die Warteschlange erfüllenQ2. Sie müssen in der Lage sein, Jobs an diese Warteschlange weiterzuleiten. Aktualisieren Sie beide Warteschlangenkonfigurationen, sodass Jobs mit diesen Speicherprofilen mithilfe des folgenden Skripts gesendet werden können:

```
# Change the value of WSALL_ID to the identifier of the WSAll storage profile
WSALL_ID=sp-00112233445566778899aabbccddeeff
# Change the value of WS1 to the identifier of the WS1 storage profile
WS1_ID=sp-00112233445566778899aabbccddeeff
# Change the value of WS2 to the identifier of the WS2 storage profile
WS2_ID=sp-00112233445566778899aabbccddeeff

aws deadline update-queue --farm-id $FARM_ID --queue-id $QUEUE1_ID \
  --allowed-storage-profile-ids-to-add $WSALL_ID $WS1_ID

aws deadline update-queue --farm-id $FARM_ID --queue-id $QUEUE2_ID \
  --allowed-storage-profile-ids-to-add $WSALL_ID $WS2_ID
```

Wenn Sie das WS2 Speicherprofil zur Liste der zulässigen Speicherprofile für die Warteschlange hinzufügen, schlägt Q1 dies fehl:

```
$ aws deadline update-queue --farm-id $FARM_ID --queue-id $QUEUE1_ID \
  --allowed-storage-profile-ids-to-add $WS2_ID

An error occurred (ValidationException) when calling the UpdateQueue operation: Storage
 profile id: sp-00112233445566778899aabbccddeeff does not have required file system
 location: FS1
```

Das liegt daran, dass das WS2 Speicherprofil keine Definition für den Dateisystemspeicherort enthältFS1, den diese Warteschlange Q1 benötigt.

Das Zuordnen einer konfigurierten Flotte zu einem Speicherprofil, das nicht in der Liste der zulässigen Speicherprofile der Warteschlange enthalten ist, schlägt ebenfalls fehl. Zum Beispiel:

```
$ aws deadline create-queue-fleet-association --farm-id $FARM_ID \
   --fleet-id $FLEET_ID \
   --queue-id $QUEUE1_ID

An error occurred (ValidationException) when calling the CreateQueueFleetAssociation
 operation: Mismatch between storage profile ids.
```

Um den Fehler zu beheben, fügen Sie das angegebene Speicherprofil der Liste der zulässigen Speicherprofile sowohl für die Warteschlange als auch für die Warteschlange `Q1` hinzu. `WorkerConfig` `Q2` Ordnen Sie dann die Flotte diesen Warteschlangen zu, sodass die Mitarbeiter der Flotte Aufträge aus beiden Warteschlangen ausführen können.

```
# Change the value of FLEET_ID to your fleet's identifier
FLEET_ID=fleet-00112233445566778899aabbccddeeff
# Change the value of WORKER_CFG_ID to your storage profile named WorkerCfg
WORKER_CFG_ID=sp-00112233445566778899aabbccddeeff

aws deadline update-queue --farm-id $FARM_ID --queue-id $QUEUE1_ID \
  --allowed-storage-profile-ids-to-add $WORKER_CFG_ID

aws deadline update-queue --farm-id $FARM_ID --queue-id $QUEUE2_ID \
  --allowed-storage-profile-ids-to-add $WORKER_CFG_ID

aws deadline create-queue-fleet-association --farm-id $FARM_ID \
  --fleet-id $FLEET_ID \
  --queue-id $QUEUE1_ID

aws deadline create-queue-fleet-association --farm-id $FARM_ID \
  --fleet-id $FLEET_ID \
  --queue-id $QUEUE2_ID
```

Leiten Sie Pfadzuordnungsregeln aus Speicherprofilen ab

Pfadzuordnungsregeln beschreiben, wie Pfade vom Job zum tatsächlichen Speicherort des Pfads auf einem Worker-Host neu zugeordnet werden sollten. Wenn eine Aufgabe auf einem Worker ausgeführt wird, wird das Speicherprofil des Jobs mit dem Speicherprofil der Worker-Flotte verglichen, um die Pfadzuordnungsregeln für die Aufgabe abzuleiten.

Deadline Cloud erstellt eine Zuordnungsregel für jeden der erforderlichen Dateisystemspeicherorte in der Konfiguration der Warteschlange. Beispielsweise hat ein Job, der mit dem `WSAll` Speicherprofil an die Warteschlange gesendet `Q1` wurde, die Pfadzuordnungsregeln:

- `FSComm`: `/shared/common -> /mnt/common`
- `FS1`: `/shared/projects/project1 -> /mnt/projects/project1`

Deadline Cloud erstellt Regeln für die Speicherorte `FSComm` und das `FS1` Dateisystem, aber nicht für den Speicherort des `FS2` Dateisystems, obwohl `WSAll` sowohl die `WorkerConfig`

Speicherprofile als auch diese definierenFS2. Dies liegt daran, dass die Liste Q1 der erforderlichen Dateisystemspeicherorte in der Warteschlange lautet`["FSComm", "FS1"]`.

Sie können die Pfadzuordnungsregeln überprüfen, die für Jobs verfügbar sind, die mit einem bestimmten Speicherprofil eingereicht wurden, indem Sie einen Job einreichen, der die Datei mit den Pfadzuordnungsregeln von Open Job Description ausdruckt, und dann das Sitzungsprotokoll lesen, nachdem der Job abgeschlossen ist:

```
# Change the value of FARM_ID to your farm's identifier
FARM_ID=farm-00112233445566778899aabbccddeeff
# Change the value of QUEUE1_ID to queue Q1's identifier
QUEUE1_ID=queue-00112233445566778899aabbccddeeff
# Change the value of WSALL_ID to the identifier of the WSALL storage profile
WSALL_ID=sp-00112233445566778899aabbccddeeff

aws deadline create-job --farm-id $FARM_ID --queue-id $QUEUE1_ID \
  --priority 50 \\
  --storage-profile-id $WSALL_ID \
  --template-type JSON --template \
  '{
    "specificationVersion": "jobtemplate-2023-09",
    "name": "DemoPathMapping",
    "steps": [
      {
        "name": "ShowPathMappingRules",
        "script": {
          "actions": {
            "onRun": {
              "command": "/bin/cat",
              "args": [ "{{Session.PathMappingRulesFile}}" ]
            }
          }
        }
      }
    ]
  }'
```

Wenn Sie die Deadline Cloud-CLI zum Senden von Jobs verwenden, legt deren `settings.storage_profile_id` Konfigurationseinstellung das Speicherprofil fest, das mit der CLI eingereichte Jobs haben. Um Jobs mit dem `WSAll` Speicherprofil einzureichen, legen Sie Folgendes fest:

```
deadline config set settings.storage_profile_id $WSALL_ID
```

Um einen vom Kunden verwalteten Worker so auszuführen, als ob er in der Beispielinfrastruktur ausgeführt würde, folgen Sie dem Verfahren unter Den Worker-Agent ausführen im Deadline Cloud-Benutzerhandbuch, um einen Worker auszuführen. AWS CloudShell Wenn Sie diese Anweisungen bereits befolgt haben, löschen Sie zuerst die `~/demoenv-persist` Verzeichnisse `~/demoenv-logs` und. Legen Sie vorher auch die Werte der `DEV_CMF_ID` Umgebungsvariablen `DEV_FARM_ID` und, auf die sich die Anweisungen beziehen, wie folgt fest:

```
DEV_FARM_ID=$FARM_ID
DEV_CMF_ID=$FLEET_ID
```

Nach der Ausführung des Jobs können Sie die Pfadzuordnungsregeln in der Protokolldatei des Jobs sehen:

```
cat demoenv-logs/${QUEUE1_ID}/*.log
...
JJSON log results (see below)
...
```

Das Protokoll enthält Zuordnungen sowohl für das `FS1` als auch für das `FSComm` Dateisystem. Der Protokolleintrag wurde aus Gründen der Lesbarkeit neu formatiert und sieht wie folgt aus:

```
{
    "version": "pathmapping-1.0",
    "path_mapping_rules": [
        {
            "source_path_format": "POSIX",
            "source_path": "/shared/projects/project1",
            "destination_path": "/mnt/projects/project1"
        },
        {
            "source_path_format": "POSIX",
            "source_path": "/shared/common",
            "destination_path": "/mnt/common"
        }
    ]
```

Sie können Jobs mit unterschiedlichen Speicherprofilen einreichen, um zu sehen, wie sich die Pfadzuordnungsregeln ändern.

Verwenden Sie Jobanhänge, um Dateien zu teilen

Verwenden Sie Jobanhänge, um Dateien, die sich nicht in gemeinsam genutzten Verzeichnissen befinden, für Ihre Jobs verfügbar zu machen und die Ausgabedateien zu erfassen, falls sie nicht in gemeinsam genutzte Verzeichnisse geschrieben wurden. Job Attachments verwendet Amazon S3, um Dateien zwischen Hosts zu übertragen. Dateien werden in S3-Buckets gespeichert, und Sie müssen eine Datei nicht hochladen, wenn sich ihr Inhalt nicht geändert hat.

Sie müssen Auftragsanhänge verwenden, wenn Sie Jobs auf vom Service verwalteten Flotten ausführen, da Hosts die Speicherorte im Dateisystem nicht gemeinsam nutzen. Jobanhänge sind auch für vom Kunden verwaltete Flotten nützlich, wenn die Eingabe- oder Ausgabedateien eines Jobs in einem gemeinsam genutzten Netzwerkdateisystem gespeichert sind, z. B. wenn Ihr Auftragspaket Shell- oder Python-Skripte enthält.

Wenn Sie ein Job-Bundle entweder mit der Deadline Cloud-CLI oder einem Deadline Cloud-Absender einreichen, verwenden Jobanhänge das Speicherprofil des Jobs und die erforderlichen Dateisystemspeicherorte der Warteschlange, um die Eingabedateien zu identifizieren, die sich nicht auf einem Worker-Host befinden und im Rahmen der Auftragsübermittlung auf Amazon S3 hochgeladen werden sollten. Diese Speicherprofile helfen Deadline Cloud auch dabei, die Ausgabedateien an Worker-Host-Standorten zu identifizieren, die auf Amazon S3 hochgeladen werden müssen, damit sie auf Ihrer Workstation verfügbar sind.

Die Beispiele für Jobanhänge verwenden die Konfigurationen für Farm, Flotte, Warteschlangen und Speicherprofile von Beispiel für eine Projektinfrastruktur undSpeicherprofile und Pfadzuweisung. Sie sollten diese Abschnitte vor diesem durchgehen.

In den folgenden Beispielen verwenden Sie ein Beispiel-Job-Bundle als Ausgangspunkt und ändern es dann, um die Funktionalität von Job Attachment zu untersuchen. Job-Bundles sind die beste Methode, um Job-Anhänge für Ihre Jobs zu verwenden. Sie kombinieren eine Jobvorlage „Open Job Description“ in einem Verzeichnis mit zusätzlichen Dateien, in denen die Dateien und Verzeichnisse aufgeführt sind, die für Jobs benötigt werden, die das Job-Bundle verwenden. Weitere Informationen zu Jobpaketen finden Sie unterVorlagen für offene Stellenbeschreibungen (OpenJD) für Deadline Cloud.

Dateien mit einem Job einreichen

Mit Deadline Cloud können Sie Job-Workflows für den Zugriff auf Eingabedateien aktivieren, die an gemeinsam genutzten Dateisystemen auf Worker-Hosts nicht verfügbar sind. Mit Auftragsanhängen

können Renderaufträge auf Dateien zugreifen, die sich nur auf einem lokalen Workstation-Laufwerk oder in einer vom Service verwalteten Flottenumgebung befinden. Wenn Sie ein Auftragspaket einreichen, können Sie Listen mit Eingabedateien und Verzeichnissen hinzufügen, die für den Job erforderlich sind. Deadline Cloud identifiziert diese nicht gemeinsam genutzten Dateien, lädt sie vom lokalen Computer auf Amazon S3 hoch und lädt sie auf den Worker-Host herunter. Es optimiert den Prozess der Übertragung von Eingabe-Assets an Renderknoten und stellt sicher, dass alle erforderlichen Dateien für die verteilte Auftragsausführung zugänglich sind.

Sie können die Dateien für Jobs direkt im Job-Bundle angeben, Parameter in der Jobvorlage verwenden, die Sie mithilfe von Umgebungsvariablen oder einem Skript bereitstellen, und die `assets_references` Datei des Jobs verwenden. Sie können eine dieser Methoden oder eine Kombination aus allen dreien verwenden. Sie können ein Speicherprofil für das Paket für den Job angeben, sodass nur Dateien hochgeladen werden, die sich auf der lokalen Arbeitsstation geändert haben.

In diesem Abschnitt wird anhand eines Beispiel-Job-Bundles von GitHub gezeigt, wie Deadline Cloud die Dateien in Ihrem Job zum Hochladen identifiziert, wie diese Dateien in Amazon S3 organisiert sind und wie sie den Worker-Hosts zur Verfügung gestellt werden, die Ihre Jobs verarbeiten.

Themen

- So lädt Deadline Cloud Dateien auf Amazon S3 hoch
- Wie Deadline Cloud die hochzuladenden Dateien auswählt
- Wie finden Jobs Eingabedateien für Jobanhänge

So lädt Deadline Cloud Dateien auf Amazon S3 hoch

Dieses Beispiel zeigt, wie Deadline Cloud Dateien von Ihrer Workstation oder Ihrem Worker-Host auf Amazon S3 hochlädt, damit sie gemeinsam genutzt werden können. Es verwendet ein Beispiel-Job-Bundle von GitHub und die Deadline Cloud-CLI, um Jobs einzureichen.

Klonen Sie zunächst das Deadline GitHub Cloud-Beispiel-Repository in Ihre AWS CloudShellUmgebung und kopieren Sie dann das `job_attachments_devguide` Job-Bundle in Ihr Home-Verzeichnis:

```
git clone https://github.com/aws-deadline/deadline-cloud-samples.git
cp -r deadline-cloud-samples/job_bundles/job_attachments_devguide ~/
```

Installieren Sie die Deadline Cloud-CLI, um Job-Bundles einzureichen:

```
pip install deadline --upgrade
```

Das `job_attachments_devguide` Job-Bundle besteht aus einem einzigen Schritt mit einer Aufgabe, die ein Bash-Shell-Skript ausführt, dessen Dateisystemspeicherort als Jobparameter übergeben wird. Die Definition des Job-Parameters lautet:

```
...
- name: ScriptFile
  type: PATH
  default: script.sh
  dataFlow: IN
  objectType: FILE
...
```

Der `IN` Wert der `dataFlow` Eigenschaft teilt Job-Anhängen mit, dass der Wert des `ScriptFile` Parameters eine Eingabe für den Job ist. Der Wert der `default` Eigenschaft ist ein relativer Speicherort zum Verzeichnis des Job-Bundles, es kann sich aber auch um einen absoluten Pfad handeln. Diese Parameterdefinition deklariert die `script.sh` Datei im Verzeichnis des Job-Bundles als Eingabedatei, die für die Ausführung des Jobs erforderlich ist.

Stellen Sie als Nächstes sicher, dass für die Deadline Cloud-CLI kein Speicherprofil konfiguriert ist, und senden Sie den Job dann in die WarteschlangeQ1:

```
# Change the value of FARM_ID to your farm's identifier
FARM_ID=farm-00112233445566778899aabbccddeeff
# Change the value of QUEUE1_ID to queue Q1's identifier
QUEUE1_ID=queue-00112233445566778899aabbccddeeff

deadline config set settings.storage_profile_id ''

deadline bundle submit --farm-id $FARM_ID --queue-id $QUEUE1_ID
 job_attachments_devguide/
```

Die Ausgabe der Deadline Cloud-CLI nach der Ausführung dieses Befehls sieht wie folgt aus:

```
Submitting to Queue: Q1
...
Hashing Attachments  [####################################]  100%
Hashing Summary:
    Processed 1 file totaling 39.0 B.
```

```
    Skipped re-processing 0 files totaling 0.0 B.
    Total processing time of 0.0327 seconds at 1.19 KB/s.

Uploading Attachments  [####################################]  100%
Upload Summary:
    Processed 1 file totaling 39.0 B.
    Skipped re-processing 0 files totaling 0.0 B.
    Total processing time of 0.25639 seconds at 152.0 B/s.

Waiting for Job to be created...
Submitted job bundle:
   job_attachments_devguide/
Job creation completed successfully
job-74148c13342e4514b63c7a7518657005
```

Wenn Sie den Job einreichen, hascht Deadline Cloud die `script.sh` Datei zuerst und lädt sie dann auf Amazon S3 hoch.

Deadline Cloud behandelt den S3-Bucket als inhaltsadressierbaren Speicher. Dateien werden in S3-Objekte hochgeladen. Der Objektname wird aus einem Hash des Dateiinhalts abgeleitet. Wenn zwei Dateien identischen Inhalt haben, haben sie unabhängig davon, wo sich die Dateien befinden oder wie sie benannt sind, denselben Hashwert. Dadurch kann Deadline Cloud vermeiden, dass eine Datei hochgeladen wird, wenn sie bereits verfügbar ist.

Sie können die AWS-CLI verwenden, um die Objekte zu sehen, die auf Amazon S3 hochgeladen wurden:

```
# The name of queue `Q1``s job attachments S3 bucket
Q1_S3_BUCKET=$(
  aws deadline get-queue --farm-id $FARM_ID --queue-id $QUEUE1_ID \
    --query 'jobAttachmentSettings.s3BucketName' | tr -d '"'
)

aws s3 ls s3://$Q1_S3_BUCKET --recursive
```

Zwei Objekte wurden auf S3 hochgeladen:

- `DeadlineCloud/Data/87cb19095dd5d78fcaf56384ef0e6241.xxh128`— Der Inhalt von`script.sh`. Der Wert `87cb19095dd5d78fcaf56384ef0e6241` im Objektschlüssel ist der Hash des Dateiinhalts, und die Erweiterung `xxh128` gibt an, dass der Hashwert als 128-Bit-xxhash berechnet wurde.

- `DeadlineCloud/Manifests/<farm-id>/<queue-id>/Inputs/<guid>/a1d221c7fd97b08175b3872a37428e8c_input`— Das Manifest-Objekt für die Auftragsübergabe. Die Werte `<farm-id>`<queue-id>, und `<guid>` sind Ihre Farm-ID, Ihre Warteschlangen-ID und ein zufälliger Hexadezimalwert. Der Wert `a1d221c7fd97b08175b3872a37428e8c` in diesem Beispiel ist ein Hashwert, der anhand der Zeichenfolge`/home/cloudshell-user/job_attachments_devguide`, dem Verzeichnis, in dem er sich `script.sh` befindet, berechnet wird.

Das Manifest-Objekt enthält die Informationen für die Eingabedateien in einem bestimmten Stammpfad, die im Rahmen der Auftragsübermittlung auf S3 hochgeladen wurden. Laden Sie diese Manifestdatei herunter (`aws s3 cp s3://$Q1_S3_BUCKET/<objectname>`). Ihr Inhalt ist ähnlich wie:

```
{
    "hashAlg": "xxh128",
    "manifestVersion": "2023-03-03",
    "paths": [
        {
            "hash": "87cb19095dd5d78fcaf56384ef0e6241",
            "mtime": 1721147454416085,
            "path": "script.sh",
            "size": 39
        }
    ],
    "totalSize": 39
}
```

Dies bedeutet, dass die Datei hochgeladen `script.sh` wurde, und der Hash des Inhalts dieser Datei lautet`87cb19095dd5d78fcaf56384ef0e6241`. Dieser Hashwert entspricht dem Wert im Objektnamen`DeadlineCloud/Data/87cb19095dd5d78fcaf56384ef0e6241.xxh128`. Es wird von Deadline Cloud verwendet, um zu wissen, welches Objekt für den Inhalt dieser Datei heruntergeladen werden muss.

Das vollständige Schema für diese Datei ist verfügbar in GitHub.

Wenn Sie den CreateJob Vorgang verwenden, können Sie den Speicherort der Manifestobjekte festlegen. Sie können die GetJobOperation verwenden, um den Standort zu sehen:

```
{
```

```
    "attachments": {
        "file system": "COPIED",
        "manifests": [
            {
                "inputManifestHash": "5b0db3d311805ea8de7787b64cbbe8b3",
                "inputManifestPath": "<farm-id>/<queue-id>/Inputs/<guid>/
a1d221c7fd97b08175b3872a37428e8c_input",
                "rootPath": "/home/cloudshell-user/job_attachments_devguide",
                "rootPathFormat": "posix"
            }
        ]
    },
    ...
}
```

Wie Deadline Cloud die hochzuladenden Dateien auswählt

Die Dateien und Verzeichnisse, die Job Attachments für den Upload auf Amazon S3 als Eingaben für Ihren Job in Betracht ziehen, sind:

- Die Werte aller Jobparameter `PATH` vom Typ -type, die in der Jobvorlage des Job-Bundles mit dem `dataFlow` Wert `IN` oder `INOUT` definiert sind.
- Die Dateien und Verzeichnisse, die als Eingaben in der Asset-Referenzdatei des Job-Bundles aufgeführt sind.

Wenn Sie einen Job ohne Speicherprofil einreichen, werden alle Dateien hochgeladen, die für den Upload in Frage kommen. Wenn Sie einen Job mit einem Speicherprofil einreichen, werden Dateien nicht auf Amazon S3 hochgeladen, wenn sie sich in den Dateisystemspeicherorten des Speicherprofils `SHARED` vom Typ -type befinden, die auch erforderliche Dateisystemspeicherorte für die Warteschlange sind. Es wird davon ausgegangen, dass diese Speicherorte auf den Worker-Hosts verfügbar sind, auf denen der Job ausgeführt wird, sodass sie nicht auf S3 hochgeladen werden müssen.

In diesem Beispiel erstellen Sie `SHARED` Dateisystemspeicherorte `WSAll` in Ihrer CloudShell AWS-Umgebung und fügen dann Dateien zu diesen Dateisystemspeicherorten hinzu. Verwenden Sie den folgenden Befehl:

```
# Change the value of WSALL_ID to the identifier of the WSAll storage profile
WSALL_ID=sp-00112233445566778899aabbccddeeff
```

```
sudo mkdir -p /shared/common /shared/projects/project1 /shared/projects/project2
sudo chown -R cloudshell-user:cloudshell-user /shared

for d in /shared/common /shared/projects/project1 /shared/projects/project2; do
  echo "File contents for $d" > ${d}/file.txt
done
```

Als Nächstes fügen Sie dem Job-Bundle eine Asset-Referenzdatei hinzu, die alle Dateien enthält, die Sie als Eingaben für den Job erstellt haben. Verwenden Sie den folgenden Befehl:

```
cat > ${HOME}/job_attachments_devguide/asset_references.yaml << EOF
assetReferences:
  inputs:
    filenames:
    - /shared/common/file.txt
    directories:
    - /shared/projects/project1
    - /shared/projects/project2
EOF
```

Als Nächstes konfigurieren Sie die Deadline Cloud-CLI so, dass Jobs mit dem `WSAll` Speicherprofil gesendet werden, und senden Sie dann das Job-Bundle:

```

# Change the value of FARM_ID to your farm's identifier
FARM_ID=farm-00112233445566778899aabbccddeeff
# Change the value of QUEUE1_ID to queue Q1's identifier
QUEUE1_ID=queue-00112233445566778899aabbccddeeff
# Change the value of WSALL_ID to the identifier of the WSAll storage profile
WSALL_ID=sp-00112233445566778899aabbccddeeff

deadline config set settings.storage_profile_id $WSALL_ID

deadline bundle submit --farm-id $FARM_ID --queue-id $QUEUE1_ID
 job_attachments_devguide/
```

Deadline Cloud lädt zwei Dateien auf Amazon S3 hoch, wenn Sie den Job einreichen. Sie können die Manifestobjekte für den Job von S3 herunterladen, um die hochgeladenen Dateien zu sehen:

```
for manifest in $( \
  aws deadline get-job --farm-id $FARM_ID --queue-id $QUEUE1_ID --job-id $JOB_ID \
```

```
    --query 'attachments.manifests[].inputManifestPath' \
    | jq -r '.[]'
); do
  echo "Manifest object: $manifest"
  aws s3 cp --quiet s3://$Q1_S3_BUCKET/DeadlineCloud/Manifests/$manifest /dev/stdout |
 jq .
done
```

In diesem Beispiel gibt es eine einzelne Manifestdatei mit dem folgenden Inhalt:

```
{
    "hashAlg": "xxh128",
    "manifestVersion": "2023-03-03",
    "paths": [
        {
            "hash": "87cb19095dd5d78fcaf56384ef0e6241",
            "mtime": 1721147454416085,
            "path": "home/cloudshell-user/job_attachments_devguide/script.sh",
            "size": 39
        },
        {
            "hash": "af5a605a3a4e86ce7be7ac5237b51b79",
            "mtime": 1721163773582362,
            "path": "shared/projects/project2/file.txt",
            "size": 44
        }
    ],
    "totalSize": 83
}
```

Verwenden Sie die GetJob Operation für das Manifest, um zu überprüfen, ob der „/“ `rootPath` ist.

```
aws deadline get-job --farm-id $FARM_ID --queue-id $QUEUE1_ID --job-id $JOB_ID --query
 'attachments.manifests[*]'
```

Der Stammpfad für eine Reihe von Eingabedateien ist immer der längste gemeinsame Unterpfad dieser Dateien. Wenn Ihr Job eingereicht wurde von Windows Stattdessen und wenn es Eingabedateien ohne gemeinsamen Unterpfad gibt, weil sie sich auf unterschiedlichen Laufwerken befanden, wird auf jedem Laufwerk ein eigener Stammpfad angezeigt. Die Pfade in einem Manifest beziehen sich immer auf den Stammpfad des Manifests. Es wurden also folgende Eingabedateien hochgeladen:

- `/home/cloudshell-user/job_attachments_devguide/script.sh`— Die Skriptdatei im Job-Bundle.
- `/shared/projects/project2/file.txt`— Die Datei an einem `SHARED` Dateisystemspeicherort im `WSAll` Speicherprofil, der nicht in der Liste der erforderlichen Dateisystemspeicherorte für die Warteschlange enthalten ist`Q1`.

Die Dateien an den Dateisystemspeicherorten `FSCommon` (`/shared/common/file.txt`) und `FS1` (`/shared/projects/project1/file.txt`) sind nicht in der Liste enthalten. Dies liegt daran, dass sich diese Dateisystemspeicherorte `SHARED` im `WSAll` Speicherprofil und beide in der Liste der erforderlichen Dateisystemspeicherorte in der Warteschlange befinden`Q1`.

Sie können die Dateisystemspeicherorte sehen, die `SHARED` für einen Job berücksichtigt wurden, der mit einem bestimmten Speicherprofil im Rahmen des GetStorageProfileForQueue Vorgangs eingereicht wird. `Q1`Verwenden Sie den folgenden Befehl, um das Speicherprofil `WSAll` für die Warteschlange abzufragen:

```
aws deadline get-storage-profile --farm-id $FARM_ID --storage-profile-id $WSALL_ID

aws deadline get-storage-profile-for-queue --farm-id $FARM_ID --queue-id $QUEUE1_ID --
storage-profile-id $WSALL_ID
```

Wie finden Jobs Eingabedateien für Jobanhänge

Damit ein Job die Dateien verwenden kann, die Deadline Cloud mithilfe von Job-Anhängen auf Amazon S3 hochlädt, benötigt Ihr Job diese Dateien, die über das Dateisystem auf den Worker-Hosts verfügbar sind. Wenn eine Sitzung für Ihren Job auf einem Worker-Host läuft, lädt Deadline Cloud die Eingabedateien für den Job in ein temporäres Verzeichnis auf dem lokalen Laufwerk des Worker-Hosts herunter und fügt Pfadzuordnungsregeln für jeden Root-Pfad des Jobs zu seinem Dateisystem-Speicherort auf dem lokalen Laufwerk hinzu.

Starten Sie für dieses Beispiel den Deadline Cloud-Worker-Agent auf einer CloudShell AWS-Tab. Lassen Sie alle zuvor eingereichten Jobs fertig laufen und löschen Sie dann die Job-Logs aus dem Logs-Verzeichnis:

```
rm -rf ~/devdemo-logs/queue-*
```

Das folgende Skript ändert das Auftragspaket so, dass es alle Dateien im temporären Arbeitsverzeichnis der Sitzung und den Inhalt der Datei mit den Pfadzuordnungsregeln anzeigt, und sendet dann einen Job mit dem geänderten Paket:

```
# Change the value of FARM_ID to your farm's identifier
FARM_ID=farm-00112233445566778899aabbccddeeff
# Change the value of QUEUE1_ID to queue Q1's identifier
QUEUE1_ID=queue-00112233445566778899aabbccddeeff
# Change the value of WSALL_ID to the identifier of the WSAll storage profile
WSALL_ID=sp-00112233445566778899aabbccddeeff

deadline config set settings.storage_profile_id $WSALL_ID

cat > ~/job_attachments_devguide/script.sh << EOF
#!/bin/bash

echo "Session working directory is: \$(pwd)"
echo
echo "Contents:"
find . -type f
echo
echo "Path mapping rules file: \$1"
jq . \$1
EOF

cat > ~/job_attachments_devguide/template.yaml << EOF
specificationVersion: jobtemplate-2023-09
name: "Job Attachments Explorer"
parameterDefinitions:
- name: ScriptFile
  type: PATH
  default: script.sh
  dataFlow: IN
  objectType: FILE
steps:
- name: Step
  script:
    actions:
      onRun:
        command: /bin/bash
        args:
        - "{{Param.ScriptFile}}"
        - "{{Session.PathMappingRulesFile}}"
```

```
EOF

deadline bundle submit --farm-id $FARM_ID --queue-id $QUEUE1_ID
 job_attachments_devguide/
```

Sie können sich das Protokoll der Ausführung des Jobs ansehen, nachdem er vom Worker in Ihrer AWS CloudShell Umgebung ausgeführt wurde:

```
cat demoenv-logs/queue-*/session*.log
```

Aus dem Protokoll geht hervor, dass in der Sitzung als Erstes die beiden Eingabedateien für den Job auf den Worker heruntergeladen werden:

```
2024-07-17 01:26:37,824 INFO ================================================
2024-07-17 01:26:37,825 INFO --------- Job Attachments Download for Job
2024-07-17 01:26:37,825 INFO ================================================
2024-07-17 01:26:37,825 INFO Syncing inputs using Job Attachments
2024-07-17 01:26:38,116 INFO Downloaded 142.0 B / 186.0 B of 2 files (Transfer rate:
 0.0 B/s)
2024-07-17 01:26:38,174 INFO Downloaded 186.0 B / 186.0 B of 2 files (Transfer rate:
 733.0 B/s)
2024-07-17 01:26:38,176 INFO Summary Statistics for file downloads:
Processed 2 files totaling 186.0 B.
Skipped re-processing 0 files totaling 0.0 B.
Total processing time of 0.09752 seconds at 1.91 KB/s.
```

Als Nächstes folgt die Ausgabe von `script.sh` run by the job:

- Die Eingabedateien, die beim Absenden des Jobs hochgeladen wurden, befinden sich in einem Verzeichnis, dessen Name mit „assetroot“ beginnt, im temporären Verzeichnis der Sitzung.
- Die Pfade der Eingabedateien wurden relativ zum Verzeichnis „assetroot“ verschoben und nicht relativ zum Stammpfad für das Eingabemanifest des Jobs (). `"/"`
- Die Datei mit den Regeln für die Pfadzuweisung enthält eine zusätzliche Regel, die dem absoluten Pfad des `"/"` Verzeichnisses „assetroot“ neu zugeordnet wird.

Zum Beispiel:

```
2024-07-17 01:26:38,264 INFO Output:
2024-07-17 01:26:38,267 INFO Session working directory is: /sessions/session-5b33f
```

```
2024-07-17 01:26:38,267 INFO
2024-07-17 01:26:38,267 INFO Contents:
2024-07-17 01:26:38,269 INFO ./tmp_xdhbsdo.sh
2024-07-17 01:26:38,269 INFO ./tmpdi00052b.json
2024-07-17 01:26:38,269 INFO ./assetroot-assetroot-3751a/shared/projects/project2/
file.txt
2024-07-17 01:26:38,269 INFO ./assetroot-assetroot-3751a/home/cloudshell-user/
job_attachments_devguide/script.sh
2024-07-17 01:26:38,269 INFO
2024-07-17 01:26:38,270 INFO Path mapping rules file: /sessions/session-5b33f/
tmpdi00052b.json
2024-07-17 01:26:38,282 INFO {
2024-07-17 01:26:38,282 INFO   "version": "pathmapping-1.0",
2024-07-17 01:26:38,282 INFO   "path_mapping_rules": [
2024-07-17 01:26:38,282 INFO     {
2024-07-17 01:26:38,282 INFO       "source_path_format": "POSIX",
2024-07-17 01:26:38,282 INFO       "source_path": "/shared/projects/project1",
2024-07-17 01:26:38,283 INFO       "destination_path": "/mnt/projects/project1"
2024-07-17 01:26:38,283 INFO     },
2024-07-17 01:26:38,283 INFO     {
2024-07-17 01:26:38,283 INFO       "source_path_format": "POSIX",
2024-07-17 01:26:38,283 INFO       "source_path": "/shared/common",
2024-07-17 01:26:38,283 INFO       "destination_path": "/mnt/common"
2024-07-17 01:26:38,283 INFO     },
2024-07-17 01:26:38,283 INFO     {
2024-07-17 01:26:38,283 INFO       "source_path_format": "POSIX",
2024-07-17 01:26:38,283 INFO       "source_path": "/",
2024-07-17 01:26:38,283 INFO       "destination_path": "/sessions/session-5b33f/
assetroot-assetroot-3751a"
2024-07-17 01:26:38,283 INFO     }
2024-07-17 01:26:38,283 INFO   ]
2024-07-17 01:26:38,283 INFO }
```

> **Note**
>
> Wenn der Job, den Sie einreichen, mehrere Manifeste mit unterschiedlichen Stammpfaden enthält, gibt es für jeden Stammpfad ein anderes Verzeichnis mit dem Namen „assetroot“.

Wenn Sie auf den verschobenen Dateisystemspeicherort einer Ihrer Eingabedateien, Verzeichnisse oder Dateisystemverzeichnisse verweisen müssen, können Sie entweder die Datei mit den Pfadzuordnungsregeln in Ihrem Job verarbeiten und die Neuzuordnung selbst durchführen oder

der Jobvorlage in Ihrem Job-Bundle einen PATH Typ-Job-Parameter hinzufügen und den Wert, den Sie neu zuordnen müssen, als Wert dieses Parameters übergeben. Im folgenden Beispiel wird das Auftragspaket so geändert, dass es einen dieser Auftragsparameter hat, und sendet dann einen Job mit dem Speicherort des Dateisystems `/shared/projects/project2` als Wert:

```
cat > ~/job_attachments_devguide/template.yaml << EOF
specificationVersion: jobtemplate-2023-09
name: "Job Attachments Explorer"
parameterDefinitions:
- name: LocationToRemap
  type: PATH
steps:
- name: Step
  script:
    actions:
      onRun:
        command: /bin/echo
        args:
        - "The location of {{RawParam.LocationToRemap}} in the session is
 {{Param.LocationToRemap}}"
EOF

deadline bundle submit --farm-id $FARM_ID --queue-id $QUEUE1_ID
 job_attachments_devguide/ \
  -p LocationToRemap=/shared/projects/project2
```

Die Protokolldatei für die Ausführung dieses Jobs enthält seine Ausgabe:

```
2024-07-17 01:40:35,283 INFO Output:
2024-07-17 01:40:35,284 INFO The location of /shared/projects/project2 in the session
 is /sessions/session-5b33f/assetroot-assetroot-3751a
```

Ausgabedateien von einem Job abrufen

Dieses Beispiel zeigt, wie Deadline Cloud die von Ihren Jobs generierten Ausgabedateien identifiziert, entscheidet, ob diese Dateien auf Amazon S3 hochgeladen werden sollen, und wie Sie diese Ausgabedateien auf Ihre Workstation übertragen können.

Verwenden Sie für dieses Beispiel das `job_attachments_devguide_output` Job-Bundle anstelle des `job_attachments_devguide` Job-Bundles. Erstellen Sie zunächst eine Kopie des Bundles in Ihrer AWS CloudShell Umgebung aus Ihrem Klon des Deadline GitHub Cloud-Beispiel-Repositorys:

```
cp -r deadline-cloud-samples/job_bundles/job_attachments_devguide_output ~/
```

Der wichtige Unterschied zwischen diesem Job-Bundle und dem `job_attachments_devguide` Job-Bundle besteht darin, dass der Job-Vorlage ein neuer Job-Parameter hinzugefügt wurde:

```
...
parameterDefinitions:
...
- name: OutputDir
  type: PATH
  objectType: DIRECTORY
  dataFlow: OUT
  default: ./output_dir
  description: This directory contains the output for all steps.
...
```

Die `dataFlow` Eigenschaft des Parameters hat den Wert`OUT`. Deadline Cloud verwendet den Wert von `dataFlow` Jobparametern mit einem Wert von `OUT` oder `INOUT` als Ausgabe Ihres Jobs. Wenn der Dateisystemspeicherort, der als Wert an diese Art von Jobparametern übergeben wurde, einem lokalen Dateisystemspeicherort auf dem Worker, der den Job ausführt, neu zugeordnet wird, sucht Deadline Cloud an dem Speicherort nach neuen Dateien und lädt diese als Jobausgaben auf Amazon S3 hoch.

Um zu sehen, wie das funktioniert, starten Sie zunächst den Deadline Cloud-Worker-Agent in einem AWS CloudShell Tab. Lassen Sie alle zuvor eingereichten Jobs die Ausführung beenden. Löschen Sie anschließend die Jobprotokolle aus dem Protokollverzeichnis:

```
rm -rf ~/devdemo-logs/queue-*
```

Reichen Sie als Nächstes einen Job mit diesem Job-Bundle ein. Nachdem der Worker in Ihren CloudShell Läufen ausgeführt wurde, schauen Sie sich die Logs an:

```
# Change the value of FARM_ID to your farm's identifier
FARM_ID=farm-00112233445566778899aabbccddeeff
# Change the value of QUEUE1_ID to queue Q1's identifier
QUEUE1_ID=queue-00112233445566778899aabbccddeeff
# Change the value of WSALL_ID to the identifier of the WSAll storage profile
WSALL_ID=sp-00112233445566778899aabbccddeeff
```

```
deadline config set settings.storage_profile_id $WSALL_ID

deadline bundle submit --farm-id $FARM_ID --queue-id $QUEUE1_ID ./
job_attachments_devguide_output
```

Das Protokoll zeigt, dass eine Datei als Ausgabe erkannt und auf Amazon S3 hochgeladen wurde:

```
2024-07-17 02:13:10,873 INFO ------------------------------------------
2024-07-17 02:13:10,873 INFO Uploading output files to Job Attachments
2024-07-17 02:13:10,873 INFO ------------------------------------------
2024-07-17 02:13:10,873 INFO Started syncing outputs using Job Attachments
2024-07-17 02:13:10,955 INFO Found 1 file totaling 117.0 B in output directory: /
sessions/session-7efa/assetroot-assetroot-3751a/output_dir
2024-07-17 02:13:10,956 INFO Uploading output manifest to
 DeadlineCloud/Manifests/farm-0011/queue-2233/job-4455/step-6677/
task-6677-0/2024-07-17T02:13:10.835545Z_sessionaction-8899-1/
c6808439dfc59f86763aff5b07b9a76c_output
2024-07-17 02:13:10,988 INFO Uploading 1 output file to S3: s3BucketName/DeadlineCloud/
Data
2024-07-17 02:13:11,011 INFO Uploaded 117.0 B / 117.0 B of 1 file (Transfer rate: 0.0
 B/s)
2024-07-17 02:13:11,011 INFO Summary Statistics for file uploads:
Processed 1 file totaling 117.0 B.
Skipped re-processing 0 files totaling 0.0 B.
Total processing time of 0.02281 seconds at 5.13 KB/s.
```

Das Protokoll zeigt auch, dass Deadline Cloud ein neues Manifest-Objekt im Amazon S3 S3-Bucket erstellt hat, das für die Verwendung durch Jobanhänge in der Warteschlange konfiguriert istQ1. Der Name des Manifest-Objekts wird von der Farm, der Warteschlange, dem Job, dem Schritt, der Aufgabe, dem Zeitstempel und den `sessionaction` Bezeichnern der Aufgabe abgeleitet, die die Ausgabe generiert hat. Laden Sie diese Manifestdatei herunter, um zu sehen, wo Deadline Cloud die Ausgabedateien für diese Aufgabe abgelegt hat:

```
# The name of queue `Q1`'s job attachments S3 bucket
Q1_S3_BUCKET=$(
  aws deadline get-queue --farm-id $FARM_ID --queue-id $QUEUE1_ID \
    --query 'jobAttachmentSettings.s3BucketName' | tr -d '"'
)

# Fill this in with the object name from your log
OBJECT_KEY="DeadlineCloud/Manifests/..."
```

```
aws s3 cp --quiet s3://$Q1_S3_BUCKET/$OBJECT_KEY /dev/stdout | jq .
```

Das Manifest sieht wie folgt aus:

```
{
  "hashAlg": "xxh128",
  "manifestVersion": "2023-03-03",
  "paths": [
    {
      "hash": "34178940e1ef9956db8ea7f7c97ed842",
      "mtime": 1721182390859777,
      "path": "output_dir/output.txt",
      "size": 117
    }
  ],
  "totalSize": 117
}
```

Dies zeigt, dass der Inhalt der Ausgabedatei auf die gleiche Weise in Amazon S3 gespeichert wird wie Jobeingabedateien. Ähnlich wie Eingabedateien wird die Ausgabedatei in S3 mit einem Objektnamen gespeichert, der den Hash der Datei und das Präfix enthält`DeadlineCloud/Data`.

```
$ aws s3 ls --recursive s3://$Q1_S3_BUCKET | grep 34178940e1ef9956db8ea7f7c97ed842
2024-07-17 02:13:11        117 DeadlineCloud/
Data/34178940e1ef9956db8ea7f7c97ed842.xxh128
```

Sie können die Ausgabe eines Jobs mit dem Deadline Cloud-Monitor oder der Deadline Cloud-CLI auf Ihre Workstation herunterladen:

```
deadline job download-output --farm-id $FARM_ID --queue-id $QUEUE1_ID --job-id $JOB_ID
```

Der Wert des `OutputDir` Job-Parameters im übermittelten Job ist`./output_dir`, sodass die Ausgabe in ein Verzeichnis heruntergeladen wird, das `output_dir` innerhalb des Job-Bundle-Verzeichnisses aufgerufen wird. Wenn Sie einen absoluten Pfad oder einen anderen relativen Speicherort als Wert für angegeben haben`OutputDir`, würden die Ausgabedateien stattdessen an diesen Speicherort heruntergeladen.

```
$ deadline job download-output --farm-id $FARM_ID --queue-id $QUEUE1_ID --job-id
 $JOB_ID
```

```
Downloading output from Job 'Job Attachments Explorer: Output'

Summary of files to download:
    /home/cloudshell-user/job_attachments_devguide_output/output_dir/output.txt (1
 file)

You are about to download files which may come from multiple root directories. Here are
 a list of the current root directories:
[0] /home/cloudshell-user/job_attachments_devguide_output
> Please enter the index of root directory to edit, y to proceed without changes, or n
 to cancel the download (0, y, n) [y]:

Downloading Outputs  [####################################]  100%
Download Summary:
    Downloaded 1 files totaling 117.0 B.
    Total download time of 0.14189 seconds at 824.0 B/s.
    Download locations (total file counts):
        /home/cloudshell-user/job_attachments_devguide_output (1 file)
```

Dateien aus einem Schritt in einem abhängigen Schritt verwenden

Dieses Beispiel zeigt, wie ein Schritt in einem Job auf die Ausgaben eines Schritts zugreifen kann, von dem er im selben Job abhängt.

Um die Ergebnisse eines Schritts für einen anderen verfügbar zu machen, fügt Deadline Cloud einer Sitzung zusätzliche Aktionen hinzu, um diese Ausgaben herunterzuladen, bevor Aufgaben in der Sitzung ausgeführt werden. Sie teilen ihr mit, aus welchen Schritten die Ausgaben heruntergeladen werden sollen, indem Sie diese Schritte als Abhängigkeiten des Schritts deklarieren, der die Ausgaben verwenden muss.

Verwenden Sie das `job_attachments_devguide_output` Job-Bundle für dieses Beispiel. Erstellen Sie zunächst in Ihrer AWS CloudShell Umgebung eine Kopie von Ihrem Klon des Deadline GitHub Cloud-Beispiel-Repositorys. Ändern Sie ihn, um einen abhängigen Schritt hinzuzufügen, der erst nach dem vorhandenen Schritt ausgeführt wird und die Ausgabe dieses Schritts verwendet:

```
cp -r deadline-cloud-samples/job_bundles/job_attachments_devguide_output ~/

cat >> job_attachments_devguide_output/template.yaml << EOF
- name: DependentStep
  dependencies:
  - dependsOn: Step
```

```
  script:
    actions:
      onRun:
        command: /bin/cat
        args:
        - "{{Param.OutputDir}}/output.txt"
EOF
```

Der mit diesem modifizierten Auftragspaket erstellte Job wird in zwei separaten Sitzungen ausgeführt, eine für die Aufgabe im Schritt „Schritt“ und dann eine zweite für die Aufgabe im Schritt "DependentStep“.

Starten Sie zunächst den Deadline Cloud-Worker-Agent in einem CloudShell Tab. Lassen Sie alle zuvor eingereichten Jobs fertig laufen und löschen Sie dann die Job-Logs aus dem Logs-Verzeichnis:

```
rm -rf ~/devdemo-logs/queue-*
```

Als Nächstes reichen Sie einen Job mit dem geänderten `job_attachments_devguide_output` Auftragspaket ein. Warten Sie, bis die Ausführung auf dem Worker in Ihrer CloudShell Umgebung abgeschlossen ist. Sehen Sie sich die Protokolle der beiden Sitzungen an:

```
# Change the value of FARM_ID to your farm's identifier
FARM_ID=farm-00112233445566778899aabbccddeeff
# Change the value of QUEUE1_ID to queue Q1's identifier
QUEUE1_ID=queue-00112233445566778899aabbccddeeff
# Change the value of WSALL_ID to the identifier of the WSAll storage profile
WSALL_ID=sp-00112233445566778899aabbccddeeff

deadline config set settings.storage_profile_id $WSALL_ID

deadline bundle submit --farm-id $FARM_ID --queue-id $QUEUE1_ID ./
job_attachments_devguide_output

# Wait for the job to finish running, and then:

cat demoenv-logs/queue-*/session-*
```

Im Sitzungsprotokoll für die Aufgabe im genannten `DependentStep` Schritt werden zwei separate Download-Aktionen ausgeführt:

```
2024-07-17 02:52:05,666 INFO ================================================
2024-07-17 02:52:05,666 INFO --------- Job Attachments Download for Job
2024-07-17 02:52:05,667 INFO ================================================
2024-07-17 02:52:05,667 INFO Syncing inputs using Job Attachments
2024-07-17 02:52:05,928 INFO Downloaded 207.0 B / 207.0 B of 1 file (Transfer rate: 0.0
 B/s)
2024-07-17 02:52:05,929 INFO Summary Statistics for file downloads:
Processed 1 file totaling 207.0 B.
Skipped re-processing 0 files totaling 0.0 B.
Total processing time of 0.03954 seconds at 5.23 KB/s.

2024-07-17 02:52:05,979 INFO
2024-07-17 02:52:05,979 INFO ================================================
2024-07-17 02:52:05,979 INFO --------- Job Attachments Download for Step
2024-07-17 02:52:05,979 INFO ================================================
2024-07-17 02:52:05,980 INFO Syncing inputs using Job Attachments
2024-07-17 02:52:06,133 INFO Downloaded 117.0 B / 117.0 B of 1 file (Transfer rate: 0.0
 B/s)
2024-07-17 02:52:06,134 INFO Summary Statistics for file downloads:
Processed 1 file totaling 117.0 B.
Skipped re-processing 0 files totaling 0.0 B.
Total processing time of 0.03227 seconds at 3.62 KB/s.
```

Bei der ersten Aktion wird die `script.sh` Datei heruntergeladen, die für den Schritt mit dem Namen „Schritt“ verwendet wurde. Bei der zweiten Aktion werden die Ausgaben aus diesem Schritt heruntergeladen. Deadline Cloud bestimmt, welche Dateien heruntergeladen werden sollen, indem das in diesem Schritt generierte Ausgabemanifest als Eingabemanifest verwendet wird.

Später im selben Protokoll können Sie die Ausgabe des Schritts "DependentStep„sehen:

```
2024-07-17 02:52:06,213 INFO Output:
2024-07-17 02:52:06,216 INFO Script location: /sessions/session-5b33f/
assetroot-assetroot-3751a/script.sh
```

Ressourcenlimits für Jobs erstellen

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 zu Fehlern aufgrund nicht verfügbarer Ressourcen 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, für die das Limit gilt. 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 Messwerte, 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, für die das Limit erforderlich ist, 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 vom Namen 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 aus.

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.

So reichen Sie einen Job bei Deadline Cloud ein

Es gibt viele verschiedene Möglichkeiten, Jobs bei AWS Deadline Cloud einzureichen. In diesem Abschnitt werden einige der Möglichkeiten beschrieben, wie Sie Jobs mithilfe der von Deadline Cloud bereitgestellten Tools oder durch die Erstellung eigener benutzerdefinierter Tools für Ihre Workloads einreichen können.

- Von einem Terminal aus — wenn Sie zum ersten Mal ein Jobpaket entwickeln oder wenn Benutzer, die einen Job einreichen, sich mit der Befehlszeile auskennen
- Aus einem Skript — zur Anpassung und Automatisierung von Workloads
- Aus einer Anwendung — wenn die Arbeit des Benutzers in einer Anwendung stattfindet oder wenn der Kontext einer Anwendung wichtig ist.

In den folgenden Beispielen werden die `deadline` Python-Bibliothek und das `deadline` Befehlszeilentool verwendet. Beide sind verfügbar PyPiund werden dort gehostet GitHub.

Themen

- Senden Sie einen Job von einem Terminal aus an Deadline Cloud
- Senden Sie einen Job mithilfe eines Skripts an Deadline Cloud
- Reichen Sie eine Stelle innerhalb einer Bewerbung ein

Senden Sie einen Job von einem Terminal aus an Deadline Cloud

Wenn Sie nur ein Job-Bundle und die Deadline Cloud-CLI verwenden, können Sie oder Ihre technisch versierten Benutzer schnell das Schreiben von Jobpaketen wiederholen, um das Einreichen eines Jobs zu testen. Verwenden Sie den folgenden Befehl, um ein Job-Bundle einzureichen:

```
deadline bundle submit <path-to-job-bundle>
```

Wenn Sie ein Job-Bundle mit Parametern einreichen, für die das Paket keine Standardwerte enthält, können Sie diese mit der `--parameter` Option`-p`/angeben.

```
deadline bundle submit <path-to-job-bundle> -p <parameter-name>=<parameter-value> -
p ...
```

Führen Sie den Befehl help aus, um eine vollständige Liste der verfügbaren Optionen zu erhalten:

```
deadline bundle submit --help
```

Senden Sie einen Job über eine GUI an Deadline Cloud

Die Deadline Cloud CLI verfügt außerdem über eine grafische Benutzeroberfläche, über die Benutzer die Parameter sehen können, die sie angeben müssen, bevor sie einen Job einreichen. Wenn Ihre Benutzer es vorziehen, nicht mit der Befehlszeile zu interagieren, können Sie eine Desktop-Verknüpfung schreiben, die einen Dialog zum Einreichen eines bestimmten Job-Bundles öffnet:

```
deadline bundle gui-submit <path-to-job-bundle>
```

Verwenden Sie die `--browse` Option can, damit der Benutzer ein Jobpaket auswählen kann:

```
deadline bundle gui-submit --browse
```

Eine vollständige Liste der verfügbaren Optionen erhalten Sie, wenn Sie den Befehl help ausführen:

```
deadline bundle gui-submit --help
```

Senden Sie einen Job mithilfe eines Skripts an Deadline Cloud

Um das Senden von Jobs an Deadline Cloud zu automatisieren, können Sie sie mithilfe von Tools wie Bash, Powershell und Batch-Dateien skripten.

Sie können Funktionen wie das Auffüllen von Jobparametern aus Umgebungsvariablen oder anderen Anwendungen hinzufügen. Sie können auch mehrere Jobs hintereinander einreichen oder die Erstellung eines Auftragspakets per Skript abschicken.

Einen Job mit Python einreichen

Deadline Cloud verfügt auch über eine Open-Source-Python-Bibliothek für die Interaktion mit dem Dienst. Der Quellcode ist verfügbar auf GitHub.

Die Bibliothek ist auf pypi über pip () verfügbar. `pip install deadline` Es ist dieselbe Bibliothek, die vom Deadline Cloud CLI-Tool verwendet wird:

```
from deadline.client import api

job_bundle_path = "/path/to/job/bundle"
job_parameters = [
    {
        "name": "parameter_name",
        "value": "parameter_value"
    },
]

job_id = api.create_job_from_job_bundle(
    job_bundle_path,
    job_parameters
)
print(job_id)
```

Um einen Dialog wie den `deadline bundle gui-submit` Befehl zu erstellen, können Sie die `show_job_bundle_submitter` Funktion von verwenden `deadline.client.ui.job_bundle_submitter`.

Das folgende Beispiel startet eine Qt-Anwendung und zeigt den Job Bundle Submitter:

```
# The GUI components must be installed with pip install "deadline[gui]"
import sys
from qtpy.QtWidgets import QApplication
from deadline.client.ui.job_bundle_submitter import show_job_bundle_submitter

app = QApplication(sys.argv)
submitter = show_job_bundle_submitter(browse=True)
submitter.show()
app.exec()
print(submitter.create_job_response)
```

Um Ihren eigenen Dialog zu erstellen, können Sie die `SubmitJobToDeadlineDialog` Klasse in verwenden. `deadline.client.ui.dialogs.submit_job_to_deadline_dialog` Sie können Werte übergeben, Ihren eigenen auftragsspezifischen Tab einbetten und festlegen, wie das Job-Bundle erstellt (oder übergeben) wird.

Reichen Sie eine Stelle innerhalb einer Bewerbung ein

Um Benutzern das Einreichen von Jobs zu erleichtern, können Sie die von einer Anwendung bereitgestellten Skriptlaufzeiten oder Plugin-Systeme verwenden. Die Benutzer haben eine vertraute Oberfläche, und Sie können leistungsstarke Tools erstellen, die die Benutzer beim Einreichen eines Workloads unterstützen.

Job-Bundles in eine Anwendung einbetten

Dieses Beispiel zeigt das Einreichen von Auftragspaketen, die Sie in der Anwendung zur Verfügung stellen.

Um einem Benutzer Zugriff auf diese Job-Bundles zu gewähren, erstellen Sie ein Skript, das in ein Menüelement eingebettet ist, das die Deadline Cloud-CLI startet.

Das folgende Skript ermöglicht es einem Benutzer, das Job-Bundle auszuwählen:

```
deadline bundle gui-submit --install-gui
```

Um stattdessen ein bestimmtes Job-Bundle in einem Menüelement zu verwenden, verwenden Sie Folgendes:

```
deadline bundle gui-submit </path/to/job/bundle> --install-gui
```

Dadurch wird ein Dialogfeld geöffnet, in dem der Benutzer die Jobparameter, Eingaben und Ausgaben ändern und den Job dann weiterleiten kann. Sie können verschiedene Menüelemente für verschiedene Jobpakete einrichten, die ein Benutzer in einer Bewerbung einreichen kann.

Wenn der Job, den Sie mit einem Job-Bundle einreichen, bei allen Einreichungen ähnliche Parameter und Ressourcenreferenzen enthält, können Sie die Standardwerte in das zugrunde liegende Job-Bundle eingeben.

Holen Sie sich Informationen aus einer Bewerbung

Um Informationen aus einer Anwendung abzurufen, sodass Benutzer sie nicht manuell zur Einreichung hinzufügen müssen, können Sie Deadline Cloud in die Anwendung integrieren, sodass Ihre Benutzer Jobs über eine vertraute Oberfläche einreichen können, ohne die Anwendung beenden oder Befehlszeilentools verwenden zu müssen.

Wenn Ihre Anwendung über eine Scripting-Runtime verfügt, die Python und pyside/pyqt unterstützt, können Sie die GUI-Komponenten aus der Deadline Cloud-Clientbibliothek verwenden, um eine Benutzeroberfläche zu erstellen. Ein Beispiel finden Sie unter Integration von Deadline Cloud für Maya unter. GitHub

Die Deadline Cloud-Clientbibliothek bietet Operationen, die Folgendes tun, um Ihnen zu helfen, ein starkes integriertes Benutzererlebnis zu bieten:

- Rufen Sie die Umgebungsparameter, Jobparameter und Asset-Referenzen aus Umgebungsvariablen ab und rufen Sie das Anwendungs-SDK auf.
- Legen Sie die Parameter im Job-Bundle fest. Um zu vermeiden, dass das ursprüngliche Paket geändert wird, sollten Sie eine Kopie des Bundles erstellen und die Kopie einreichen.

Wenn Sie den `deadline bundle gui-submit` Befehl verwenden, um das Job-Bundle zu senden, müssen Sie die `parameter_values.yaml` und `asset_references.yaml` -Dateien programmgesteuert verwenden, um die Informationen aus der Anwendung zu übergeben. Weitere Informationen zu diesen Dateien finden Sie unter. Vorlagen für offene Stellenbeschreibungen (OpenJD) für Deadline Cloud

Wenn Sie komplexere Steuerelemente als die von OpenJD angebotenen benötigen, den Job vom Benutzer abstrahieren müssen oder die Integration an den visuellen Stil der Anwendung anpassen möchten, können Sie Ihren eigenen Dialog schreiben, der die Deadline Cloud-Clientbibliothek aufruft, um den Job einzureichen.

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 }}
```

Pipelining von Sitzungsaktionen

Durch das Pipelining von Sitzungsaktionen kann ein Scheduler einem Worker mehrere Sitzungsaktionen vorab zuweisen. Der Worker kann diese Aktionen dann sequenziell ausführen, wodurch die Leerlaufzeit zwischen Aufgaben reduziert oder ganz vermieden wird.

Um eine erste Zuweisung zu erstellen, erstellt der Scheduler eine Sitzung mit einer Aufgabe, der Worker schließt die Aufgabe ab und anschließend analysiert der Scheduler die Aufgabendauer, um future Zuweisungen zu bestimmen.

Damit der Scheduler effektiv ist, gibt es Regeln für die Aufgabendauer. Für Aufgaben unter einer Minute verwendet der Scheduler ein Power-of-2-Wachstumsmuster. Bei einer 1-Sekunden-Aufgabe weist der Scheduler beispielsweise 2 neue Aufgaben zu, dann 4 und dann 8. Für Aufgaben, die länger als eine Minute dauern, weist der Scheduler nur eine neue Aufgabe zu, und das Pipelining bleibt deaktiviert.

Um die Pipeline-Größe zu berechnen, geht der Scheduler wie folgt vor:

- Verwendet die durchschnittliche Aufgabendauer abgeschlossener Aufgaben
- Zielt darauf ab, den Mitarbeiter eine Minute lang zu beschäftigen

- Berücksichtigt nur Aufgaben innerhalb derselben Sitzung
- Gibt Daten zur Dauer nicht an alle Mitarbeiter weiter

Durch die Weiterleitung von Sitzungsaktionen können Mitarbeiter sofort mit neuen Aufgaben beginnen und es gibt keine Wartezeiten zwischen den Anfragen des Terminplaners. Es sorgt auch für eine höhere Effizienz der Mitarbeiter und eine bessere Aufgabenverteilung bei lang andauernden Prozessen.

Wenn ein neuer Job mit höherer Priorität verfügbar ist, beendet der Mitarbeiter außerdem die gesamte ihm zuvor zugewiesene Arbeit, bevor die aktuelle Sitzung endet und eine neue Sitzung aus einem Job mit höherer Priorität zugewiesen wird.

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!
```

Einen Job in Deadline Cloud ändern

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.

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` oder`PENDING`, 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` sind`CANCELED`.

```
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 markiert`FAILED`.

```
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
```

Kundenverwaltete Flotten von Deadline Cloud erstellen und verwenden

Wenn Sie eine kundenverwaltete Flotte (CMF) einrichten, haben Sie die volle Kontrolle über Ihre Verarbeitungspipeline. Sie definieren die Netzwerk- und Softwareumgebung für jeden Mitarbeiter. Deadline Cloud fungiert als Repository und Scheduler für Ihre Jobs.

Ein Mitarbeiter kann eine Amazon Elastic Compute Cloud (Amazon EC2) -Instance, ein Mitarbeiter in einer Colocation-Einrichtung oder ein Mitarbeiter vor Ort sein. Jeder Mitarbeiter muss den Deadline Cloud-Worker-Agent ausführen. Alle Mitarbeiter müssen Zugriff auf den Deadline Cloud-Serviceendpunkt haben.

In den folgenden Themen erfahren Sie, wie Sie mithilfe von EC2 Amazon-Instances ein einfaches CMF erstellen.

Themen

Erstellen Sie eine vom Kunden verwaltete Flotte

Gehen Sie wie folgt vor, um eine kundenverwaltete Flotte (CMF) zu erstellen.

Deadline Cloud console

Um mit der Deadline Cloud-Konsole eine vom Kunden verwaltete Flotte zu erstellen

1. Öffnen Sie die Deadline Cloud-Konsole.

2. Wählen Sie Farmen aus. Eine Liste der verfügbaren Farmen wird angezeigt.
3. Wählen Sie den Namen der Farm aus, in der Sie arbeiten möchten.
4. Wählen Sie die Registerkarte Flotten und dann Flotte erstellen aus.
5. Geben Sie einen Namen für Ihre Flotte ein.
6. (Optional) Geben Sie eine Beschreibung für Ihre Flotte ein.
7. Wählen Sie als Flottenart die Option Vom Kunden verwaltet aus.
8. Wählen Sie den Servicezugang Ihrer Flotte aus.

    a. Wir empfehlen, für jede Flotte die Option Neue Servicerolle erstellen und verwenden zu verwenden, um die Berechtigungen detaillierter steuern zu können. Diese Option ist standardmäßig ausgewählt.

    b. Sie können auch eine bestehende Servicerolle verwenden, indem Sie eine Servicerolle auswählen auswählen.
9. Überprüfen Sie Ihre Auswahl und wählen Sie dann Weiter.
10. Wählen Sie ein Betriebssystem für Ihre Flotte aus. Alle Mitarbeiter einer Flotte müssen über ein gemeinsames Betriebssystem verfügen.
11. Wählen Sie die Host-CPU-Architektur aus.
12. Wählen Sie die minimalen und maximalen vCPU- und Speicher-Hardwarekapazitäten aus, um den Workload-Anforderungen Ihrer Flotten gerecht zu werden.
13. Wählen Sie einen Auto Scaling-Typ aus. Weitere Informationen finden Sie unter Verwendung EventBridge zur Behandlung von Auto Scaling Scaling-Ereignissen.

    - Keine Skalierung: Sie erstellen eine lokale Flotte und möchten Deadline Cloud Auto Scaling deaktivieren.
    - Empfehlungen zur Skalierung: Sie erstellen eine Amazon Elastic Compute Cloud (Amazon EC2) -Flotte.
14. (Optional) Wählen Sie den Pfeil aus, um den Abschnitt Funktionen hinzufügen zu erweitern.
15. (Optional) Aktivieren Sie das Kontrollkästchen GPU-Fähigkeit hinzufügen — Optional und geben Sie dann den Mindest- GPUs und Höchstwert sowie den Arbeitsspeicher ein.
16. Überprüfen Sie Ihre Auswahl und wählen Sie dann Weiter.
17. (Optional) Definieren Sie benutzerdefinierte Worker-Funktionen und wählen Sie dann Weiter.
18. Wählen Sie in der Dropdownliste eine oder mehrere Warteschlangen aus, die Sie der Flotte zuordnen möchten.

> **Note**
>
> Wir empfehlen, eine Flotte nur Warteschlangen zuzuordnen, die sich alle innerhalb derselben Vertrauensgrenze befinden. Dadurch wird eine starke Sicherheitsgrenze zwischen der Ausführung von Aufträgen auf demselben Worker gewährleistet.

19. Überprüfen Sie die Warteschlangenzuordnungen und wählen Sie dann Weiter.
20. (Optional) Für die standardmäßige Conda-Warteschlangenumgebung erstellen wir eine Umgebung für Ihre Warteschlange, in der die von Jobs angeforderten Conda-Pakete installiert werden.

> **Note**
>
> Die Conda-Warteschlangenumgebung wird verwendet, um Conda-Pakete zu installieren, die von Jobs angefordert werden. Normalerweise sollten Sie die Conda-Warteschlangenumgebung für die zugehörigen Warteschlangen deaktivieren, CMFs da dort die erforderlichen Conda-Befehle standardmäßig CMFs nicht installiert sind.

21. (Optional) Fügen Sie Ihrem CMF Tags hinzu. Weitere Informationen finden Sie unter Taggen Ihrer AWS Ressourcen.
22. Überprüfen Sie Ihre Flottenkonfiguration, nehmen Sie alle Änderungen vor und wählen Sie dann Flotte erstellen.
23. Wählen Sie die Registerkarte Flotten aus und notieren Sie sich die Flotten-ID.

AWS CLI

Um den zu verwenden AWS CLI , um eine vom Kunden verwaltete Flotte zu erstellen

1. Öffnen Sie ein -Terminalfenster.
2. `fleet-trust-policy.json`In einem neuen Editor erstellen.

   a. Fügen Sie die folgende IAM-Richtlinie hinzu und ersetzen Sie den *`ITALICIZED`* Text durch Ihre AWS Konto-ID und Deadline Cloud-Farm-ID.

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

```
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "credentials.deadline.amazonaws.com"
            },
            "Action": "sts:AssumeRole",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "ACCOUNT_ID"
                },
                "ArnEquals": {
                    "aws:SourceArn":
 "arn:aws:deadline:*:ACCOUNT_ID:farm/FARM_ID"
                }
            }
        }
    ]
}
```

b. Speichern Sie Ihre Änderungen.

3. Geben Sie einen Namen für den Benutzer ein und klicken Sie dann auf `fleet-policy.json`.

   a. Fügen Sie die folgende IAM-Richtlinie hinzu.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "deadline:AssumeFleetRoleForWorker",
                "deadline:UpdateWorker",
                "deadline:DeleteWorker",
                "deadline:UpdateWorkerSchedule",
                "deadline:BatchGetJobEntity",
                "deadline:AssumeQueueRoleForWorker"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": "${aws:ResourceAccount}"
                }
```

```
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream"
            ],
            "Resource": "arn:aws:logs:*:*:*:/aws/deadline/*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": "${aws:ResourceAccount}"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents",
                "logs:GetLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:*:/aws/deadline/*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalAccount": "${aws:ResourceAccount}"
                }
            }
        }
    ]
}
```

b. Speichern Sie Ihre Änderungen.

4. Fügen Sie eine IAM-Rolle hinzu, die die Mitarbeiter in Ihrer Flotte verwenden können.

```
aws iam create-role --role-name FleetWorkerRoleName --assume-role-policy-
document file://fleet-trust-policy.json
aws iam put-role-policy --role-name FleetWorkerRoleName --policy-name
 FleetWorkerPolicy --policy-document file://fleet-policy.json
```

5. Geben Sie einen Namen für den Benutzer ein und klicken Sie dann auf `create-fleet-request.json`.

   a. Fügen Sie die folgende IAM-Richtlinie hinzu und ersetzen Sie den KURSIV gedruckten Text durch die Werte Ihres CMF.

> **Note**
>
> Sie finden die in der. *ROLE_ARN* `create-cmf-fleet.json`
> Für *OS_FAMILY* die müssen Sie eines von`linux`, `macos` oder wählen`windows`.

```
{
    "farmId": "FARM_ID",
    "displayName": "FLEET_NAME",
    "description": "FLEET_DESCRIPTION",
    "roleArn": "ROLE_ARN",
    "minWorkerCount": 0,
    "maxWorkerCount": 10,
    "configuration": {
        "customerManaged": {
            "mode": "NO_SCALING",
            "workerCapabilities": {
                "vCpuCount": {
                    "min": 1,
                    "max": 4
                },
                "memoryMiB": {
                    "min": 1024,
                    "max": 4096
                },
                "osFamily": "OS_FAMILY",
                "cpuArchitectureType": "x86_64",
            },
        },
    }
}
```

b. Speichern Sie Ihre Änderungen.

6. Stellen Sie Ihre Flotte zusammen.

```
aws deadline create-fleet --cli-input-json file://create-fleet-request.json
```

Einrichtung und Konfiguration des Worker-Hosts

Ein Worker-Host bezieht sich auf einen Host-Computer, auf dem ein Deadline Cloud-Worker ausgeführt wird. In diesem Abschnitt wird erklärt, wie Sie den Worker-Host einrichten und für Ihre spezifischen Bedürfnisse konfigurieren. Jeder Worker-Host führt ein Programm aus, das als Worker-Agent bezeichnet wird. Der Worker-Agent ist verantwortlich für:

- Verwaltung des Lebenszyklus des Arbeitnehmers.
- Synchronisieren der zugewiesenen Arbeit, ihres Fortschritts und ihrer Ergebnisse.
- Überwachung laufender Arbeiten.
- Logs an konfigurierte Ziele weiterleiten.

Wir empfehlen Ihnen, den mitgelieferten Deadline Cloud-Worker-Agent zu verwenden. Der Worker Agent ist Open Source und wir freuen uns über Funktionsanfragen, aber Sie können ihn auch entwickeln und an Ihre Bedürfnisse anpassen.

Um die Aufgaben in den folgenden Abschnitten ausführen zu können, benötigen Sie Folgendes:

Linux

- A Linuxbasierte Amazon Elastic Compute Cloud (Amazon EC2) -Instanz. Wir empfehlen Amazon Linux 2023.
- `sudo`Privilegien
- Python 3.9 oder höher

Windows

- A Windowsbasierte Amazon Elastic Compute Cloud (Amazon EC2) -Instanz. Wir empfehlen Windows Server 2022.
- Administratorzugriff auf den Worker-Host
- Python 3.9 oder höher für alle Benutzer installiert

Erstellen und konfigurieren Sie eine virtuelle Python-Umgebung

Sie können eine virtuelle Python-Umgebung erstellen auf Linux wenn Sie Python 3.9 oder höher installiert und in Ihrem abgelegt habenPATH.

> **Note**
>
> Ein Windows, Agentendateien müssen im globalen Site-Packages-Verzeichnis von Python installiert werden. Virtuelle Python-Umgebungen werden derzeit nicht unterstützt.

So erstellen und aktivieren Sie eine virtuelle Python-Umgebung

1. Öffnen Sie ein Terminal als `root` Benutzer (oder verwenden Siesudo/su).
2. Erstellen und aktivieren Sie eine virtuelle Python-Umgebung.

```
python3 -m venv /opt/deadline/worker
source /opt/deadline/worker/bin/activate
pip install --upgrade pip
```

Installieren Sie den Deadline Cloud Worker Agent

Nachdem Sie Ihr Python eingerichtet und eine virtuelle Umgebung erstellt haben Linux, installieren Sie die Python-Pakete für den Deadline Cloud Worker Agent.

Um die Python-Pakete für den Worker Agent zu installieren

Linux

1. Öffnen Sie ein Terminal als `root` Benutzer (oder verwenden Siesudo/su).
2. Laden Sie die Deadline Cloud Worker Agent-Pakete von PyPI herunter und installieren Sie sie:

```
/opt/deadline/worker/bin/python -m pip install deadline-cloud-worker-agent
```

Windows

1. Öffnen Sie eine Administrator-Befehlszeile oder PowerShell ein Terminal.

2. Laden Sie die Deadline Cloud Worker Agent-Pakete von PyPI herunter und installieren Sie sie:

```
python -m pip install deadline-cloud-worker-agent
```

Wenn dein Windows Worker-Host benötigt lange Pfadnamen (mehr als 250 Zeichen), müssen Sie lange Pfadnamen wie folgt aktivieren:

Um lange Pfade zu aktivieren für Windows Worker-Hosts

1. Stellen Sie sicher, dass der Registrierungsschlüssel mit langem Pfad aktiviert ist. Weitere Informationen finden Sie unter Registrierungseinstellung zur Aktivierung von Protokollpfaden auf der Microsoft-Website.
2. Installieren Sie das Windows SDK für C++ x86-Desktop-Apps. Weitere Informationen finden Sie unter .Windows SDK im Windows Entwicklungszentrum.
3. Öffnen Sie den Python-Installationsort in Ihrer Umgebung, in dem der Worker-Agent installiert ist. Der Standardwert ist `C:\Program Files\Python311`. Es gibt eine ausführbare Datei mit dem Namen`pythonservice.exe`.
4. Erstellen Sie eine neue Datei mit `pythonservice.exe.manifest` dem Namen am selben Ort. Fügen Sie Folgendes hinzu:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
  <assemblyIdentity type="win32" name="pythonservice" processorArchitecture="x86"
 version="1.0.0.0"/>
  <application xmlns="urn:schemas-microsoft-com:asm.v3">
    <windowsSettings>
      <longPathAware xmlns="http://schemas.microsoft.com/SMI/2016/
WindowsSettings">true</longPathAware>
    </windowsSettings>
  </application>
</assembly>
```

5. Öffnen Sie eine Befehlszeile und führen Sie den folgenden Befehl am Speicherort der von Ihnen erstellten Manifestdatei aus:

```
"C:\Program Files (x86)\Windows Kits\10\bin\10.0.26100.0\x86\mt.exe" -manifest
 pythonservice.exe.manifest -outputresource:pythonservice.exe;#1
```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
Microsoft (R) Manifest Tool
Copyright (c) Microsoft Corporation.
All rights reserved.
```

Der Worker kann jetzt auf lange Pfade zugreifen. Um zu bereinigen, entfernen Sie die `pythonservice.exe.manifest` Datei und deinstallieren Sie das SDK.

Konfigurieren Sie den Deadline Cloud Worker Agent

Sie können die Deadline Cloud-Worker-Agent-Einstellungen auf drei Arten konfigurieren. Wir empfehlen Ihnen, das Betriebssystem-Setup zu verwenden, indem Sie das `install-deadline-worker` Tool ausführen.

Der Worker-Agent unterstützt die Ausführung als Domänenbenutzer unter Windows nicht. Um einen Job als Domänenbenutzer auszuführen, können Sie ein Domänenbenutzerkonto angeben, wenn Sie einen Warteschlangenbenutzer für die Ausführung von Jobs konfigurieren. Weitere Informationen finden Sie unter Schritt 7 unter Deadline Cloud-Warteschlangen im AWS Deadline Cloud-Benutzerhandbuch.

Befehlszeilenargumente — Sie können Argumente angeben, wenn Sie den Deadline Cloud-Worker-Agent von der Befehlszeile aus ausführen. Einige Konfigurationseinstellungen sind nicht über Befehlszeilenargumente verfügbar. Geben Sie ein, um alle verfügbaren Befehlszeilenargumente anzuzeigen`deadline-worker-agent --help`.

Umgebungsvariablen — Sie können den Deadline Cloud-Worker-Agent konfigurieren, indem Sie die Umgebungsvariable festlegen, die mit beginnt`DEADLINE_WORKER_`. Um beispielsweise alle verfügbaren Befehlszeilenargumente zu sehen, können `export DEADLINE_WORKER_VERBOSE=true` Sie die Ausgabe des Worker-Agents auf ausführlich setzen. Weitere Beispiele und Informationen finden Sie unter `/etc/amazon/deadline/worker.toml.example` Linux oder `C:\ProgramData\Amazon\Deadline\Config\worker.toml.example` auf Windows.

Konfigurationsdatei — Wenn Sie den Worker-Agent installieren, erstellt er eine Konfigurationsdatei unter `/etc/amazon/deadline/worker.toml` on Linux oder `C:\ProgramData\Amazon\Deadline\Config\worker.toml` auf Windows. Der Worker-Agent lädt diese

Konfigurationsdatei, wenn er gestartet wird. Sie können die Beispielkonfigurationsdatei verwenden (`/etc/amazon/deadline/worker.toml.exampleauf` Linux oder `C:\ProgramData\Amazon\Deadline\Config\worker.toml.example` auf Windows), um die Standard-Worker-Agent-Konfigurationsdatei an Ihre spezifischen Bedürfnisse anzupassen.

Schließlich empfehlen wir Ihnen, das auto Herunterfahren für den Worker Agent zu aktivieren, nachdem Ihre Software bereitgestellt wurde und wie erwartet funktioniert. Auf diese Weise kann die Mitarbeiterflotte bei Bedarf erweitert und nach Abschluss eines Auftrags heruntergefahren werden. Durch die automatische Skalierung wird sichergestellt, dass Sie nur die benötigten Ressourcen nutzen. Damit eine von der Auto Scaling-Gruppe gestartete Instanz heruntergefahren werden kann, müssen Sie der `worker.toml` Konfigurationsdatei etwas hinzufügen`shutdown_on_stop=true`.

Um die auto Abschaltung zu aktivieren

Als **`root`** Benutzer:

- Installieren Sie den Worker Agent mit Parametern**`--allow-shutdown`**.

  Linux

  Geben Sie ein:

  ```
  /opt/deadline/worker/bin/install-deadline-worker \
    --farm-id FARM_ID \
    --fleet-id FLEET_ID \
    --region REGION \
    --allow-shutdown
  ```

  Windows

  Geben Sie ein:

  ```
  install-deadline-worker ^
    --farm-id FARM_ID ^
    --fleet-id FLEET_ID ^
    --region REGION ^
    --allow-shutdown
  ```

Job-Benutzer und Gruppen erstellen

In diesem Abschnitt wird die erforderliche Benutzer- und Gruppenbeziehung zwischen dem Agent-Benutzer und den in Ihren Warteschlangen `jobRunAsUser` definierten Benutzern beschrieben.

Der Deadline Cloud-Worker-Agent sollte als dedizierter agentenspezifischer Benutzer auf dem Host ausgeführt werden. Sie sollten die `jobRunAsUser` Eigenschaft der Deadline Cloud-Warteschlangen so konfigurieren, dass Mitarbeiter die Warteschlangenjobs als ein bestimmter Betriebssystembenutzer und eine bestimmte Gruppe ausführen. Das bedeutet, dass Sie die gemeinsamen Dateisystemberechtigungen für Ihre Jobs kontrollieren können. Es stellt auch eine wichtige Sicherheitsgrenze zwischen Ihren Jobs und dem Worker-Agent-Benutzer dar.

Linux Jobbenutzer und Gruppen

Um einen lokalen Worker Agent-Benutzer einzurichten`jobRunAsUser`, stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen. Wenn Sie ein Linux Pluggable Authentication Module (PAM) wie Active Directory oder LDAP verwenden, ist Ihr Verfahren möglicherweise anders.

Der Worker-Agent-Benutzer und die gemeinsam genutzte `jobRunAsUser` Gruppe werden bei der Installation des Worker-Agents festgelegt. Die Standardwerte sind `deadline-worker-agent` und`deadline-job-users`, aber Sie können diese ändern, wenn Sie den Worker Agent installieren.

```
install-deadline-worker \
    --user AGENT_USER_NAME \
    --group JOB_USERS_GROUP
```

Befehle sollten als Root-Benutzer ausgeführt werden.

- Jeder `jobRunAsUser` sollte eine passende Primärgruppe haben. Wenn Sie einen Benutzer mit dem `adduser` Befehl erstellen, wird normalerweise eine passende Primärgruppe erstellt.

  ```
  adduser -r -m jobRunAsUser
  ```

- Die primäre Gruppe von `jobRunAsUser` ist eine sekundäre Gruppe für den Worker Agent-Benutzer. Die gemeinsam genutzte Gruppe ermöglicht es dem Worker-Agent, Dateien für den Job während der Ausführung verfügbar zu machen.

  ```
  usermod -a -G jobRunAsUser deadline-worker-agent
  ```

- Der `jobRunAsUser` muss Mitglied der gemeinsam genutzten Auftragsgruppe sein.

```
usermod -a -G deadline-job-users jobRunAsUser
```

- Der `jobRunAsUser` darf nicht zur primären Gruppe des Worker Agent-Benutzers gehören. Vertrauliche Dateien, die vom Worker-Agenten geschrieben wurden, gehören der primären Gruppe des Agenten. Wenn a Teil dieser Gruppe `jobRunAsUser` ist, können Jobs, die auf dem Worker ausgeführt werden, auf Dateien des Worker-Agents zugreifen.
- Die Standardeinstellung AWS-Region muss der Region der Farm entsprechen, zu der der Worker gehört. Dies sollte auf alle `jobRunAsUser` Konten des Arbeiters angewendet werden.

```
sudo -u jobRunAsUser aws configure set default.region aws-region
```

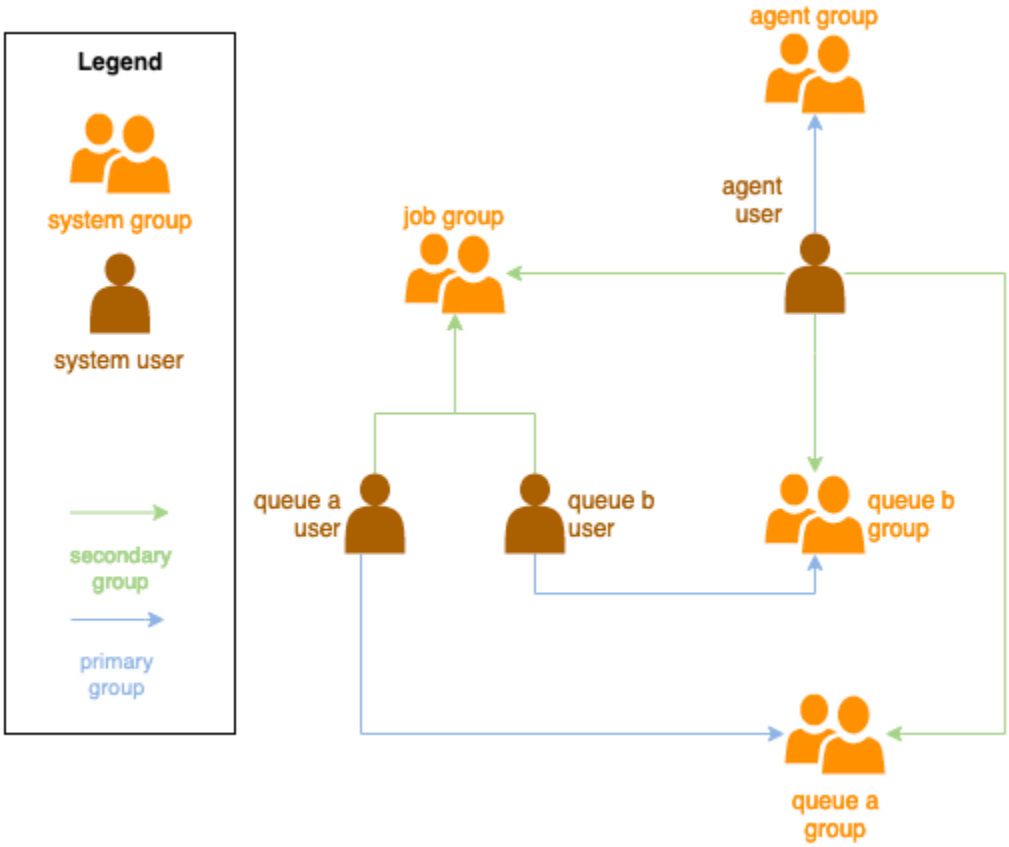
- Der Worker-Agent-Benutzer muss in der Lage sein, `sudo` Befehle als auszuführen`jobRunAsUser`. Führen Sie den folgenden Befehl aus, um einen Editor zum Erstellen einer neuen Sudoers-Regel zu öffnen:

  ```
  visudo -f /etc/sudoers.d/deadline-worker-job-user
  ```

  Fügen Sie der Datei Folgendes hinzu:

  ```
  # Allows the Deadline Cloud worker agent OS user to run commands
   # as the queue OS user without requiring a password.
  deadline-worker-agent ALL=(jobRunAsUser) NOPASSWD:ALL
  ```

Das folgende Diagramm veranschaulicht die Beziehung zwischen dem Agent-Benutzer und den `jobRunAsUser` Benutzern und Gruppen für Warteschlangen, die der Flotte zugeordnet sind.



Windows Benutzer

Um eine zu verwenden Windows als Benutzer muss `jobRunAsUser` es die folgenden Anforderungen erfüllen:

- Alle `jobRunAsUser` Benutzer der Warteschlange müssen vorhanden sein.
- Ihre Passwörter müssen dem Wert des Geheimnisses entsprechen, das im `JobRunAsUser` Feld ihrer Warteschlange angegeben ist. Eine Anleitung finden Sie in Schritt 7 unter Deadline Cloud-Warteschlangen im AWS Deadline Cloud-Benutzerhandbuch.
- Der Agent-Benutzer muss sich als dieser Benutzer anmelden können.

Zugriff verwalten auf Windows Geheimnisse von Jobnutzern

Wenn Sie eine Warteschlange mit einem konfigurieren Windows `jobRunAsUser`, müssen Sie ein AWS Secrets Manager Manager-Geheimnis angeben. Es wird erwartet, dass der Wert dieses Geheimnisses ein JSON-kodiertes Objekt der folgenden Form ist:

```
{
    "password": "JOB_USER_PASSWORD"
}
```

Damit Worker Jobs so ausführen können, wie die Warteschlange konfiguriert ist`jobRunAsUser`, muss die IAM-Rolle der Flotte über die erforderlichen Berechtigungen verfügen, um den Wert des Geheimnisses abzurufen. Wenn das Geheimnis mit einem vom Kunden verwalteten KMS-Schlüssel verschlüsselt wird, muss die IAM-Rolle der Flotte auch über Berechtigungen zur Entschlüsselung mit dem KMS-Schlüssel verfügen.

Es wird dringend empfohlen, bei diesen Geheimnissen das Prinzip der geringsten Rechte einzuhalten. Das bedeutet, dass der Zugriff zum Abrufen des geheimen Werts von `jobRunAsUser` → → `windows` einer Warteschlange wie folgt sein sollte: `passwordArn`

- wird einer Flottenrolle zugewiesen, wenn zwischen der Flotte und der Warteschlange eine Verbindung zwischen Warteschlange und Flotte erstellt wird
- wird einer Flottenrolle entzogen, wenn zwischen der Flotte und der Warteschlange eine Flottenverbindung zwischen der Flotte und der Warteschlange gelöscht wird

Außerdem sollte das AWS Secrets Manager Manager-Geheimnis, das das `jobRunAsUser` Passwort enthält, gelöscht werden, wenn es nicht mehr verwendet wird.

Gewähren Sie Zugriff auf ein geheimes Passwort

Deadline Cloud-Flotten benötigen Zugriff auf das `jobRunAsUser` Passwort, das im Passwortgeheimnis der Warteschlange gespeichert ist, wenn die Warteschlange und die Flotte verknüpft werden. Wir empfehlen, die AWS Secrets Manager Manager-Ressourcenrichtlinie zu verwenden, um Zugriff auf die Flottenrollen zu gewähren. Wenn Sie sich strikt an diese Richtlinie halten, ist es einfacher festzustellen, welche Flottenrollen Zugriff auf den geheimen Schlüssel haben.

Um Zugriff auf das Geheimnis zu gewähren

1. Öffnen Sie die AWS Secret Manager-Konsole für das Geheimnis.
2. Fügen Sie im Abschnitt „Ressourcenberechtigungen“ eine Richtlinienerklärung der folgenden Form hinzu:

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

```
  "Statement" : [
    //...
    {
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "FLEET_ROLE_ARN"
      },
      "Action" : "secretsmanager:GetSecretValue",
      "Resource" : "*"
    }
    //...
  ]
}
```

Widerrufen Sie den Zugriff auf ein geheimes Passwort

Wenn eine Flotte keinen Zugriff mehr auf eine Warteschlange benötigt, entfernen Sie den Zugriff auf das geheime Passwort für die Warteschlange`jobRunAsUser`. Wir empfehlen, die AWS Secrets Manager Manager-Ressourcenrichtlinie zu verwenden, um Zugriff auf die Flottenrollen zu gewähren. Wenn Sie sich strikt an diese Richtlinie halten, ist es einfacher festzustellen, welche Flottenrollen Zugriff auf den geheimen Schlüssel haben.

Um den Zugriff auf das Geheimnis zu entziehen

1. Öffnen Sie die AWS Secret Manager-Konsole für das Geheimnis.
2. Entfernen Sie im Abschnitt Ressourcenberechtigungen die Richtlinienerklärung in der folgenden Form:

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    //...
    {
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "FLEET_ROLE_ARN"
      },
      "Action" : "secretsmanager:GetSecretValue",
      "Resource" : "*"
    }
    //...
```

```
  ]
}
```

Installation und Konfiguration der für Jobs erforderlichen Software

Nachdem Sie den Deadline Cloud-Worker-Agent eingerichtet haben, können Sie den Worker-Host mit jeder Software vorbereiten, die für die Ausführung von Jobs erforderlich ist.

Wenn Sie einen Job an eine Warteschlange senden, der ein zugeordneter Job zugeordnet ist`jobRunAsUser`, wird der Job als dieser Benutzer ausgeführt. Wenn ein Job mit Befehlen übermittelt wird, bei denen es sich nicht um einen absoluten Pfad handelt, muss sich dieser Befehl im `PATH` Verzeichnis dieses Benutzers befinden.

Unter Linux können Sie das `PATH` für einen Benutzer in einer der folgenden Optionen angeben:

- ihr `~/.bashrc` oder `~/.bash_profile`
- Systemkonfigurationsdateien wie `/etc/profile.d/*` und `/etc/profile`
- Shell-Startskripte:`/etc/bashrc`.

Unter Windows können Sie das `PATH` für einen Benutzer in einer der folgenden Optionen angeben:

- ihre benutzerspezifischen Umgebungsvariablen
- die systemweiten Umgebungsvariablen

Installieren Sie die Adapter für Tools zur Erstellung digitaler Inhalte

Deadline Cloud bietet OpenJobDescription Adapter für die Nutzung beliebter DCC-Anwendungen (Digital Content Creation). Um diese Adapter in einer vom Kunden verwalteten Flotte zu verwenden, müssen Sie die DCC-Software und die Anwendungsadapter installieren. Stellen Sie anschließend sicher, dass die ausführbaren Programme der Software im Systemsuchpfad verfügbar sind (z. B. in der `PATH` Umgebungsvariablen).

Um DCC-Adapter in einer vom Kunden verwalteten Flotte zu installieren

1. Öffnen Sie das A-Terminal.

    a. Öffnen Sie unter Linux ein Terminal als `root` Benutzer (oder verwenden Sie`sudo/su`)

b. Öffnen Sie unter Windows eine Administrator-Befehlszeile oder ein PowerShell Terminal.

2. Installieren Sie die Deadline Cloud-Adapterpakete.

```
pip install deadline deadline-cloud-for-maya deadline-cloud-for-nuke deadline-
cloud-for-blender
```

AWS Anmeldeinformationen konfigurieren

Die Anfangsphase des Lebenszyklus eines Mitarbeiters ist Bootstrapping. In dieser Phase erstellt die Worker-Agent-Software einen Worker in Ihrer Flotte und bezieht die AWS Anmeldeinformationen für den weiteren Betrieb von der Rolle Ihres Fuhrparks.

AWS credentials for Amazon EC2

So erstellen Sie eine IAM-Rolle für Amazon EC2 mit Deadline Cloud-Worker-Hostberechtigungen

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Rollen und anschließend Rolle erstellen aus.
3. Wählen Sie AWS Dienst aus.
4. Wählen Sie EC2als Dienst oder Anwendungsfall aus und wählen Sie dann Weiter aus.
5. Um die erforderlichen Berechtigungen zu gewähren, fügen Sie die `AWSDeadlineCloud-WorkerHost` AWS verwaltete Richtlinie bei.

On-premises AWS credentials

Ihre Mitarbeiter vor Ort verwenden Anmeldeinformationen, um auf Deadline Cloud zuzugreifen. Für den sichersten Zugriff empfehlen wir die Verwendung von IAM Roles Anywhere zur Authentifizierung Ihrer Mitarbeiter. Weitere Informationen finden Sie unter IAM Roles Anywhere.

Zum Testen können Sie IAM-Benutzerzugriffsschlüssel für AWS Anmeldeinformationen verwenden. Wir empfehlen, dass Sie ein Ablaufdatum für den IAM-Benutzer festlegen, indem Sie eine restriktive Inline-Richtlinie einbeziehen.

> **Important**
>
> Beachten Sie die folgenden Warnungen:

- Verwenden Sie NICHT die Root-Anmeldeinformationen Ihres Kontos, um auf AWS Ressourcen zuzugreifen. Diese Anmeldeinformationen bieten uneingeschränkten Zugriff auf Konten und können nur schwer widerrufen werden.
- Geben Sie KEINE wörtlichen Zugriffsschlüssel oder Anmeldeinformationen in Ihre Anwendungsdateien ein. Wenn Sie dies tun, riskieren Sie damit, dass Ihre Kontodaten versehentlich offengelegt werden, falls Sie z. B. das Projekt in ein öffentliches Repository hochladen.
- Fügen Sie KEINE Dateien in Ihrem Projektbereich hinzu, die Anmeldeinformationen enthalten.
- Sichern Sie Ihre Zugangsschlüssel. Geben Sie Ihre Zugangsschlüssel nicht an Unbefugte weiter, auch nicht, um Ihre Kontokennungen zu finden. Wenn Sie dies tun, gewähren Sie anderen Personen möglicherweise den permanenten Zugriff auf Ihr Konto.
- Beachten Sie, dass alle in der Datei mit den gemeinsam genutzten AWS Anmeldeinformationen gespeicherten Anmeldeinformationen im Klartext gespeichert werden.

Weitere Informationen finden Sie unter Bewährte Methoden für die Verwaltung von AWS Zugriffsschlüsseln in der AWS Allgemeinen Referenz.

Erstellen eines IAM-Benutzers

1. Öffnen Sie unter https://console.aws.amazon.com/iam/ die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Benutzer und anschließend Benutzer erstellen aus.
3. Geben Sie dem Benutzer einen Namen. Deaktivieren Sie das Kontrollkästchen für Benutzerzugriff auf gewähren AWS Management Console, und wählen Sie dann Weiter.
4. Wählen Sie Richtlinien direkt anhängen aus.
5. Wählen Sie aus der Liste der Berechtigungsrichtlinien die AWSDeadlineCloud-WorkerHostRichtlinie aus und klicken Sie dann auf Weiter.
6. Überprüfen Sie die Benutzerdetails und wählen Sie dann Benutzer erstellen aus.

Beschränken Sie den Benutzerzugriff auf ein begrenztes Zeitfenster

Bei allen IAM-Benutzerzugriffsschlüsseln, die Sie erstellen, handelt es sich um langfristige Anmeldeinformationen. Um sicherzustellen, dass diese Anmeldeinformationen ablaufen, falls sie falsch behandelt werden, können Sie diese Anmeldeinformationen zeitgebunden machen, indem Sie eine Inline-Richtlinie erstellen, die ein Datum festlegt, nach dem die Schlüssel nicht mehr gültig sind.

1. Öffnen Sie den IAM-Benutzer, den Sie gerade erstellt haben. Wählen Sie auf der Registerkarte „Berechtigungen“ die Option „Berechtigungen hinzufügen“ und dann „Inline-Richtlinie erstellen“ aus.
2. Geben Sie im JSON-Editor die folgenden Berechtigungen an. Um diese Richtlinie zu verwenden, ersetzen Sie den `aws:CurrentTime` Zeitstempelwert in der Beispielrichtlinie durch Ihre eigene Uhrzeit und Ihr eigenes Datum.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "DateGreaterThan": {
          "aws:CurrentTime": "2024-01-01T00:00:00Z"
        }
      }
    }
  ]
}
```

Erstellen eines Zugriffsschlüssels

1. Wählen Sie auf der Seite mit den Benutzerdetails die Registerkarte Sicherheitsanmeldeinformationen aus. Wählen Sie im Abschnitt Access keys (Zugriffsschlüssel) Create access key (Zugriffsschlüssel erstellen).
2. Geben Sie an, dass Sie den Schlüssel für Andere verwenden möchten, klicken Sie dann auf Weiter und anschließend auf Zugriffsschlüssel erstellen.

3. Wählen Sie auf der Seite Zugriffsschlüssel abrufen die Option Anzeigen aus, um den Wert des geheimen Zugriffsschlüssels Ihres Benutzers anzuzeigen. Sie können die Anmeldeinformationen kopieren oder eine CSV-Datei herunterladen.

Speichern Sie die Benutzerzugriffsschlüssel

- Speichern Sie die Benutzerzugriffsschlüssel in der Datei mit den AWS Anmeldeinformationen des Agent-Benutzers auf dem Worker-Host-System:
  - Ein Linux, die Datei befindet sich unter `~/.aws/credentials`
  - Ein Windows, die Datei befindet sich unter `%USERPROVILE\.aws\credentials`

  Ersetzen Sie die folgenden Schlüssel:

```
[default]
aws_access_key_id=ACCESS_KEY_ID
aws_access_key_id=SECRET_ACCESS_KEY
```

> **Important**
>
> Wenn Sie diesen IAM-Benutzer nicht mehr benötigen, empfehlen wir, ihn zu entfernen, um den bewährten AWS Sicherheitsmethoden zu entsprechen. Wir empfehlen, dass Ihre menschlichen Benutzer AWS IAM Identity Centerbeim Zugriff AWS temporäre Anmeldeinformationen verwenden müssen.

Konfiguration des Netzwerks für AWS-Endpunktverbindungen

Deadline Cloud erfordert für einen ordnungsgemäßen Betrieb eine sichere Konnektivität zu verschiedenen AWS Service-Endpunkten. Um Deadline Cloud verwenden zu können, müssen Sie sicherstellen, dass Ihre Netzwerkumgebung es Ihren Deadline Cloud-Mitarbeitern ermöglicht, sich mit diesen Endpunkten zu verbinden.

Wenn Sie über eine Netzwerk-Firewall verfügen, die ausgehende Verbindungen blockiert, müssen Sie möglicherweise Firewall-Ausnahmen für bestimmte Endpunkte hinzufügen. Für Deadline Cloud müssen Sie Ausnahmen für die folgenden Dienste hinzufügen:

- Deadline Cloud-Endpunkte
- Amazon CloudWatch Logs-Endpunkte
- Amazon Simple Storage Service-Endpunkte

Wenn Ihre Jobs andere AWS Dienste nutzen, müssen Sie möglicherweise auch Ausnahmen für diese Dienste hinzufügen. Sie finden diese Endpunkte im Kapitel Service-Endpunkte und Kontingente des AWS General Reference Guide. Nachdem Sie die erforderlichen Endpunkte identifiziert haben, erstellen Sie Regeln für ausgehenden Datenverkehr in Ihrer Firewall, um den Datenverkehr zu diesen spezifischen Endpunkten zuzulassen.

Für einen ordnungsgemäßen Betrieb muss sichergestellt werden, dass auf diese Endpunkte zugegriffen werden kann. Erwägen Sie außerdem die Implementierung geeigneter Sicherheitsmaßnahmen, wie z. B. die Verwendung virtueller privater Clouds (VPCs), Sicherheitsgruppen und Netzwerkzugriffskontrolllisten (ACLs), um eine sichere Umgebung aufrechtzuerhalten und gleichzeitig den erforderlichen Deadline-Cloud-Verkehr zuzulassen.

Testen Sie die Konfiguration Ihres Worker-Hosts

Nachdem Sie den Worker Agent installiert, die für die Verarbeitung Ihrer Jobs erforderliche Software installiert und die AWS Anmeldeinformationen für den Worker Agent konfiguriert haben, sollten Sie testen, ob die Installation Ihre Jobs verarbeiten kann, bevor Sie einen erstellen AMI für Ihre Flotte. Sie sollten Folgendes testen:

- Der Deadline Cloud-Worker-Agent ist ordnungsgemäß für die Ausführung als Systemdienst konfiguriert.
- Dass der Worker die zugehörige Warteschlange nach Arbeit abfragt.
- Dass der Mitarbeiter erfolgreich Aufträge verarbeitet, die an die der Flotte zugeordnete Warteschlange gesendet wurden.

Nachdem Sie die Konfiguration getestet haben und repräsentative Jobs erfolgreich verarbeiten können, können Sie mit dem konfigurierten Worker eine erstellen AMI für EC2 Amazon-Mitarbeiter oder als Modell für Ihre Mitarbeiter vor Ort.

> **Note**
>
> Wenn Sie die Worker-Host-Konfiguration einer Auto Scaling-Flotte testen, können Sie in den folgenden Situationen Schwierigkeiten haben, Ihren Worker zu testen:
>
> - Wenn sich keine Arbeit in der Warteschlange befindet, stoppt Deadline Cloud den Worker-Agent kurz nach dem Start des Workers.
> - Wenn der Worker-Agent so konfiguriert ist, dass er den Host beim Stoppen herunterfährt, fährt der Agent die Maschine herunter, wenn sich keine Arbeit in der Warteschlange befindet.
>
> Um diese Probleme zu vermeiden, sollten Sie eine Staging-Flotte verwenden, die nicht auto skaliert, um Ihre Mitarbeiter zu konfigurieren und zu testen. Stellen Sie nach dem Testen des Worker-Hosts sicher, dass Sie die richtige Flotten-ID angeben, bevor Sie ein AMI.

Um Ihre Worker-Host-Konfiguration zu testen

1. Führen Sie den Worker-Agent aus, indem Sie den Betriebssystemdienst starten.

   Linux

   Führen Sie in einer Root-Shell den folgenden Befehl aus:

   ```
   systemctl start deadline-worker
   ```

   Windows

   Von einer Administrator-Befehlszeile aus oder PowerShell Terminal, geben Sie den folgenden Befehl ein:

   ```
   sc.exe start DeadlineWorker
   ```

2. Überwachen Sie den Mitarbeiter, um sicherzustellen, dass er startet und nach Arbeit fragt.

   Linux

   Führen Sie in einer Root-Shell den folgenden Befehl aus:

```
systemctl status deadline-worker
```

Der Befehl sollte eine Antwort wie die folgende zurückgeben:

```
Active: active (running) since Wed 2023-06-14 14:44:27 UTC; 7min ago
```

Wenn die Antwort nicht so aussieht, überprüfen Sie die Protokolldatei mit dem folgenden Befehl:

```
tail -n 25 /var/log/amazon/deadline/worker-agent.log
```

Windows

Von einer Administrator-Befehlszeile aus oder PowerShell Terminal, geben Sie den folgenden Befehl ein:

```
sc.exe query DeadlineWorker
```

Der Befehl sollte eine Antwort wie die folgende zurückgeben:

```
STATE   : 4 RUNNING
```

Wenn die Antwort keine enthältRUNNING, überprüfen Sie die Worker-Protokolldatei. Öffne und verwalte PowerShell fordern Sie den folgenden Befehl auf und führen Sie ihn aus:

```
Get-Content -Tail 25 -Path $env:PROGRAMDATA\Amazon\Deadline\Logs\worker-
agent.log
```

3. Reichen Sie Jobs in die Warteschlange ein, die mit Ihrer Flotte verknüpft ist. Die Jobs sollten repräsentativ für die Jobs sein, die von der Flotte verarbeitet werden.
4. Überwachen Sie den Fortschritt des Jobs mithilfe des Deadline Cloud-Monitors oder der CLI. Wenn ein Job fehlschlägt, überprüfen Sie die Sitzungs- und Worker-Protokolle.
5. Aktualisieren Sie die Konfiguration des Worker-Hosts nach Bedarf, bis die Jobs erfolgreich abgeschlossen wurden.
6. Wenn die Testjobs erfolgreich waren, können Sie den Worker beenden:

Linux

Führen Sie in einer Root-Shell den folgenden Befehl aus:

```
systemctl stop deadline-worker
```

Windows

Von einer Administrator-Befehlszeile aus oder PowerShell Terminal, geben Sie den folgenden Befehl ein:

```
sc.exe stop DeadlineWorker
```

Erstelle eine Amazon Machine Image

Um ein zu erstellen Amazon Machine Image (AMI) zur Verwendung in einer kundenverwalteten Amazon Elastic Compute Cloud (Amazon EC2) -Flotte (CMF), führen Sie die Aufgaben in diesem Abschnitt aus. Sie müssen eine EC2 Amazon-Instance erstellen, bevor Sie fortfahren können. Weitere Informationen finden Sie unter Starten Ihrer Instance im EC2 Amazon-Benutzerhandbuch für Linux-Instances.

> **Important**
>
> Erstellen eines AMI erstellt einen Snapshot der angehängten Volumes der EC2 Amazon-Instance. Jegliche Software, die auf der Instance installiert ist, bleibt bestehen, sodass Instances wiederverwendet werden, wenn Sie Instances von AMI. Wir empfehlen, eine Patch-Strategie zu verfolgen und alle neuen regelmäßig zu aktualisieren AMI mit aktualisierter Software, bevor Sie sie auf Ihre Flotte anwenden.

Bereiten Sie die EC2 Amazon-Instance vor

Bevor Sie eine erstellen AMI, müssen Sie den Arbeiterstatus löschen. Der Worker-Status bleibt auch zwischen den Starts des Worker-Agents bestehen. Wenn dieser Status auch auf dem AMI, dann haben alle Instances, die von dort aus gestartet werden, denselben Status.

Wir empfehlen außerdem, alle vorhandenen Protokolldateien zu löschen. Protokolldateien können auf einer EC2 Amazon-Instance verbleiben, wenn Sie das AMI vorbereiten. Durch das Löschen dieser Dateien wird Verwirrung bei der Diagnose möglicher Probleme in Arbeiterflotten, die das AMI verwenden, minimiert.

Sie sollten auch den Worker-Agent-Systemdienst aktivieren, damit der Deadline Cloud-Worker-Agent gestartet wird, wenn Amazon gestartet EC2 wird.

Schließlich empfehlen wir Ihnen, das auto Herunterfahren des Worker-Agents zu aktivieren. Auf diese Weise kann die Worker-Flotte bei Bedarf hochskaliert und heruntergefahren werden, wenn der Rendering-Job abgeschlossen ist. Diese auto Skalierung stellt sicher, dass Sie Ressourcen nur nach Bedarf verwenden.

So bereiten Sie die EC2 Amazon-Instance vor

1. Öffnen Sie die EC2 Amazon-Konsole.
2. Starten Sie eine EC2 Amazon-Instance. Weitere Informationen finden Sie unter Starten Sie Ihre Instance.
3. Richten Sie den Host so ein, dass er eine Verbindung zu Ihrem Identity Provider (IdP) herstellt, und mounten Sie dann jedes gemeinsam genutzte Dateisystem, das er benötigt.
4. Folgen Sie den Anleitungen zu Installieren Sie den Deadline Cloud Worker AgentWorker Agent konfigurieren, dann und. Job-Benutzer und Gruppen erstellen
5. Wenn Sie eine vorbereiten AMI basiert auf Amazon Linux 2023, um Software auszuführen, die mit der VFX Reference Platform kompatibel ist, müssen Sie mehrere Anforderungen aktualisieren. Weitere Informationen finden Sie unter Kompatibilität der VFX Reference Platform im AWS Deadline Cloud-Benutzerhandbuch.
6. Öffnen Sie ein -Terminalfenster.
   a. Öffnen Sie unter Linux ein Terminal als `root` Benutzer (oder verwenden Sie`sudo/su`)
   b. Ein Windows, öffnen Sie eine Administrator-Befehlszeile oder ein PowerShell Terminal.
7. Stellen Sie sicher, dass der Worker-Dienst nicht läuft und nicht so konfiguriert ist, dass er beim Booten gestartet wird:
   a. Führen Sie unter Linux Folgendes aus

```
systemctl stop deadline-worker
systemctl enable deadline-worker
```

b. Ein Windows, lauf

```
sc.exe stop DeadlineWorker
sc.exe config DeadlineWorker start= auto
```

8. Löscht den Arbeiterstatus.

a. Führen Sie unter Linux Folgendes aus

```
rm -rf /var/lib/deadline/*
```

b. Ein Windows, lauf

```
del /Q /S %PROGRAMDATA%\Amazon\Deadline\Cache\*
```

9. Löschen Sie die Protokolldateien.

a. Führen Sie unter Linux Folgendes aus

```
rm -rf /var/log/amazon/deadline/*
```

b. Ein Windows, lauf

```
del /Q /S %PROGRAMDATA%\Amazon\Deadline\Logs\*
```

10. Ein Windows, es wird empfohlen, die Anwendung Amazon EC2 Launch Settings im Startmenü auszuführen, um die letzte Vorbereitung und das Herunterfahren der Instance auf dem Host abzuschließen.

> **Note**
>
> Sie MÜSSEN Shutdown without Sysprep wählen und dürfen niemals Shutdown with Sysprep wählen. Beim Herunterfahren mit Sysprep werden alle lokalen Benutzer unbrauchbar. Weitere Informationen finden Sie im Abschnitt Bevor Sie beginnen des Themas Erstellen eines benutzerdefinierten AMIs im Benutzerhandbuch für Windows-Instances.

Erstellen Sie das AMI

Um das zu bauen AMI

1. Öffnen Sie die EC2 Amazon-Konsole.
2. Wählen Sie im Navigationsbereich Instances und dann Ihre Instance aus.
3. Wählen Sie Instanzstatus und dann Instanz beenden aus.
4. Nachdem die Instance gestoppt wurde, wählen Sie Actions aus.
5. Wählen Sie „Bild und Vorlagen“ und anschließend „Bild erstellen“.
6. Geben Sie einen Bildnamen ein.
7. (Optional) Geben Sie eine Beschreibung für Ihr Bild ein.
8. Wählen Sie Create Image (Image erstellen) aus.

Erstellen Sie eine Flotteninfrastruktur mit einer Amazon EC2 Auto Scaling Scaling-Gruppe

In diesem Abschnitt wird erklärt, wie Sie eine Amazon EC2 Auto Scaling Scaling-Flotte erstellen.

Verwenden Sie die folgende AWS CloudFormation YAML-Vorlage, um eine Amazon EC2 Auto Scaling (Auto Scaling) -Gruppe, eine Amazon Virtual Private Cloud (Amazon VPC) mit zwei Subnetzen, einem Instance-Profil und einer Instance-Zugriffsrolle zu erstellen. Diese sind erforderlich, um die Instance mithilfe von Auto Scaling in den Subnetzen zu starten.

Sie sollten die Liste der Instance-Typen überprüfen und aktualisieren, damit sie Ihren Rendering-Anforderungen entspricht.

Eine vollständige Erläuterung der in der CloudFormation YAML-Vorlage verwendeten Ressourcen und Parameter finden Sie in der Referenz zum Deadline Cloud-Ressourcentyp im AWS CloudFormation Benutzerhandbuch.

So erstellen Sie eine Amazon EC2 Auto Scaling Scaling-Flotte

1. Verwenden Sie das folgende Beispiel, um eine CloudFormation Vorlage zu erstellen`FarmID`, die die `AMIId` Parameter`FleetID`, und definiert. Speichern Sie die Vorlage in einer `.YAML` Datei auf Ihrem lokalen Computer.

```
AWSTemplateFormatVersion: 2010-09-09
```

```
Description: Amazon Deadline Cloud customer-managed fleet
Parameters:
  FarmId:
    Type: String
    Description: Farm ID
  FleetId:
    Type: String
    Description: Fleet ID
  AMIId:
    Type: String
    Description: AMI ID for launching workers
Resources:
  deadlineVPC:
    Type: 'AWS::EC2::VPC'
    Properties:
      CidrBlock: 100.100.0.0/16
  deadlineWorkerSecurityGroup:
    Type: 'AWS::EC2::SecurityGroup'
    Properties:
      GroupDescription: !Join
        - ' '
        - - Security group created for Deadline Cloud workers in the fleet
          - !Ref FleetId
      GroupName: !Join
        - ''
        - - deadlineWorkerSecurityGroup-
          - !Ref FleetId
      SecurityGroupEgress:
        - CidrIp: 0.0.0.0/0
          IpProtocol: '-1'
      SecurityGroupIngress: []
      VpcId: !Ref deadlineVPC
  deadlineIGW:
    Type: 'AWS::EC2::InternetGateway'
    Properties: {}
  deadlineVPCGatewayAttachment:
    Type: 'AWS::EC2::VPCGatewayAttachment'
    Properties:
      VpcId: !Ref deadlineVPC
      InternetGatewayId: !Ref deadlineIGW
  deadlinePublicRouteTable:
    Type: 'AWS::EC2::RouteTable'
    Properties:
      VpcId: !Ref deadlineVPC
```

```
  deadlinePublicRoute:
    Type: 'AWS::EC2::Route'
    Properties:
      RouteTableId: !Ref deadlinePublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref deadlineIGW
    DependsOn:
      - deadlineIGW
      - deadlineVPCGatewayAttachment
  deadlinePublicSubnet0:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref deadlineVPC
      CidrBlock: 100.100.16.0/22
      AvailabilityZone: !Join
        - ''
        - - !Ref 'AWS::Region'
          - a
  deadlineSubnetRouteTableAssociation0:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref deadlinePublicRouteTable
      SubnetId: !Ref deadlinePublicSubnet0
  deadlinePublicSubnet1:
    Type: 'AWS::EC2::Subnet'
    Properties:
      VpcId: !Ref deadlineVPC
      CidrBlock: 100.100.20.0/22
      AvailabilityZone: !Join
        - ''
        - - !Ref 'AWS::Region'
          - c
  deadlineSubnetRouteTableAssociation1:
    Type: 'AWS::EC2::SubnetRouteTableAssociation'
    Properties:
      RouteTableId: !Ref deadlinePublicRouteTable
      SubnetId: !Ref deadlinePublicSubnet1
  deadlineInstanceAccessAccessRole:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: !Join
        - '-'
        - - deadline
          - InstanceAccess
```

```
          - !Ref FleetId
      AssumeRolePolicyDocument:
        Statement:
          - Effect: Allow
            Principal:
              Service: ec2.amazonaws.com
            Action:
              - 'sts:AssumeRole'
      Path: /
      ManagedPolicyArns:
        - 'arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy'
        - 'arn:aws:iam::aws:policy/AmazonSSMManagedInstanceCore'
        - 'arn:aws:iam::aws:policy/AWSDeadlineCloud-WorkerHost'
  deadlineInstanceProfile:
    Type: 'AWS::IAM::InstanceProfile'
    Properties:
      Path: /
      Roles:
        - !Ref deadlineInstanceAccessAccessRole
  deadlineLaunchTemplate:
    Type: 'AWS::EC2::LaunchTemplate'
    Properties:
      LaunchTemplateName: !Join
        - ''
        - - deadline-LT-
          - !Ref FleetId
      LaunchTemplateData:
        NetworkInterfaces:
          - DeviceIndex: 0
            AssociatePublicIpAddress: true
            Groups:
              - !Ref deadlineWorkerSecurityGroup
            DeleteOnTermination: true
        ImageId: !Ref AMIId
        InstanceInitiatedShutdownBehavior: terminate
        IamInstanceProfile:
          Arn: !GetAtt
            - deadlineInstanceProfile
            - Arn
        MetadataOptions:
          HttpTokens: required
          HttpEndpoint: enabled

  deadlineAutoScalingGroup:
```

```
    Type: 'AWS::AutoScaling::AutoScalingGroup'
    Properties:
      AutoScalingGroupName: !Join
        - ''
        - - deadline-ASG-autoscalable-
          - !Ref FleetId
      MinSize: 0
      MaxSize: 10
      VPCZoneIdentifier:
        - !Ref deadlinePublicSubnet0
        - !Ref deadlinePublicSubnet1
      NewInstancesProtectedFromScaleIn: true
      MixedInstancesPolicy:
        InstancesDistribution:
          OnDemandBaseCapacity: 0
          OnDemandPercentageAboveBaseCapacity: 0
          SpotAllocationStrategy: capacity-optimized
          OnDemandAllocationStrategy: lowest-price
        LaunchTemplate:
          LaunchTemplateSpecification:
            LaunchTemplateId: !Ref deadlineLaunchTemplate
            Version: !GetAtt
              - deadlineLaunchTemplate
              - LatestVersionNumber
          Overrides:
            - InstanceType: m5.large
            - InstanceType: m5d.large
            - InstanceType: m5a.large
            - InstanceType: m5ad.large
            - InstanceType: m5n.large
            - InstanceType: m5dn.large
            - InstanceType: m4.large
            - InstanceType: m3.large
            - InstanceType: r5.large
            - InstanceType: r5d.large
            - InstanceType: r5a.large
            - InstanceType: r5ad.large
            - InstanceType: r5n.large
            - InstanceType: r5dn.large
            - InstanceType: r4.large
      MetricsCollection:
        - Granularity: 1Minute
          Metrics:
            - GroupMinSize
```

```
            - GroupMaxSize
            - GroupDesiredCapacity
            - GroupInServiceInstances
            - GroupTotalInstances
            - GroupInServiceCapacity
            - GroupTotalCapacity
```

2. Öffnen Sie die AWS CloudFormation Konsole unter https://console.aws.amazon.com/cloudformation.

   Verwenden Sie die AWS CloudFormation Konsole, um einen Stack anhand der Anweisungen zum Hochladen der von Ihnen erstellten Vorlagendatei zu erstellen. Weitere Informationen finden Sie im AWS CloudFormation Benutzerhandbuch unter Erstellen eines Stacks auf der AWS CloudFormation Konsole.

> **Note**
>
> - Anmeldeinformationen aus der IAM-Rolle, die an die EC2 Amazon-Instance Ihres Workers angehängt sind, sind für alle Prozesse verfügbar, die auf diesem Worker ausgeführt werden, einschließlich Jobs. Der Worker sollte die geringsten Betriebsberechtigungen haben: `deadline:CreateWorker` und `deadline:AssumeFleetRoleForWorker`.
> - Der Worker-Agent ruft die Anmeldeinformationen für die Warteschlangenrolle ab und konfiguriert sie für die Verwendung bei der Ausführung von Jobs. Die EC2 Amazon-Instance-Profilrolle sollte keine Berechtigungen enthalten, die für Ihre Jobs erforderlich sind.

Skalieren Sie Ihre EC2 Amazon-Flotte automatisch mit der Deadline Cloud-Funktion für Skalierungsempfehlungen

Deadline Cloud nutzt eine Amazon EC2 Auto Scaling-Gruppe (Auto Scaling), um die EC2 kundenverwaltete Amazon-Flotte (CMF) automatisch zu skalieren. Sie müssen den Flottenmodus konfigurieren und die erforderliche Infrastruktur in Ihrem Konto bereitstellen, damit Ihre Flotte auto skaliert werden kann. Die von Ihnen bereitgestellte Infrastruktur funktioniert für alle Flotten, sodass Sie sie nur einmal einrichten müssen.

Der grundlegende Arbeitsablauf ist: Sie konfigurieren Ihren Flottenmodus so, dass er auto skaliert, und dann sendet Deadline Cloud ein EventBridge Ereignis für diese Flotte aus, wenn sich die

empfohlene Flottengröße ändert (ein Ereignis enthält die Flotten-ID, die empfohlene Flottengröße und andere Metadaten). Sie werden eine EventBridge Regel haben, um die relevanten Ereignisse zu filtern, und ein Lambda, um sie zu verarbeiten. Das Lambda wird in Amazon EC2 Auto Scaling integriert`AutoScalingGroup`, um die EC2 Amazon-Flotte automatisch zu skalieren.

Stellen Sie den Flottenmodus auf **`EVENT_BASED_AUTO_SCALING`**

Konfigurieren Sie Ihren Flottenmodus auf`EVENT_BASED_AUTO_SCALING`. Sie können dazu die Konsole verwenden oder die verwenden, AWS CLI um die `CreateFleet` `UpdateFleet` OR-API direkt aufzurufen. Nachdem der Modus konfiguriert wurde, beginnt Deadline Cloud mit dem Senden von EventBridge Ereignissen, sobald sich die empfohlene Flottengröße ändert.

- `UpdateFleet`Beispielbefehl:

```
aws deadline update-fleet \
  --farm-id FARM_ID \
  --fleet-id FLEET_ID \
  --configuration file://configuration.json
```

- `CreateFleet`Beispielbefehl:

```
aws deadline create-fleet \
  --farm-id FARM_ID \
  --display-name "Fleet name" \
  --max-worker-count 10 \
  --configuration file://configuration.json
```

Das Folgende ist ein Beispiel für die `configuration.json` Verwendung in den obigen CLI-Befehlen (`--configuration file://configuration.json`).

- Um Auto Scaling für Ihre Flotte zu aktivieren, sollten Sie den Modus auf einstellen`EVENT_BASED_AUTO_SCALING`.
- Dies `workerCapabilities` sind die Standardwerte, die dem CMF bei der Erstellung zugewiesen wurden. Sie können diese Werte ändern, wenn Sie mehr Ressourcen benötigen, die Ihrem CMF zur Verfügung stehen.

Nachdem Sie den Flottenmodus konfiguriert haben, sendet Deadline Cloud Ereignisse mit Empfehlungen zur Flottengröße für diese Flotte aus.

```
{
    "customerManaged": {
        "mode": "EVENT_BASED_AUTO_SCALING",
        "workerCapabilities": {
            "vCpuCount": {
                "min": 1,
                "max": 4
            },
            "memoryMiB": {
                "min": 1024,
                "max": 4096
            },
            "osFamily": "linux",
            "cpuArchitectureType": "x86_64"
        }
    }
}
```

Stellen Sie den Auto Scaling Scaling-Stack mithilfe der AWS CloudFormation Vorlage bereit

Sie können eine EventBridge Regel zum Filtern von Ereignissen, ein Lambda zum Verwerten der Ereignisse und zur Steuerung von Auto Scaling und eine SQS-Warteschlange zum Speichern unverarbeiteter Ereignisse einrichten. Verwenden Sie die folgende AWS CloudFormation Vorlage, um alles in einem Stack bereitzustellen. Nachdem Sie die Ressourcen erfolgreich bereitgestellt haben, können Sie einen Auftrag einreichen und die Flotte wird automatisch skaliert.

```
Resources:
  AutoScalingLambda:
    Type: 'AWS::Lambda::Function'
    Properties:
      Code:
        ZipFile: |-
          """
          This lambda is configured to handle "Fleet Size Recommendation Change"
          messages. It will handle all such events, and requires
          that the ASG is named based on the fleet id. It will scale up/down the fleet
          based on the recommended fleet size in the message.

          Example EventBridge message:
          {
              "version": "0",
              "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
```

```
            "detail-type": "Fleet Size Recommendation Change",
            "source": "aws.deadline",
            "account": "111122223333",
            "time": "2017-12-22T18:43:48Z",
            "region": "us-west-1",
            "resources": [],
            "detail": {
                "farmId": "farm-12345678900000000000000000000000",
                "fleetId": "fleet-12345678900000000000000000000000",
                "oldFleetSize": 1,
                "newFleetSize": 5,
            }
        }
        """

        import json
        import boto3
        import logging

        logger = logging.getLogger()
        logger.setLevel(logging.INFO)

        auto_scaling_client = boto3.client("autoscaling")

        def lambda_handler(event, context):
            logger.info(event)
            event_detail = event["detail"]
            fleet_id = event_detail["fleetId"]
            desired_capacity = event_detail["newFleetSize"]

            asg_name = f"deadline-ASG-autoscalable-{fleet_id}"
            auto_scaling_client.set_desired_capacity(
                AutoScalingGroupName=asg_name,
                DesiredCapacity=desired_capacity,
                HonorCooldown=False,
            )

            return {
                'statusCode': 200,
                'body': json.dumps(f'Successfully set desired_capacity for {asg_name}
to {desired_capacity}')
            }
    Handler: index.lambda_handler
    Role: !GetAtt
```

```
        - AutoScalingLambdaServiceRole
        - Arn
      Runtime: python3.11
    DependsOn:
      - AutoScalingLambdaServiceRoleDefaultPolicy
      - AutoScalingLambdaServiceRole
  AutoScalingEventRule:
    Type: 'AWS::Events::Rule'
    Properties:
      EventPattern:
        source:
          - aws.deadline
        detail-type:
          - Fleet Size Recommendation Change
      State: ENABLED
      Targets:
        - Arn: !GetAtt
            - AutoScalingLambda
            - Arn
          DeadLetterConfig:
            Arn: !GetAtt
              - UnprocessedAutoScalingEventQueue
              - Arn
          Id: Target0
          RetryPolicy:
            MaximumRetryAttempts: 15
  AutoScalingEventRuleTargetPermission:
    Type: 'AWS::Lambda::Permission'
    Properties:
      Action: 'lambda:InvokeFunction'
      FunctionName: !GetAtt
        - AutoScalingLambda
        - Arn
      Principal: events.amazonaws.com
      SourceArn: !GetAtt
        - AutoScalingEventRule
        - Arn
  AutoScalingLambdaServiceRole:
    Type: 'AWS::IAM::Role'
    Properties:
      AssumeRolePolicyDocument:
        Statement:
          - Action: 'sts:AssumeRole'
            Effect: Allow
```

```
            Principal:
              Service: lambda.amazonaws.com
        Version: 2012-10-17
      ManagedPolicyArns:
        - !Join
          - ''
          - - 'arn:'
            - !Ref 'AWS::Partition'
            - ':iam::aws:policy/service-role/AWSLambdaBasicExecutionRole'
  AutoScalingLambdaServiceRoleDefaultPolicy:
    Type: 'AWS::IAM::Policy'
    Properties:
      PolicyDocument:
        Statement:
          - Action: 'autoscaling:SetDesiredCapacity'
            Effect: Allow
            Resource: '*'
        Version: 2012-10-17
      PolicyName: AutoScalingLambdaServiceRoleDefaultPolicy
      Roles:
        - !Ref AutoScalingLambdaServiceRole
  UnprocessedAutoScalingEventQueue:
    Type: 'AWS::SQS::Queue'
    Properties:
      QueueName: deadline-unprocessed-autoscaling-events
    UpdateReplacePolicy: Delete
    DeletionPolicy: Delete
  UnprocessedAutoScalingEventQueuePolicy:
    Type: 'AWS::SQS::QueuePolicy'
    Properties:
      PolicyDocument:
        Statement:
          - Action: 'sqs:SendMessage'
            Condition:
              ArnEquals:
                'aws:SourceArn': !GetAtt
                  - AutoScalingEventRule
                  - Arn
            Effect: Allow
            Principal:
              Service: events.amazonaws.com
            Resource: !GetAtt
              - UnprocessedAutoScalingEventQueue
              - Arn
```

```
        Version: 2012-10-17
      Queues:
        - !Ref UnprocessedAutoScalingEventQueue
```

Führen Sie einen Flottenzustandscheck durch

Nachdem Sie Ihre Flotte erstellt haben, sollten Sie einen individuellen Zustandscheck erstellen, um sicherzustellen, dass Ihre Flotte fehlerfrei bleibt und keine blockierten Instanzen auftreten, um unnötige Kosten zu vermeiden. Weitere Informationen finden Sie unter Bereitstellung eines Deadline Cloud-Flottenzustandschecks. GitHub Dadurch kann das Risiko einer versehentlichen Änderung Ihres Amazon Machine Image, Startvorlage oder Netzwerkkonfiguration, die unentdeckt läuft.

Konfiguration und Verwendung von vom Service verwalteten Deadline Cloud-Flotten

Eine Service-Managed Fleet (SMF) ist eine Sammlung von Mitarbeitern, die von Deadline Cloud verwaltet werden. Ein SMF macht die Verwaltung der Flottenskalierung zur Bearbeitung von Anforderungen oder die Reduzierung der Flottengröße nach Abschluss einer Aufgabe überflüssig.

Wenn ein SMF mithilfe der standardmäßigen Conda-Warteschlangenumgebung einer Warteschlange zugeordnet wird, konfiguriert Deadline Cloud die Mitarbeiter in der Flotte mit dem entsprechenden Softwarepaket. Informationen zu unterstützten Partneranwendungen finden Sie unter Standard-Conda-Warteschlangenumgebung im AWS Deadline Cloud-Benutzerhandbuch.

In den meisten Fällen müssen Sie ein SMF nicht ändern, um Ihre Workloads zu verarbeiten. In einigen Situationen müssen Sie jedoch möglicherweise Änderungen an Ihren Flotten vornehmen. Dazu zählen:

- Ausführen von Skripts, für die zum Installieren von Software oder Docker Containern erhöhte Berechtigungen erforderlich sind.

Themen

Führen Sie Skripts als Administrator aus, um Worker zu konfigurieren

Mithilfe von benutzerdefinierten Skripten für die Konfiguration von Fleet-Hosts können Sie administrative Aufgaben, wie z. B. die Softwareinstallation, für Ihre vom Service verwalteten Flottenmitarbeiter ausführen. Diese Skripts werden mit erhöhten Rechten ausgeführt, sodass Sie Ihre Mitarbeiter flexibel für Ihr System konfigurieren können.

Deadline Cloud führt das Skript aus, nachdem der Worker den `STARTING` Status erreicht hat und bevor er irgendwelche Aufgaben ausführt.

> **Important**
>
> Das Skript wird mit erhöhten Rechten `sudo` auf Linux Systemen und mit „Administrator“ auf Windows Systemen ausgeführt. Es liegt in Ihrer Verantwortung sicherzustellen, dass das Skript keine Sicherheitsprobleme verursacht.
> Wenn Sie ein Admin-Skript verwenden, sind Sie dafür verantwortlich, den Zustand Ihrer Flotte zu überwachen.

Zu den häufigsten Verwendungszwecken des Skripts gehören:

- Installation von Software, für die Administratorzugriff erforderlich ist
- Installation von Docker Containern

Sie können ein Host-Konfigurationsskript mit der Konsole oder mit dem erstellen und aktualisieren AWS CLI.

Console

1. Wählen Sie auf der Seite mit den Flottendetails die Registerkarte Konfigurationen aus.
2. Geben Sie im Feld Skript das Skript ein, das mit erhöhten Rechten ausgeführt werden soll. Sie können Import wählen, um ein Skript von Ihrer Workstation zu laden.
3. Legen Sie eine Zeitüberschreitung in Sekunden für die Ausführung des Skripts fest. Der Standardwert ist 300 Sekunden (5 Minuten).
4. Wählen Sie Änderungen speichern, um das Skript zu speichern.

Create with CLI

Verwenden Sie den folgenden AWS CLI Befehl, um eine Flotte mit einem Host-Konfigurationsskript zu erstellen. Ersetzen Sie den *`placeholder`* Text durch Ihre Informationen.

```
aws deadline-internal create-fleet \
--farm-id farm-12345 \
--display-name "fleet-name" \
--max-worker-count 1 \
--configuration '{
  "serviceManagedEc2": {
```

```
    "instanceCapabilities": {
      "vCpuCount": {"min": 2},
      "memoryMiB": {"min": 4096},
      "osFamily": "linux",
      "cpuArchitectureType": "x86_64"
    },
    "instanceMarketOptions": {"type":"spot"}
  }
}' \
--role-arn arn:aws:iam::111122223333:role/role-name \
--host-configuration '{ "scriptBody": "script body", "scriptTimeoutSeconds": timeout
 value}'
```

Update with CLI

Verwenden Sie den folgenden AWS CLI Befehl, um das Host-Konfigurationsskript einer Flotte zu aktualisieren. Ersetzen Sie den *placeholder* Text durch Ihre Informationen.

```
aws deadline update-fleet \
--farm-id farm-12345 \
--fleet-id fleet-455678 \
--host-configuration '{ "scriptBody": "script body", "scriptTimeoutSeconds": timeout
 value}'
```

Die folgenden Skripte demonstrieren:

- Die für das Skript verfügbaren Umgebungsvariablen
- Diese AWS Anmeldeinformationen funktionieren in der Shell
- Dass das Skript in einer Shell mit erhöhten Rechten ausgeführt wird

Linux

Verwenden Sie das folgende Skript, um zu zeigen, dass ein Skript mit `root` Rechten ausgeführt wird:

```
# Print environment variables
set
# Check AWS Credentials
aws sts get-caller-identity
```

Windows

Verwenden Sie das folgende PowerShell Skript, um zu zeigen, dass ein Skript mit Administratorrechten ausgeführt wird:

```
Get-ChildItem env: | ForEach-Object { "$($_.Name)=$($_.Value)" }
aws sts get-caller-identity
function Test-AdminPrivileges {
    $currentUser = New-Object
 Security.Principal.WindowsPrincipal([Security.Principal.WindowsIdentity]::GetCurrent())
    $isAdmin =
 $currentUser.IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)

    return $isAdmin
}

if (Test-AdminPrivileges) {
    Write-Host "The current PowerShell session is elevated (running as
 Administrator)."
} else {
    Write-Host "The current PowerShell session is not elevated (not running as
 Administrator)."
}
exit 0
```

Fehlerbehebung bei Host-Konfigurationsskripten

Wenn Sie das Host-Konfigurationsskript ausführen:

- Bei Erfolg: Der Worker führt den Job aus
- Bei einem Fehler (Exit-Code ungleich Null oder Absturz):
  - Der Worker wird heruntergefahren

  Die Flotte startet automatisch einen neuen Worker unter Verwendung des neuesten Host-Konfigurationsskripts

Um das Skript zu überwachen:

1. Öffnen Sie die Flottenseite in der Deadline Cloud-Konsole
2. Wählen Sie Mitarbeiter anzeigen, um den Deadline Cloud-Monitor zu öffnen

3. Sehen Sie sich den Mitarbeiterstatus auf der Monitorseite an

Wichtige Hinweise:

- Mitarbeiter, die aufgrund eines Fehlers heruntergefahren wurden, sind in der Worker-Liste im Monitor nicht verfügbar. Verwenden Sie CloudWatch Logs, um die Worker-Logs in der folgenden Protokollgruppe einzusehen:

  ```
  /aws/deadline/farm-XXXXX/fleet-YYYYY
  ```

  Innerhalb dieser Protokollgruppe befindet sich ein Stream von

  ```
  worker-ZZZZZ
  ```

- CloudWatch Logs speichert Worker-Protokolle entsprechend der von Ihnen konfigurierten Aufbewahrungsfrist.

Verwendung von Softwarelizenzen mit Deadline Cloud

Deadline Cloud bietet zwei Methoden zur Bereitstellung von Softwarelizenzen für Ihre Jobs:

- Nutzungsbasierte Lizenzierung (UBL) — Nachverfolgung und Abrechnung basieren auf der Anzahl der Stunden, die Ihre Flotte für die Bearbeitung eines Auftrags benötigt. Es gibt keine festgelegte Anzahl an Lizenzen, sodass Ihre Flotte nach Bedarf skaliert werden kann. UBL ist Standard für servicemanagierte Flotten. Für vom Kunden verwaltete Flotten können Sie einen Deadline Cloud-Lizenzendpunkt für UBL verbinden. UBL stellt Lizenzen für Ihre Deadline Cloud-Mitarbeiter zum Rendern bereit, stellt jedoch keine Lizenzen für Ihre DCC-Anwendungen bereit.
- Bring Your Own License (BYOL) — ermöglicht es Ihnen, bestehende Softwarelizenzen mit Ihren vom Service oder vom Kunden verwalteten Flotten zu verwenden. Sie können BYOL verwenden, um eine Verbindung zu Lizenzservern für Software herzustellen, die nicht von den nutzungsbasierten Lizenzen von Deadline Cloud unterstützt wird. Sie können BYOL mit vom Service verwalteten Flotten verwenden, indem Sie eine Verbindung zu einem benutzerdefinierten Lizenzserver herstellen.

Themen

Connect vom Service verwaltete Flotten mit einem benutzerdefinierten Lizenzserver

Sie können Ihren eigenen Lizenzserver verwenden, um ihn mit einer vom Service verwalteten Deadline Cloud-Flotte zu verwenden. Um Ihre eigene Lizenz mitzubringen, können Sie einen Lizenzserver mithilfe einer Warteschlangenumgebung in Ihrer Farm konfigurieren. Um Ihren Lizenzserver zu konfigurieren, sollten Sie bereits eine Farm und eine Warteschlange eingerichtet haben.

Wie Sie eine Verbindung zu einem Softwarelizenzserver herstellen, hängt von der Konfiguration Ihrer Flotte und den Anforderungen des Softwareanbieters ab. In der Regel greifen Sie auf zwei Arten auf den Server zu:

- Direkt zum Lizenzserver. Ihre Mitarbeiter erhalten über das Internet eine Lizenz vom Lizenzserver des Softwareanbieters. Alle Ihre Mitarbeiter müssen in der Lage sein, eine Verbindung zum Server herzustellen.
- Über einen Lizenz-Proxy. Ihre Mitarbeiter stellen eine Verbindung zu einem Proxyserver in Ihrem lokalen Netzwerk her. Nur der Proxyserver darf über das Internet eine Verbindung zum Lizenzserver des Anbieters herstellen.

Mit den folgenden Anweisungen verwenden Sie Amazon EC2 Systems Manager (SSM), um Ports von einer Worker-Instance an Ihren Lizenzserver oder Ihre Proxy-Instance weiterzuleiten.

Themen

Schritt 1: Konfigurieren Sie die Warteschlangenumgebung

Sie können in Ihrer Warteschlange eine Warteschlangenumgebung für den Zugriff auf Ihren Lizenzserver konfigurieren. Stellen Sie zunächst sicher, dass Sie eine AWS Instanz mit Lizenzserverzugriff konfiguriert haben, indem Sie eine der folgenden Methoden verwenden:

- Lizenzserver — Die Instanz hostet die Lizenzserver direkt.
- Lizenzproxy — Die Instanz hat Netzwerkzugriff auf den Lizenzserver und leitet die Lizenzserverports an den Lizenzserver weiter. Einzelheiten zur Konfiguration einer Lizenz-Proxyinstanz finden Sie unterSchritt 2: (Optional) Einrichtung der Lizenz-Proxyinstanz.

So fügen Sie der Warteschlangenrolle die erforderlichen Berechtigungen hinzu

1. Wählen Sie in der Deadline Cloud-Konsole die Option Gehe zum Dashboard aus.
2. Wählen Sie im Dashboard die Farm und dann die Warteschlange aus, die Sie konfigurieren möchten.
3. Wählen Sie unter Warteschlangendetails > Servicerolle die Rolle aus.
4. Wählen Sie „Berechtigung hinzufügen“ und anschließend „Inline-Richtlinie erstellen“.

5. Wählen Sie den JSON-Richtlinieneditor aus, kopieren Sie dann den folgenden Text und fügen Sie ihn in den Editor ein.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Action": [
                "ssm:StartSession"
            ],
            "Resource": [
                "arn:aws:ssm:region::document/AWS-StartPortForwardingSession",
                "arn:aws:ec2:region:account_id:instance/instance_id"
            ]
        }
    ]
}
```

6. Bevor Sie die neue Richtlinie speichern, ersetzen Sie die folgenden Werte im Richtlinientext:

   - `region`Ersetzen Sie durch die AWS Region, in der sich Ihre Farm befindet
   - `instance_id`Ersetzen Sie es durch die Instanz-ID für den Lizenzserver oder die Proxyinstanz, die Sie verwenden
   - `account_id`Ersetzen Sie es durch die AWS Kontonummer, die Ihre Farm enthält
7. Wählen Sie Weiter aus.
8. Geben Sie als Namen der Richtlinie ein**`LicenseForwarding`**.
9. Wählen Sie Richtlinie erstellen aus, um Ihre Änderungen zu speichern und die Richtlinie mit den erforderlichen Berechtigungen zu erstellen.

Um der Warteschlange eine neue Warteschlangenumgebung hinzuzufügen

1. Wählen Sie in der Deadline Cloud-Konsole Gehe zum Dashboard, falls Sie dies noch nicht getan haben.
2. Wählen Sie im Dashboard die Farm und dann die Warteschlange aus, die Sie konfigurieren möchten.

3. Wählen Sie „Warteschlangenumgebungen“ > „Aktionen“ > „Mit YAML neu erstellen“.
4. Kopieren Sie den folgenden Text und fügen Sie ihn in den YAML-Skripteditor ein.

   Windows

```
specificationVersion: "environment-2023-09"
parameterDefinitions:
  - name: LicenseInstanceId
    type: STRING
    description: >
      The Instance ID of the license server/proxy instance
    default: ""
  - name: LicenseInstanceRegion
    type: STRING
    description: >
      The region containing this farm
    default: ""
  - name: LicensePorts
    type: STRING
    description: >
      Comma-separated list of ports to be forwarded to the license server/proxy
 instance.
      Example: "2700,2701,2702"
    default: ""
environment:
  name: BYOL License Forwarding
  variables:
    example_LICENSE: 2700@localhost
  script:
    actions:
      onEnter:
        command: powershell
        args: [ "{{Env.File.Enter}}"]
      onExit:
        command: powershell
        args: [ "{{Env.File.Exit}}" ]
    embeddedFiles:
      - name: Enter
        filename: enter.ps1
        type: TEXT
        runnable: True
        data: |
```

```
          $ZIP_NAME="SessionManagerPlugin.zip"
          Invoke-WebRequest -Uri "https://s3.amazonaws.com/session-manager-
downloads/plugin/latest/windows/$ZIP_NAME" -OutFile $ZIP_NAME
          Expand-Archive -Path $ZIP_NAME
          Expand-Archive -Path .\SessionManagerPlugin\package.zip
          conda activate
          python {{Env.File.StartSession}} {{Session.WorkingDirectory}}\package
\bin\session-manager-plugin.exe
      - name: Exit
        filename: exit.ps1
        type: TEXT
        runnable: True
        data: |
          Write-Output "Killing SSM Manager Plugin PIDs: $env:BYOL_SSM_PIDS"
          "$env:BYOL_SSM_PIDS".Split(",") | ForEach {
            Write-Output "Killing $_"
            Stop-Process -Id $_ -Force
          }
      - name: StartSession
        type: TEXT
        data: |
          import boto3
          import json
          import subprocess
          import sys

          instance_id = "{{Param.LicenseInstanceId}}"
          region = "{{Param.LicenseInstanceRegion}}"
          license_ports_list = "{{Param.LicensePorts}}".split(",")

          ssm_client = boto3.client("ssm", region_name=region)
          pids = []

          for port in license_ports_list:
            session_response = ssm_client.start_session(
              Target=instance_id,
              DocumentName="AWS-StartPortForwardingSession",
              Parameters={"portNumber": [port], "localPortNumber": [port]}
            )

            cmd = [
              sys.argv[1],
              json.dumps(session_response),
              region,
```

```
              "StartSession",
              "",
              json.dumps({"Target": instance_id}),
              f"https://ssm.{region}.amazonaws.com"
            ]

            process = subprocess.Popen(cmd, stdout=subprocess.DEVNULL,
 stderr=subprocess.DEVNULL)
            pids.append(process.pid)
            print(f"SSM Port Forwarding Session started for port {port}")

          print(f"openjd_env: BYOL_SSM_PIDS={','.join(str(pid) for pid in
 pids)}")
```

Linux

```
specificationVersion: "environment-2023-09"
parameterDefinitions:
  - name: LicenseInstanceId
    type: STRING
    description: >
      The Instance ID of the license server/proxy instance
    default: ""
  - name: LicenseInstanceRegion
    type: STRING
    description: >
      The region containing this farm
    default: ""
  - name: LicensePorts
    type: STRING
    description: >
      Comma-separated list of ports to be forwarded to the license server/proxy
 instance.
      Example: "2700,2701,2702"
    default: ""
environment:
  name: BYOL License Forwarding
  variables:
    example_LICENSE: 2700@localhost
  script:
    actions:
```

```
      onEnter:
        command: bash
        args: [ "{{Env.File.Enter}}"]
      onExit:
        command: bash
        args: [ "{{Env.File.Exit}}" ]
    embeddedFiles:
      - name: Enter
        type: TEXT
        runnable: True
        data: |
          curl https://s3.amazonaws.com/session-manager-downloads/plugin/
latest/linux_64bit/session-manager-plugin.rpm -Ls | rpm2cpio - | cpio -iv
 --to-stdout ./usr/local/sessionmanagerplugin/bin/session-manager-plugin >
 {{Session.WorkingDirectory}}/session-manager-plugin
          chmod +x {{Session.WorkingDirectory}}/session-manager-plugin
          conda activate
          python {{Env.File.StartSession}} {{Session.WorkingDirectory}}/session-
manager-plugin
      - name: Exit
        type: TEXT
        runnable: True
        data: |
          echo Killing SSM Manager Plugin PIDs: $BYOL_SSM_PIDS
          for pid in ${BYOL_SSM_PIDS//,/ }; do kill $pid; done
      - name: StartSession
        type: TEXT
        data: |
          import boto3
          import json
          import subprocess
          import sys

          instance_id = "{{Param.LicenseInstanceId}}"
          region = "{{Param.LicenseInstanceRegion}}"
          license_ports_list = "{{Param.LicensePorts}}".split(",")

          ssm_client = boto3.client("ssm", region_name=region)
          pids = []

          for port in license_ports_list:
            session_response = ssm_client.start_session(
              Target=instance_id,
              DocumentName="AWS-StartPortForwardingSession",
```

```
            Parameters={"portNumber": [port], "localPortNumber": [port]}
          )

          cmd = [
            sys.argv[1],
            json.dumps(session_response),
            region,
            "StartSession",
            "",
            json.dumps({"Target": instance_id}),
            f"https://ssm.{region}.amazonaws.com"
          ]

          process = subprocess.Popen(cmd, stdout=subprocess.DEVNULL,
stderr=subprocess.DEVNULL)
          pids.append(process.pid)
          print(f"SSM Port Forwarding Session started for port {port}")

        print(f"openjd_env: BYOL_SSM_PIDS={','.join(str(pid) for pid in
pids)}")
```

5. Nehmen Sie vor dem Speichern der Warteschlangenumgebung nach Bedarf die folgenden Änderungen am Umgebungstext vor:

   - Aktualisieren Sie die Standardwerte für die folgenden Parameter entsprechend Ihrer Umgebung:
     - LicenseInstanceID — Die EC2 Amazon-Instance-ID Ihres Lizenzservers oder Ihrer Proxy-Instance
     - LicenseInstanceRegion— Die AWS Region, in der sich Ihre Farm befindet
     - LicensePorts— Eine durch Kommas getrennte Liste von Ports, die an den Lizenzserver oder die Proxyinstanz weitergeleitet werden sollen (z. B. 2700,2701)
   - Fügen Sie dem Variablenbereich alle erforderlichen Umgebungsvariablen für die Lizenzierung hinzu. Diese Variablen sollten den Link DCCs zu localhost auf dem Lizenzserverport weiterleiten. Wenn Ihr Foundry-Lizenzserver beispielsweise Port 6101 abhört, würden Sie die Variable als hinzufügen. **`foundry_LICENSE: 6101@localhost`**

6. (Optional) Sie können die Priorität auf 0 belassen oder sie so ändern, dass die Priorität in Umgebungen mit mehreren Warteschlangen unterschiedlich angeordnet wird.

7. Wählen Sie „Warteschlangenumgebung erstellen“, um die neue Umgebung zu speichern.

Wenn die Warteschlangenumgebung eingerichtet ist, rufen Aufträge, die an diese Warteschlange gesendet werden, Lizenzen vom konfigurierten Lizenzserver ab.

Schritt 2: (Optional) Einrichtung der Lizenz-Proxyinstanz

Als Alternative zur Verwendung eines Lizenzservers können Sie einen Lizenzproxy verwenden. Um einen Lizenz-Proxy zu erstellen, erstellen Sie eine neue Amazon Linux 2023-Instance, die Netzwerkzugriff auf den Lizenzserver hat. Bei Bedarf können Sie diesen Zugriff über eine VPN-Verbindung konfigurieren. Weitere Informationen finden Sie unter VPN-Verbindungen im Amazon VPC-Benutzerhandbuch.

Um eine Lizenz-Proxyinstanz für Deadline Cloud einzurichten, folgen Sie den Schritten in diesem Verfahren. Führen Sie die folgenden Konfigurationsschritte auf dieser neuen Instanz durch, um die Weiterleitung des Lizenzverkehrs an Ihren Lizenzserver zu ermöglichen

1. Um das HAProxy Paket zu installieren, geben Sie Folgendes ein

```
sudo yum install haproxy
```

2. Aktualisieren Sie den Abschnitt listen license-server der Konfigurationsdatei/etc/haproxy/haproxy.cfg wie folgt:

   a. Ersetzen Sie LicensePort1 und LicensePort2 durch die Portnummern, die an den Lizenzserver weitergeleitet werden sollen. Fügen Sie kommagetrennte Werte hinzu oder entfernen Sie sie, um der erforderlichen Anzahl von Anschlüssen gerecht zu werden.

   b. LicenseServerHostErsetzen Sie durch den Hostnamen oder die IP-Adresse des Lizenzservers.

```
lobal
    log         127.0.0.1 local2
    chroot      /var/lib/haproxy
    user        haproxy
    group       haproxy
    daemon

defaults
    timeout queue           1m
    timeout connect         10s
```

```
    timeout client          1m
    timeout server          1m
    timeout http-keep-alive 10s
    timeout check           10s

listen license-server
     bind *:LicensePort1,*:LicensePort2
     server license-server LicenseServerHost
```

3. Führen Sie die folgenden Befehle aus, um den HAProxy Dienst zu aktivieren und zu starten:

```
sudo systemctl enable haproxy
sudo service haproxy start
```

Nach Abschluss der Schritte sollten Lizenzanfragen, die aus der Weiterleitungswarteschlangenumgebung an localhost gesendet werden, an den angegebenen Lizenzserver weitergeleitet werden.

Schritt 3: Einrichtung der AWS CloudFormation Vorlage

Sie können eine AWS CloudFormation Vorlage verwenden, um eine gesamte Farm so zu konfigurieren, dass sie Ihre eigene Lizenzierung verwendet.

1. Ändern Sie die im nächsten Schritt bereitgestellte Vorlage, um dem Variablenbereich unter Umgebung alle erforderlichen BYOLQueueUmgebungsvariablen für die Lizenzierung hinzuzufügen.
2. Verwenden Sie die folgende AWS CloudFormation Vorlage.

```
AWSTemplateFormatVersion: 2010-09-09
Description: "Create Deadline Cloud resources for BYOL"

Parameters:
  LicenseInstanceId:
    Type: AWS::EC2::Instance::Id
    Description: Instance ID for the license server/proxy instance
  LicensePorts:
    Type: String
    Description: Comma-separated list of ports to forward to the license instance

Resources:
```

```
  JobAttachmentBucket:
    Type: AWS::S3::Bucket
    Properties:
      BucketName: !Sub byol-example-ja-bucket-${AWS::AccountId}-${AWS::Region}
      BucketEncryption:
        ServerSideEncryptionConfiguration:
          - ServerSideEncryptionByDefault:
              SSEAlgorithm: AES256

  Farm:
    Type: AWS::Deadline::Farm
    Properties:
      DisplayName: BYOLFarm

  QueuePolicy:
    Type: AWS::IAM::ManagedPolicy
    Properties:
      ManagedPolicyName: BYOLQueuePolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Action:
              - s3:GetObject
              - s3:PutObject
              - s3:ListBucket
              - s3:GetBucketLocation
            Resource:
              - !Sub ${JobAttachmentBucket.Arn}
              - !Sub ${JobAttachmentBucket.Arn}/job-attachments/*
            Condition:
              StringEquals:
                aws:ResourceAccount: !Sub ${AWS::AccountId}
          - Effect: Allow
            Action: logs:GetLogEvents
            Resource: !Sub arn:aws:logs:${AWS::Region}:${AWS::AccountId}:log-
group:/aws/deadline/${Farm.FarmId}/*
          - Effect: Allow
            Action:
              - s3:ListBucket
              - s3:GetObject
            Resource:
              - "*"
            Condition:
```

```
              ArnLike:
                s3:DataAccessPointArn:
                  - arn:aws:s3:*:*:accesspoint/deadline-software-*
              StringEquals:
                s3:AccessPointNetworkOrigin: VPC

  BYOLSSMPolicy:
    Type: AWS::IAM::ManagedPolicy
    Properties:
      ManagedPolicyName: BYOLSSMPolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Action:
              - ssm:StartSession
            Resource:
              - !Sub arn:aws:ssm:${AWS::Region}::document/AWS-
StartPortForwardingSession
              - !Sub arn:aws:ec2:${AWS::Region}:${AWS::AccountId}:instance/
${LicenseInstanceId}


  WorkerPolicy:
    Type: AWS::IAM::ManagedPolicy
    Properties:
      ManagedPolicyName: BYOLWorkerPolicy
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Action:
              - logs:CreateLogStream
            Resource: !Sub arn:aws:logs:${AWS::Region}:${AWS::AccountId}:log-
group:/aws/deadline/${Farm.FarmId}/*
            Condition:
              ForAnyValue:StringEquals:
                aws:CalledVia:
                  - deadline.amazonaws.com
          - Effect: Allow
            Action:
              - logs:PutLogEvents
              - logs:GetLogEvents
```

```
            Resource: !Sub arn:aws:logs:${AWS::Region}:${AWS::AccountId}:log-
group:/aws/deadline/${Farm.FarmId}/*


  QueueRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: BYOLQueueRole
      ManagedPolicyArns:
        - !Ref QueuePolicy
        - !Ref BYOLSSMPolicy
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Action:
              - sts:AssumeRole
            Principal:
              Service:
                - credentials.deadline.amazonaws.com
                - deadline.amazonaws.com
            Condition:
              StringEquals:
                aws:SourceAccount: !Sub ${AWS::AccountId}
              ArnEquals:
                aws:SourceArn: !Ref Farm

  WorkerRole:
    Type: AWS::IAM::Role
    Properties:
      RoleName: BYOLWorkerRole
      ManagedPolicyArns:
        - arn:aws:iam::aws:policy/AWSDeadlineCloud-FleetWorker
        - !Ref WorkerPolicy
      AssumeRolePolicyDocument:
        Version: 2012-10-17
        Statement:
          - Effect: Allow
            Action:
              - sts:AssumeRole
            Principal:
              Service: credentials.deadline.amazonaws.com
```

```
  Queue:
    Type: AWS::Deadline::Queue
    Properties:
      DisplayName: BYOLQueue
      FarmId: !GetAtt Farm.FarmId
      RoleArn: !GetAtt QueueRole.Arn
      JobRunAsUser:
        Posix:
          Group: ""
          User: ""
        RunAs: WORKER_AGENT_USER
      JobAttachmentSettings:
        RootPrefix: job-attachments
        S3BucketName: !Ref JobAttachmentBucket

  Fleet:
    Type: AWS::Deadline::Fleet
    Properties:
      DisplayName: BYOLFleet
      FarmId: !GetAtt Farm.FarmId
      MinWorkerCount: 1
      MaxWorkerCount: 2
      Configuration:
        ServiceManagedEc2:
          InstanceCapabilities:
            VCpuCount:
              Min: 4
              Max: 16
            MemoryMiB:
              Min: 4096
              Max: 16384
            OsFamily: LINUX
            CpuArchitectureType: x86_64
          InstanceMarketOptions:
            Type: on-demand
      RoleArn: !GetAtt WorkerRole.Arn

  QFA:
    Type: AWS::Deadline::QueueFleetAssociation
    Properties:
      FarmId: !GetAtt Farm.FarmId
      FleetId: !GetAtt Fleet.FleetId
      QueueId: !GetAtt Queue.QueueId
```

```
  CondaQueueEnvironment:
    Type: AWS::Deadline::QueueEnvironment
    Properties:
      FarmId: !GetAtt Farm.FarmId
      Priority: 5
      QueueId: !GetAtt Queue.QueueId
      TemplateType: YAML
      Template: |
        specificationVersion: 'environment-2023-09'
        parameterDefinitions:
        - name: CondaPackages
          type: STRING
          description: >
            This is a space-separated list of Conda package match specifications to
 install for the job.
            E.g. "blender=3.6" for a job that renders frames in Blender 3.6.

            See https://docs.conda.io/projects/conda/en/latest/user-guide/concepts/
pkg-specs.html#package-match-specifications
          default: ""
          userInterface:
            control: LINE_EDIT
            label: Conda Packages
        - name: CondaChannels
          type: STRING
          description: >
            This is a space-separated list of Conda channels from which to install
 packages. Deadline Cloud SMF packages are
            installed from the "deadline-cloud" channel that is configured by
 Deadline Cloud.

            Add "conda-forge" to get packages from the https://conda-forge.org/
 community, and "defaults" to get packages
            from Anaconda Inc (make sure your usage complies with https://
www.anaconda.com/terms-of-use).
          default: "deadline-cloud"
          userInterface:
            control: LINE_EDIT
            label: Conda Channels
        environment:
          name: Conda
          script:
            actions:
              onEnter:
```

```
                command: "conda-queue-env-enter"
                args: ["{{Session.WorkingDirectory}}/.env", "--packages",
 "{{Param.CondaPackages}}", "--channels", "{{Param.CondaChannels}}"]
              onExit:
                command: "conda-queue-env-exit"

  BYOLQueueEnvironment:
    Type: AWS::Deadline::QueueEnvironment
    Properties:
      FarmId: !GetAtt Farm.FarmId
      Priority: 10
      QueueId: !GetAtt Queue.QueueId
      TemplateType: YAML
      Template: !Sub |
        specificationVersion: "environment-2023-09"
        parameterDefinitions:
          - name: LicenseInstanceId
            type: STRING
            description: >
              The Instance ID of the license server/proxy instance
            default: "${LicenseInstanceId}"
          - name: LicenseInstanceRegion
            type: STRING
            description: >
              The region containing this farm
            default: "${AWS::Region}"
          - name: LicensePorts
            type: STRING
            description: >
              Comma-separated list of ports to be forwarded to the license server/
proxy instance.
              Example: "2700,2701,2702"
            default: "${LicensePorts}"
        environment:
          name: BYOL License Forwarding
          variables:
            example_LICENSE: 2700@localhost
          script:
            actions:
              onEnter:
                command: bash
                args: [ "{{Env.File.Enter}}"]
              onExit:
                command: bash
```

```
                args: [ "{{Env.File.Exit}}" ]
            embeddedFiles:
              - name: Enter
                type: TEXT
                runnable: True
                data: |
                  curl https://s3.amazonaws.com/session-manager-downloads/
plugin/latest/linux_64bit/session-manager-plugin.rpm -Ls | rpm2cpio - | cpio
 -iv --to-stdout ./usr/local/sessionmanagerplugin/bin/session-manager-plugin >
 {{Session.WorkingDirectory}}/session-manager-plugin
                  chmod +x {{Session.WorkingDirectory}}/session-manager-plugin
                  conda activate
                  python {{Env.File.StartSession}} {{Session.WorkingDirectory}}/
session-manager-plugin
              - name: Exit
                type: TEXT
                runnable: True
                data: |
                  echo Killing SSM Manager Plugin PIDs: $BYOL_SSM_PIDS
                  for pid in ${!BYOL_SSM_PIDS//,/ }; do kill $pid; done
              - name: StartSession
                type: TEXT
                data: |
                  import boto3
                  import json
                  import subprocess
                  import sys

                  instance_id = "{{Param.LicenseInstanceId}}"
                  region = "{{Param.LicenseInstanceRegion}}"
                  license_ports_list = "{{Param.LicensePorts}}".split(",")

                  ssm_client = boto3.client("ssm", region_name=region)
                  pids = []

                  for port in license_ports_list:
                    session_response = ssm_client.start_session(
                      Target=instance_id,
                      DocumentName="AWS-StartPortForwardingSession",
                      Parameters={"portNumber": [port], "localPortNumber": [port]}
                    )

                    cmd = [
                      sys.argv[1],
```

```
                    json.dumps(session_response),
                    region,
                    "StartSession",
                    "",
                    json.dumps({"Target": instance_id}),
                    f"https://ssm.{region}.amazonaws.com"
                  ]

                  process = subprocess.Popen(cmd, stdout=subprocess.DEVNULL,
stderr=subprocess.DEVNULL)
                  pids.append(process.pid)
                  print(f"SSM Port Forwarding Session started for port {port}")

                print(f"openjd_env: BYOL_SSM_PIDS={','.join(str(pid) for pid in
pids)}")
```

3. Geben Sie bei der Bereitstellung der AWS CloudFormation Vorlage die folgenden Parameter an:
   - Aktualisieren Sie die LicenseInstanceID mit der EC2 Amazon-Instance-ID Ihres Lizenzservers oder Ihrer Proxy-Instance
   - Aktualisieren Sie die LicensePortsmit einer durch Kommas getrennten Liste von Ports, die an den Lizenzserver oder die Proxy-Instance weitergeleitet werden sollen (z. B. 2700,2701)
4. Stellen Sie die Vorlage bereit, um Ihre Farm mit der Funktion „Bring Your Own License“ einzurichten.

Vom Kunden verwaltete Flotten mit einem Lizenzendpunkt Connect

Der nutzungsbasierte Lizenzserver von AWS Deadline Cloud bietet On-Demand-Lizenzen für ausgewählte Produkte von Drittanbietern. Bei nutzungsabhängigen Lizenzen können Sie nutzungsabhängig bezahlen. Ihnen wird nur die Nutzungsdauer in Rechnung gestellt. Bei der nutzungsbasierten Lizenzierung werden Lizenzen für das Rendern Ihrer Deadline Cloud-Mitarbeiter bereitgestellt, nicht jedoch Lizenzen für Ihre DCC-Anwendungen.

Der nutzungsbasierte Lizenzserver von Deadline Cloud kann mit jedem Flotten-Typ verwendet werden, sofern die Deadline Cloud-Mitarbeiter mit dem Lizenzserver kommunizieren können. Dies wird automatisch für vom Service verwaltete Flotten eingerichtet. Dieses Setup ist nur für vom Kunden verwaltete Flotten erforderlich.

Um den Lizenzserver zu erstellen, benötigen Sie eine Sicherheitsgruppe für die VPC Ihrer Farm, die Datenverkehr für Drittanbieterlizenzen zulässt.

Themen

Schritt 1: Erstellen Sie eine Sicherheitsgruppe

Verwenden Sie die Amazon VPC-Konsole, um eine Sicherheitsgruppe für die VPC Ihrer Farm zu erstellen. Konfigurieren Sie die Sicherheitsgruppe so, dass sie die folgenden Regeln für eingehenden Datenverkehr zulässt:

- Autodesk Maya und Arnold — 2701 — 2702, TCP,, IPv4 IPv6
- Autodesk 3ds Max — 2704, TCP, IPv4 IPv6
- Kino 4D — 7057, TCP,, IPv4 IPv6
- KeyShot — 2703, TCP, IPv4 IPv6
- Foundry Nuke — 6101, TCP,, IPv4 IPv6
- Redshift — 7054, TCP, IPv4 IPv6
- SideFX Houdini, Mantra und Karma — 1715 - 1717, TCP,, IPv4 IPv6

Die Quelle für jede eingehende Regel ist die Worker-Sicherheitsgruppe der Flotte.

Weitere Informationen zum Erstellen einer Sicherheitsgruppe finden Sie unter Erstellen einer Sicherheitsgruppe im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Schritt 2: Richten Sie den Lizenzendpunkt ein

Ein Lizenzendpunkt bietet Zugriff auf Lizenzserver für Produkte von Drittanbietern. Lizenzanfragen werden an den Lizenzendpunkt gesendet. Der Endpunkt leitet sie an den entsprechenden Lizenzserver weiter. Der Lizenzserver verfolgt Nutzungsbeschränkungen und Berechtigungen. Durch das Erstellen eines Lizenzendpunkts in Deadline Cloud wird ein AWS PrivateLink

Schnittstellenendpunkt in Ihrer VPC bereitgestellt. Diese Endpunkte werden gemäß den Standardpreisen abgerechnet. AWS PrivateLink Weitere Informationen finden Sie unter AWS PrivateLink Preise.

Mit den entsprechenden Berechtigungen können Sie Ihren Lizenzendpunkt erstellen. Die für die Erstellung eines Lizenzendpunkts erforderliche Richtlinie finden Sie unter Richtlinie zur Zulassung der Erstellung eines Lizenzendpunkts.

Sie können Ihren Lizenzendpunkt über Ihr Dashboard in der Deadline Cloud-Konsole erstellen.

1. Wählen Sie im linken Navigationsbereich Lizenzendpunkte und dann Lizenzendpunkt erstellen aus.
2. Gehen Sie auf der Seite Lizenzendpunkt erstellen wie folgt vor:
   - Wählen Sie eine VPC aus.
   - Wählen Sie die Subnetze aus, die Ihre Deadline Cloud-Worker enthalten. Sie können bis zu 10 Subnetze auswählen.
   - Wählen Sie die Sicherheitsgruppe aus, die Sie in Schritt 1 erstellt haben. Sie können bis zu 10 Sicherheitsgruppen für kompliziertere Szenarien auswählen.
   - (Optional) Wählen Sie Neues Tag hinzufügen und fügen Sie ein oder mehrere Tags hinzu. Sie können bis zu 50 Tags hinzufügen.
3. Wählen Sie Lizenzendpunkt erstellen aus. Wenn der Lizenzendpunkt erstellt wird, wird er auf der Seite mit den Lizenzendpunkten angezeigt.
4. Wählen Sie im Bereich „Gemessene Produkte“ die Option Produkte hinzufügen und wählen Sie dann die Produkte aus, die Sie Ihrem Lizenzendpunkt hinzufügen möchten. Wählen Sie Hinzufügen aus.

Um ein Produkt von einem Lizenzendpunkt zu entfernen, wählen Sie im Bereich Produkte mit Nutzungsdauer das Produkt aus und klicken Sie dann auf Entfernen. Wählen Sie in der Bestätigung erneut Entfernen aus.

Schritt 3: Eine Rendering-Anwendung mit einem Endpunkt Connect

Nachdem der Lizenzendpunkt eingerichtet wurde, verwenden Anwendungen ihn genauso wie einen Lizenzserver eines Drittanbieters. In der Regel konfigurieren Sie den Lizenzserver für die Anwendung, indem Sie eine Umgebungsvariable oder eine andere Systemeinstellung, z. B. einen Microsoft Windows-Registrierungsschlüssel, auf einen Lizenzserverport und eine Adresse festlegen.

Um den DNS-Namen des Lizenzendpunkts abzurufen, wählen Sie den Lizenzendpunkt in der Konsole aus und klicken Sie dann im Bereich DNS-Name auf das Kopiersymbol.

Beispiele für Konfigurationen

Example — Autodesk Maya und Arnold

Setzen Sie die Umgebungsvariable `ADSKFLEX_LICENSE_FILE` auf:

```
2702@VPC_Endpoint_DNS_Name:2701@VPC_Endpoint_DNS_Name
```

> **Note**
>
> Verwenden Sie für Windows Worker ein Semikolon (;) anstelle eines Doppelpunkts (:), um die Endpunkte voneinander zu trennen.

Example — Autodesk 3ds Max

Stellen Sie die Umgebungsvariable wie folgt `ADSKFLEX_LICENSE_FILE` ein:

```
2704@VPC_Endpoint_DNS_Name
```

Example — Kino 4D

Setzen Sie die Umgebungsvariable `g_licenseServerRLM` auf:

```
VPC_Endpoint_DNS_Name:7057
```

Nachdem Sie die Umgebungsvariable erstellt haben, sollten Sie in der Lage sein, ein Bild mit einer Befehlszeile ähnlich der folgenden zu rendern:

```
"C:\Program Files\Maxon Cinema 4D 2025\Commandline.exe" -render ^
    "C:\Users\User\MyC4DFileWithRedshift.c4d" -frame 0 ^
    -oimage "C:\Users\Administrator\User\MyOutputImage.png
```

Example – KeyShot

Setzen Sie die Umgebungsvariable `LUXION_LICENSE_FILE` auf:

```
2703@VPC_Endpoint_DNS_Name
```

Nach der Installation KeyShot und Ausführung können `pip install deadline-cloud-for-keyshot` Sie mit dem folgenden Befehl testen, ob die Lizenz funktioniert. Das Skript validiert Ihre Einstellungen, rendert aber nichts.

```
"C:\Program Files\KeyShot12\bin\keyshot_headless.exe" ^
    -floating_feature keyshot2 ^
    -floating_license_server 2703@VPC_Endpoint_DNS_Name ^
    -script "C:\Program Files\Python311\Lib\site-packages\deadline\keyshot_adaptor
\KeyShotClient\keyshot_handler.py"
```

Die Antwort sollte Folgendes ohne Fehlermeldungen enthalten:

```
Connecting to floating license server
```

Example — Foundry Nuke

Setzen Sie die Umgebungsvariable `foundry_LICENSE` auf:

```
6101@VPC_Endpoint_DNS_Name
```

Um zu testen, ob die Lizenzierung ordnungsgemäß funktioniert, können Sie Nuke in einem Terminal ausführen:

```
~/nuke/Nuke14.0v5/Nuke14.0 -x
```

Example — Redshift

Setzen Sie die Umgebungsvariable `redshift_LICENSE` auf:

```
7054@VPC_Endpoint_DNS_Name
```

Nachdem Sie die Umgebungsvariable erstellt haben, sollten Sie in der Lage sein, ein Bild mit einer Befehlszeile ähnlich der folgenden zu rendern:

```
C:\ProgramData\redshift\bin\redshiftCmdLine.exe ^
    C:\demo\proxy\RS_Proxy_Demo.rs ^
```

```
    -oip C:\demo\proxy\images
```

Example — SideFX Houdini, Mantra und Karma

Führen Sie den folgenden Befehl aus:

```
/opt/hfs19.5.640/bin/hserver -S
 "http://VPC_Endpoint_DNS_Name:1715;http://VPC_Endpoint_DNS_Name:1716;http://
VPC_Endpoint_DNS_Name:1717;"
```

Um zu testen, ob die Lizenzierung ordnungsgemäß funktioniert, können Sie eine Houdini-Szene mit diesem Befehl rendern:

```
/opt/hfs19.5.640/bin/hython ~/forpentest.hip -c "hou.node('/out/mantra1').render()"
```

Schritt 4: Löschen Sie einen Lizenzendpunkt

Denken Sie beim Löschen Ihrer kundenverwalteten Flotte daran, Ihren Lizenzendpunkt zu löschen. Wenn Sie den Lizenzendpunkt nicht löschen, werden Ihnen weiterhin die AWS PrivateLink Fixkosten in Rechnung gestellt

Sie können Ihren Lizenzendpunkt in Ihrem Dashboard in der Deadline Cloud-Konsole löschen.

1. Wählen Sie im linken Navigationsbereich Lizenzendpunkte aus.
2. Wählen Sie den Endpunkt aus, den Sie löschen möchten, und klicken Sie dann zur Bestätigung erneut auf Löschen.

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 im AWS Rahmen von 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.

Themen

Protokollieren von Deadline Cloud API-Aufrufen mit AWS CloudTrail

Deadline Cloud ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem ausgeführten Aktionen bereitstellt AWS-Service. CloudTrail erfasst alle API-Aufrufe Deadline Cloud als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Deadline Cloud Konsole und Codeaufrufen für die Deadline Cloud API-Operationen. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, an die die Anfrage gestellt wurde Deadline Cloud, die IP-Adresse, von der aus die Anfrage gestellt wurde, den Zeitpunkt der Anfrage und weitere Details ermitteln.

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

- Ob die Anfrage mit Anmeldeinformationen des Root-Benutzers oder des Benutzers gestellt wurde.

- Die Anforderung wurde im Namen eines IAM-Identity-Center-Benutzers erstellt.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde.

CloudTrail ist in Ihrem aktiv AWS-Konto , wenn Sie das Konto erstellen, und Sie haben automatisch Zugriff auf den CloudTrail Eventverlauf. Der CloudTrail Ereignisverlauf bietet eine einsehbare, durchsuchbare, herunterladbare und unveränderliche Aufzeichnung der aufgezeichneten Verwaltungsereignisse der letzten 90 Tage in einem. AWS-Region Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Arbeiten mit dem CloudTrail Ereignisverlauf. Für die Anzeige des Eventverlaufs CloudTrail fallen keine Gebühren an.

Für eine fortlaufende Aufzeichnung der Ereignisse in AWS-Konto den letzten 90 Tagen erstellen Sie einen Trail- oder CloudTrailLake-Event-Datenspeicher.

CloudTrail Pfade

Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Alle mit dem erstellten Pfade AWS Management Console sind regionsübergreifend. Sie können mithilfe von AWS CLI einen Einzel-Region- oder einen Multi-Region-Trail erstellen. Es wird empfohlen, einen Trail mit mehreren Regionen zu erstellen, da Sie alle Aktivitäten AWS-Regionen in Ihrem Konto erfassen. Wenn Sie einen Einzel-Region-Trail erstellen, können Sie nur die Ereignisse anzeigen, die im AWS-Region des Trails protokolliert wurden. Weitere Informationen zu Trails finden Sie unter Erstellen eines Trails für Ihr AWS-Konto und Erstellen eines Trails für eine Organisation im AWS CloudTrail -Benutzerhandbuch.

Sie können eine Kopie Ihrer laufenden Verwaltungsereignisse kostenlos an Ihren Amazon S3 S3-Bucket senden, CloudTrail indem Sie einen Trail erstellen. Es fallen jedoch Amazon S3 S3-Speichergebühren an. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preise. Informationen zu Amazon-S3-Preisen finden Sie unter Amazon S3 – Preise.

CloudTrail Datenspeicher für Ereignisse in Lake

CloudTrail Mit Lake können Sie SQL-basierte Abfragen für Ihre Ereignisse ausführen. CloudTrail Lake konvertiert bestehende Ereignisse im zeilenbasierten JSON-Format in das Apache ORC-Format. ORC ist ein spaltenförmiges Speicherformat, das für den schnellen Abruf von Daten optimiert ist. Die Ereignisse werden in Ereignisdatenspeichern zusammengefasst, bei denen es sich um unveränderliche Sammlungen von Ereignissen handelt, die auf Kriterien basieren, die

Sie mit Hilfe von erweiterten Ereignisselektoren auswählen. Die Selektoren, die Sie auf einen Ereignisdatenspeicher anwenden, steuern, welche Ereignisse bestehen bleiben und für Sie zur Abfrage verfügbar sind. Weitere Informationen zu CloudTrail Lake finden Sie unter Arbeiten mit AWS CloudTrail Lake im AWS CloudTrail Benutzerhandbuch.

CloudTrail Für das Speichern und Abfragen von Ereignisdaten in Lake fallen Kosten an. Beim Erstellen eines Ereignisdatenspeichers wählen Sie die Preisoption aus, die für den Ereignisdatenspeicher genutzt werden soll. Die Preisoption bestimmt die Kosten für die Erfassung und Speicherung von Ereignissen sowie die standardmäßige und maximale Aufbewahrungsdauer für den Ereignisdatenspeicher. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preise.

Deadline Cloud Datenereignisse in CloudTrail

Datenereignisse liefern Informationen über die Ressourcenoperationen, die auf oder in einer Ressource ausgeführt werden (z. B. Lesen oder Schreiben in ein Amazon-S3-Objekt). Sie werden auch als Vorgänge auf Datenebene bezeichnet. Datenereignisse sind oft Aktivitäten mit hohem Volume. Protokolliert standardmäßig CloudTrail keine Datenereignisse. Der CloudTrail Ereignisverlauf zeichnet keine Datenereignisse auf.

Für Datenereignisse werden zusätzliche Gebühren fällig. Weitere Informationen zur CloudTrail Preisgestaltung finden Sie unter AWS CloudTrail Preisgestaltung.

Sie können Datenereignisse für die Deadline Cloud Ressourcentypen mithilfe der CloudTrail Konsole oder CloudTrail API-Operationen protokollieren. AWS CLI Weitere Informationen zum Protokollieren von Datenereignissen finden Sie unter Protokollieren von Datenereignissen mit dem AWS Management Console und Protokollieren von Datenereignissen mit dem AWS Command Line Interface im AWS CloudTrail -Benutzerhandbuch.

In der folgenden Tabelle sind die Deadline Cloud Ressourcentypen aufgeführt, für die Sie Datenereignisse protokollieren können. In der Spalte Datenereignistyp (Konsole) wird der Wert angezeigt, den Sie in der Liste Datenereignistyp auf der CloudTrail Konsole auswählen können. In der Wertspalte resources.type wird der `resources.type` Wert angezeigt, den Sie bei der Konfiguration erweiterter Event-Selektoren mithilfe von oder angeben würden. AWS CLI CloudTrail APIs In der CloudTrail Spalte APIs Protokollierte Daten werden die API-Aufrufe angezeigt, die CloudTrail für den Ressourcentyp protokolliert wurden.

Typ des Datenereignisses (Konsole)	resources.type-Wert	Daten, die APIs protokolliert wurden CloudTrail
Deadline Fleet	`AWS::Deadline::Fleet`	• SearchWorkers
Warteschlange	`AWS::Deadline::Fleet`	• SearchJobs
Deadline Worker	`AWS::Deadline::Worker`	• GetWorker • ListSessionsForWorker • UpdateWorkerSchedule • BatchGetJobEntity • ListWorkers
Job mit Deadline	`AWS::Deadline::Job`	• ListStepConsumers • UpdateTask • ListJobs • GetStep • ListSteps • GetJob • GetTask • GetSession • ListSessions • CreateJob • ListSessionActions • ListTasks • CopyJobTemplate • UpdateSession • UpdateStep • UpdateJob • ListJobParameterDefinitions • GetSessionAction • ListStepDependencies

Typ des Datenereignisses (Konsole)	resources.type-Wert	Daten, die APIs protokolliert wurden CloudTrail
		• SearchTasks • SearchSteps

Sie können erweiterte Event-Selektoren so konfigurieren, dass sie nach den Feldern `eventName`, `readOnly` und `resources.ARN` filtern, sodass nur die Ereignisse protokolliert werden, die für Sie wichtig sind. Weitere Informationen zu diesen Feldern finden Sie unter AdvancedFieldSelector in der API-Referenz zu AWS CloudTrail

Deadline Cloud Managementereignisse in CloudTrail

Verwaltungsereignisse bieten Informationen über Verwaltungsvorgänge, die an Ressourcen in Ihrem ausgeführt werden AWS-Konto. Sie werden auch als Vorgänge auf Steuerebene bezeichnet. CloudTrail Protokolliert standardmäßig Verwaltungsereignisse.

AWS Deadline Cloud protokolliert die folgenden Operationen auf der Deadline Cloud Steuerungsebene CloudTrail als Verwaltungsereignisse.

- associate-member-to-farm
- associate-member-to-fleet
- associate-member-to-job
- associate-member-to-queue
- assume-fleet-role-for-gelesen
- assume-fleet-role-for-Arbeiter
- assume-queue-role-for-gelesen
- assume-queue-role-for-Benutzer
- assume-queue-role-for-Arbeiter
- Budget erstellen
- Farm erstellen
- create-fleet
- create-license-endpoint
- Limit erstellen

- Monitor erstellen
- Warteschlange erstellen
- create-queue-environment
- create-queue-fleet-association
- create-queue-limit-association
- create-storage-profile
- Mitarbeiter erstellen
- Budget löschen
- Farm löschen
- delete-fleet
- delete-license-endpoint
- Limit löschen
- delete-metered-product
- Monitor löschen
- Warteschlange löschen
- delete-queue-environment
- delete-queue-fleet-association
- delete-queue-limit-association
- delete-storage-profile
- Mitarbeiter löschen
- disassociate-member-from-farm
- disassociate-member-from-fleet
- disassociate-member-from-job
- disassociate-member-from-queue
- get-application-version
- Holen Sie sich ein Budget
- Farm abrufen
- get-feature-map
- Holen Sie sich die Flotte

- get-license-endpoint
- Limit abrufen
- Monitor abrufen
- Warteschlange abrufen
- get-queue-environment
- get-queue-fleet-association
- get-queue-limit-association
- get-sessions-statistics-aggregation
- get-storage-profile
- get-storage-profile-for-Warteschlange
- list-available-metered-products
- Budgets auflisten
- list-farm-members
- Farmen auflisten
- list-fleet-members
- Flotten auflisten
- list-job-members
- list-license-endpoints
- Limit für die Liste
- list-metered-products
- listet Monitore
- list-queue-environments
- list-queue-fleet-associations
- list-queue-limit-associations
- list-queue-members
- list-queues
- list-storage-profiles
- list-storage-profiles-for-Warteschlange
- list-tags-for-resource
- put-metered-product

- start-sessions-statistics-aggregation
- tag-resource
- untag-resource
- Budget aktualisieren
- Farm aktualisieren
- Flotte aktualisieren
- Limit aktualisieren
- Monitor aktualisieren
- Aktualisierungswarteschlange
- update-queue-environment
- update-queue-fleet-association
- update-queue-limit-association
- update-storage-profile
- Update-Worker

Deadline Cloud Beispiele für Ereignisse

Ein Ereignis stellt eine einzelne Anfrage aus einer beliebigen Quelle dar und enthält Informationen über den angeforderten API-Vorgang, Datum und Uhrzeit des Vorgangs, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass Ereignisse nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt ein CloudTrail Ereignis, das den `CreateFarm` Vorgang demonstriert.

```
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
```

```
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:25:49Z"
            }
        }
    },
    "eventTime": "2021-03-08T23:25:49Z",
    "eventSource": "deadline.amazonaws.com",
    "eventName": "CreateFarm",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "displayName": "example-farm",
        "kmsKeyArn": "arn:aws:kms:us-west-2:111122223333:key/111122223333",
        "X-Amz-Client-Token": "12abc12a-1234-1abc-123a-1a11bc1111a",
        "description": "example-description",
        "tags": {
            "purpose_1": "e2e"
            "purpose_2": "tag_test"
        }
    },
    "responseElements": {
        "farmId": "EXAMPLE-farmID"
    },
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333"
    "eventCategory": "Management",
}
```


Das JSON-Beispiel zeigt die AWS-Region IP-Adresse und andere "" wie `requestParameters` "" und "`displayName`", die Ihnen bei der Identifizierung des Ereignisses helfen können. `kmsKeyArn`

Informationen zu CloudTrail Datensatzinhalten finden Sie im AWS CloudTrail Benutzerhandbuch unter CloudTrailDatensatzinhalte.

Überwachung mit CloudWatch

Amazon CloudWatch (CloudWatch) sammelt Rohdaten und verarbeitet sie zu lesbaren, nahezu in Echtzeit verfügbaren Metriken. Sie können die CloudWatch Konsole unter öffnen https://console.aws.amazon.com/cloudwatch/, um Deadline Cloud-Metriken anzuzeigen und zu filtern.

Diese Statistiken werden 15 Monate lang aufbewahrt, sodass Sie auf historische Informationen zugreifen können, um einen besseren Überblick über die Leistung Ihrer Webanwendung oder Ihres Dienstes zu erhalten. Sie können auch Alarme einrichten, die auf bestimmte Grenzwerte achten und Benachrichtigungen senden oder Aktivitäten auslösen, wenn diese Grenzwerte erreicht werden. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Deadline Cloud hat zwei Arten von Protokollen — Aufgabenprotokolle und Worker-Logs. Ein Aufgabenprotokoll liegt vor, wenn Sie Ausführungsprotokolle als Skript oder während der Ausführung von DCC ausführen. In einem Aufgabenprotokoll können Ereignisse wie das Laden von Objekten, das Rendern von Kacheln oder das Nichtauffinden von Texturen angezeigt werden.

In einem Worker-Protokoll werden die Prozesse des Worker-Agents aufgeführt. Dazu können Dinge gehören, z. B. wann der Worker-Agent startet, sich selbst registriert, Fortschritte meldet, Konfigurationen lädt oder Aufgaben abschließt.

Der Namespace für diese Protokolle lautet`/aws/deadline/*`.

Für Deadline Cloud laden Mitarbeiter diese Protokolle in Logs hoch. CloudWatch Standardmäßig laufen Protokolle nie ab. Wenn bei einem Auftrag eine große Datenmenge ausgegeben wird, können zusätzliche Kosten anfallen. Weitere Informationen finden Sie unter CloudWatch Amazon-Preise.

Sie können die Aufbewahrungsrichtlinie für jede Protokollgruppe anpassen. Eine kürzere Aufbewahrung entfernt alte Protokolle und kann zur Senkung der Speicherkosten beitragen. Um Protokolle aufzubewahren, können Sie sie in Amazon Simple Storage Service archivieren, bevor Sie das Protokoll entfernen. Weitere Informationen finden Sie unter Exportieren von Protokolldaten nach Amazon S3 mithilfe der Konsole im CloudWatch Amazon-Benutzerhandbuch.

> **Note**
>
> CloudWatch Das Lesen von Protokollen ist begrenzt durch AWS. Wenn Sie planen, viele Künstler an Bord zu nehmen, empfehlen wir Ihnen, sich an den AWS Kundensupport zu

wenden und eine Erhöhung des `GetLogEvents` Kontingents in zu beantragen CloudWatch. Außerdem empfehlen wir Ihnen, das Log-Tailing-Portal zu schließen, wenn Sie nicht debuggen.

Weitere Informationen finden Sie unter CloudWatch Log-Kontingente im CloudWatch Amazon-Benutzerhandbuch.

CloudWatch Metriken

Deadline Cloud sendet Metriken an Amazon CloudWatch. Sie können die AWS Management Console, die oder eine API verwenden AWS CLI, um die Metriken aufzulisten, an die Deadline Cloud sendet CloudWatch. Standardmäßig deckt jeder Datenpunkt die 1 Minute ab, die auf die Startzeit der Aktivität folgt. Informationen darüber, wie Sie die verfügbaren Metriken mit dem AWS Management Console oder dem anzeigen können AWS CLI, finden Sie unter Verfügbare Metriken anzeigen im CloudWatch Amazon-Benutzerhandbuch.

Vom Kunden verwaltete Flottenkennzahlen

Der `AWS/DeadlineCloud` Namespace enthält die folgenden Kennzahlen für Ihre vom Kunden verwalteten Flotten:

Metrik	Beschreibung	Einheit
`RecommendedFleetSize`	Die Anzahl der Mitarbeiter, die Deadline Cloud für die Bearbeitung von Aufträgen empfiehlt. Sie können diese Kennzahl verwenden, um die Anzahl der Mitarbeiter aus Ihrer Flotte zu erhöhen oder zu verringern.	Anzahl
`UnhealthyWorkerCount`	Die Anzahl der Mitarbeiter, die für die Bearbeitung von Aufträgen zuständig sind, die nicht korrekt sind.	Anzahl

Sie können die folgenden Dimensionen verwenden, um die vom Kunden verwalteten Flottenkennzahlen zu verfeinern:

Dimension	Beschreibung
FarmId	Diese Dimension filtert die Daten, die Sie für die angegebene Farm anfordern.
FleetId	Diese Dimension filtert die Daten, die Sie für die angegebene Mitarbeiterflotte anfordern.

Metriken zum Ressourcenlimit

Der `AWS/DeadlineCloud` Namespace enthält die folgenden Metriken für Ressourcenlimits:

Metrik	Beschreibung	Einheit
`CurrentCount`	Die Anzahl der Ressourcen, die nach diesem verwendeten Limit modelliert werden.	Anzahl
`MaxCount`	Die maximale Anzahl von Ressourcen, die nach diesem Limit modelliert werden. Wenn Sie den `maxCount` Wert mithilfe der API auf -1 setzen, gibt Deadline Cloud die `MaxCount` Metrik nicht aus.	Anzahl

Sie können die folgenden Dimensionen verwenden, um die Metriken für das gleichzeitige Limit zu verfeinern:

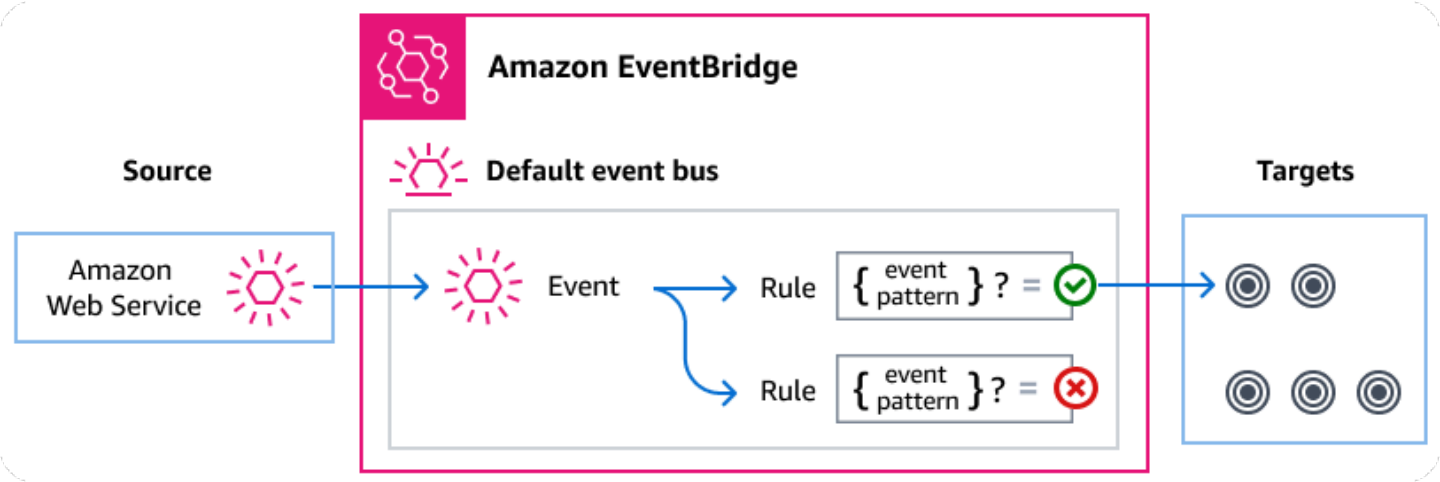
Dimension	Beschreibung
FarmId	Diese Dimension filtert die Daten, die Sie für die angegebene Farm anfordern.
LimitId	Diese Dimension filtert die von Ihnen angeforderten Daten bis zum angegebenen Grenzwert.

Verwaltung von Deadline Cloud-Ereignissen mit Amazon EventBridge

Amazon EventBridge ist ein serverloser Dienst, der Ereignisse verwendet, um Anwendungskomponenten miteinander zu verbinden, sodass Sie leichter skalierbare, ereignisgesteuerte Anwendungen erstellen können. Bei der ereignisgesteuerten Architektur werden lose gekoppelte Softwaresysteme entwickelt, die zusammenarbeiten, indem sie Ereignisse senden und darauf reagieren. Ereignisse stellen eine Änderung in einer Ressource oder Umgebung dar.

Funktionsweise:

Wie bei vielen AWS Diensten generiert Deadline Cloud Ereignisse und sendet sie an den EventBridge Standard-Eventbus. (Der Standard-Event-Bus wird automatisch in jedem AWS Konto bereitgestellt.) Ein Event Bus ist ein Router, der Ereignisse empfängt und sie an null oder mehr Ziele weiterleitet. Regeln, die Sie für den Event-Bus angeben, werten Ereignisse aus, sobald sie eintreffen. Jede Regel prüft, ob ein Ereignis dem Ereignismuster der Regel entspricht. Wenn das Ereignis übereinstimmt, sendet der Event-Bus das Ereignis an die angegebenen Ziele.



Themen

Frist für Cloud-Ereignisse

Deadline Cloud sendet die folgenden Ereignisse automatisch an den EventBridge Standard-Event-Bus. Ereignisse, die dem Ereignismuster einer Regel entsprechen, werden nach bestem Wissen und Gewissen an die angegebenen Ziele übermittelt. Ereignisse werden möglicherweise nicht in der richtigen Reihenfolge zugestellt.

Weitere Informationen finden Sie im Amazon EventBridge Benutzerhandbuch unter EventBridge Ereignisse.

Art der Einzelheiten des Ereignisses	Beschreibung
Budgetschwellenwert erreicht	Wird gesendet, wenn eine Warteschlange einen bestimmten Prozentsatz des zugewiesenen Budgets erreicht.
Änderung des Status des Joblebenszyklus	Wird gesendet, wenn sich der Lebenszyklusstatus eines Jobs ändert.
Änderung des Status der Auftragsausführung	Wird gesendet, wenn sich der Gesamtstatus der Aufgaben in einem Job ändert.
Schritt: Änderung des Lebenszyklusstatus	Wird gesendet, wenn sich der Lebenszyklusstatus eines Schritts in einem Job ändert.
Schritt „Ausführen“: Status ändern	Wird gesendet, wenn sich der Gesamtstatus der Aufgaben in einem Schritt ändert.
Änderung des Status der Aufgabenausführung	Wird gesendet, wenn sich der Status einer Aufgabe ändert.

Bereitstellung von Deadline Cloud-Ereignissen mithilfe von EventBridge Regeln

Damit der EventBridge Standard-Eventbus Deadline Cloud-Ereignisse an ein Ziel sendet, müssen Sie eine Regel erstellen. Jede Regel enthält ein Ereignismuster, das EventBridge mit jedem Ereignis übereinstimmt, das auf dem Event-Bus empfangen wurde. Wenn die Ereignisdaten mit dem angegebenen Ereignismuster EventBridge übereinstimmen, wird dieses Ereignis an die Ziele der Regel gesendet.

Umfassende Anweisungen zum Erstellen von Event-Bus-Regeln finden Sie im EventBridge Benutzerhandbuch unter Erstellen von Regeln, die auf Ereignisse reagieren.

Ereignismuster erstellen, die Deadline Cloud-Ereignissen entsprechen

Jedes Ereignismuster ist ein JSON-Objekt, das Folgendes enthält:

- Ein `source`-Attribut, das den Service identifiziert, der das Ereignis sendet. Für Deadline Cloud-Ereignisse lautet die Quelle`aws.deadline`.
- (Optional): Ein `detail-type`-Attribut, das ein Array der zuzuordnenden Ereignistypen enthält.
- (Optional): Ein `detail`-Attribut, das alle anderen Ereignisdaten für den Abgleich enthält.

Das folgende Ereignismuster entspricht beispielsweise allen Ereignissen zur Änderung der Fleet Size Recommendation für die `farmId` für Deadline Cloud angegebenen Ereignisse:

```
{
  "source": ["aws.deadline"],
  "detail-type": ["Fleet Size Recommendation Change"],
  "detail": {
     "farmId": "farm-12345678900000000000000000000000"
  }
}
```

Weitere Informationen zum Schreiben von Ereignismustern finden Sie unter Ereignismuster im EventBridge Benutzerhandbuch.

Detaillierte Referenz zu Deadline Cloud-Ereignissen

Alle Ereignisse von AWS Diensten haben einen gemeinsamen Satz von Feldern, die Metadaten über das Ereignis enthalten, z. B. den AWS Dienst, der die Quelle des Ereignisses ist, den Zeitpunkt, zu

dem das Ereignis generiert wurde, das Konto und die Region, in der das Ereignis stattgefunden hat, und andere. Definitionen dieser allgemeinen Felder finden Sie unter Referenz zur Ereignisstruktur im Amazon EventBridge Benutzerhandbuch.

Darüber hinaus weist jedes Ereignis ein `detail`-Feld auf, das spezifische Daten für das betreffende Ereignis enthält. In der folgenden Referenz werden die Detailfelder für die verschiedenen Deadline Cloud-Ereignisse definiert.

Bei der EventBridge Auswahl und Verwaltung von Deadline Cloud-Ereignissen ist es hilfreich, Folgendes zu beachten:

- Das `source` Feld für alle Ereignisse aus Deadline Cloud ist auf gesetzt`aws.deadline`.
- Das Feld `detail-type` gibt den Ereignistyp an.

  Beispiel, `Fleet Size Recommendation Change`.
- Das Feld `detail` enthält die Daten, die für das betreffende Ereignis spezifisch sind.

Informationen zur Erstellung von Ereignismustern, die es Regeln ermöglichen, Deadline Cloud-Ereignissen zu entsprechen, finden Sie unter Ereignismuster im Amazon EventBridge Benutzerhandbuch.

Weitere Informationen zu Ereignissen und deren EventBridge Verarbeitung finden Sie unter Amazon EventBridge Ereignisse im Amazon EventBridge Benutzerhandbuch.

Themen

- Ereignis „Budgetschwellenwert erreicht“
- Empfehlung zur Flottengröße: Ereignis ändern
- Ereignis zur Änderung des Joblebenszyklusstatus
- Ereignis zur Änderung des Status der Auftragsausführung
- Schritt: Ereignis „Lebenszyklusstatus ändern“
- Schritt: Ereignis „Status ändern“ ausführen
- Ereignis „Status der Aufgabe ausführen“

Ereignis „Budgetschwellenwert erreicht“

Sie können das Ereignis „Budgetschwellenwert erreicht“ verwenden, um zu überwachen, wie viel Prozent eines Budgets verwendet wurden. Deadline Cloud sendet Ereignisse, wenn der verwendete Prozentsatz die folgenden Schwellenwerte überschreitet:

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

Die Häufigkeit, mit der Deadline Cloud Ereignisse vom Typ Budget Threshold Reached sendet, nimmt zu, wenn sich das Budget seinem Limit nähert. Auf diese Weise können Sie ein Budget genau beobachten, wenn es sich seinem Limit nähert, und Maßnahmen ergreifen, um zu verhindern, dass zu viel ausgegeben wird. Sie können auch Ihre eigenen Budgetschwellenwerte festlegen. Deadline Cloud sendet ein Ereignis, wenn die Nutzung Ihre benutzerdefinierten Schwellenwerte überschreitet.

Wenn Sie die Höhe eines Budgets ändern, basiert das nächste Mal, wenn Deadline Cloud das Ereignis „Budgetschwellenwert erreicht“ sendet, auf dem aktuellen Prozentsatz des Budgets, der verwendet wurde. Wenn Sie beispielsweise 50$ zu einem Budget von 100$ hinzufügen, das sein Limit erreicht hat, zeigt das nächste Ereignis „Budgetschwellenwert erreicht“ an, dass das Budget bei 75 Prozent liegt.

Im Folgenden finden Sie die Detailfelder für das `Budget Threshold Reached` Ereignis.

Die `detail-type` Felder `source` und sind unten aufgeführt, da sie spezifische Werte für Deadline Cloud-Ereignisse enthalten. Definitionen der anderen Metadatenfelder, die in allen Ereignissen enthalten sind, finden Sie unter Referenz zur Ereignisstruktur im Amazon EventBridge Benutzerhandbuch.

```
{
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Budget Threshold Reached",
    "source": "aws.deadline",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "aa-example-1",
    "resources": [],
    "detail": {
        "farmId": "farm-12345678900000000000000000000000",
        "budgetId": "budget-12345678900000000000000000000000",
        "thresholdInPercent": 0
    }
```

```
}
```

`detail-type`

Identifiziert den Ereignistyp.

Für dieses Ereignis ist dieser Wert`Budget Threshold Reached`.

`source`

Identifiziert den Service, aus dem das Ereignis stammt. Für Deadline Cloud-Ereignisse ist dieser Wert`aws.deadline`.

`detail`

Ein JSON-Objekt, das Informationen zum Ereignis enthält. Der Service, der das Ereignis generiert, bestimmt den Inhalt dieses Feldes.

Für dieses Ereignis beinhalten diese Daten:

`farmId`

Die ID der Farm, die den Job enthält.

`budgetId`

Die Kennung des Budgets, das einen Schwellenwert erreicht hat.

`thresholdInPercent`

Der Prozentsatz des Budgets, der verwendet wurde.

Empfehlung zur Flottengröße: Ereignis ändern

Wenn Sie Ihre Flotte so konfigurieren, dass sie ereignisbasiertes Auto Scaling verwendet, sendet Deadline Cloud Ereignisse, mit denen Sie Ihre Flotten verwalten können. Jedes dieser Ereignisse enthält Informationen über die aktuelle Größe und die angeforderte Größe einer Flotte. Ein Beispiel für die Verwendung eines EventBridge Ereignisses und eine Lambda-Beispielfunktion zur Behandlung des Ereignisses finden Sie unter Automatische Skalierung Ihrer EC2 Amazon-Flotte mit der Deadline Cloud-Skalierungsempfehlungsfunktion.

Das Ereignis zur Änderung der Empfehlung zur Flottengröße wird gesendet, wenn Folgendes eintritt:

- Wenn sich die empfohlene Flottengröße ändert und oldFleetSize sich von unterscheidet newFleetSize.

- Wenn der Service feststellt, dass die tatsächliche Flottengröße nicht der empfohlenen Flottengröße entspricht. Die tatsächliche Flottengröße können Sie dem WorkerCount in der GetFleet Betriebsantwort entnehmen. Dies kann passieren, wenn sich eine aktive EC2 Amazon-Instance nicht als Deadline Cloud-Worker registrieren kann.

Im Folgenden finden Sie die Detailfelder für die `Fleet Size Recommendation Change` Veranstaltung.

Die `detail-type` Felder `source` und sind unten aufgeführt, da sie spezifische Werte für Deadline Cloud-Ereignisse enthalten. Definitionen der anderen Metadatenfelder, die in allen Ereignissen enthalten sind, finden Sie unter Referenz zur Ereignisstruktur im Amazon EventBridge Benutzerhandbuch.

```
{
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Fleet Size Recommendation Change",
    "source": "aws.deadline",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "aa-example-1",
    "resources": [],
    "detail": {
        "farmId": "farm-12345678900000000000000000000000",
        "fleetId": "fleet-12345678900000000000000000000000",
        "oldFleetSize": 1,
        "newFleetSize": 5,
    }
}
```

`detail-type`

Identifiziert den Ereignistyp.

Für dieses Ereignis ist dieser Wert`Fleet Size Recommendation Change`.

`source`

Identifiziert den Service, aus dem das Ereignis stammt. Für Deadline Cloud-Ereignisse ist dieser Wert`aws.deadline`.

`detail`

Ein JSON-Objekt, das Informationen zum Ereignis enthält. Der Service, der das Ereignis generiert, bestimmt den Inhalt dieses Feldes.

Für dieses Ereignis beinhalten diese Daten:

`farmId`

Die ID der Farm, die den Job enthält.

`fleetId`

Die Kennung der Flotte, deren Größe geändert werden muss.

`oldFleetSize`

Die aktuelle Größe der Flotte.

`newFleetSize`

Die empfohlene neue Größe für die Flotte.

Ereignis zur Änderung des Joblebenszyklusstatus

Wenn Sie einen Job erstellen oder aktualisieren, legt Deadline Cloud den Lebenszyklusstatus so fest, dass der Status der letzten vom Benutzer initiierten Aktion angezeigt wird.

Bei jeder Änderung des Lebenszyklusstatus wird ein Ereignis zur Änderung des Joblebenszyklusstatus gesendet, auch wenn der Job erstellt wird.

Im Folgenden finden Sie die Detailfelder für das `Job Lifecycle Status Change` Ereignis.

Die `detail-type` Felder `source` und sind unten aufgeführt, da sie spezifische Werte für Deadline Cloud-Ereignisse enthalten. Definitionen der anderen Metadatenfelder, die in allen Ereignissen enthalten sind, finden Sie unter Referenz zur Ereignisstruktur im Amazon EventBridge Benutzerhandbuch.

```
{
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Job Lifecycle Status Change",
    "source": "aws.deadline",
    "account": "111122223333",
```

```
    "time": "2017-12-22T18:43:48Z",
    "region": "aa-example-1",
    "resources": [],
    "detail": {
        "farmId": "farm-12345678900000000000000000000000",
        "queueId": "queue-12345678900000000000000000000000",
        "jobId": "job-12345678900000000000000000000000",
        "previousLifecycleStatus": "UPDATE_IN_PROGRESS",
        "lifecycleStatus": "UPDATE_SUCCEEDED"
    }
}
```

`detail-type`

Identifiziert den Ereignistyp.

Für dieses Ereignis ist dieser Wert`Job Lifecycle Status Change`.

`source`

Identifiziert den Service, aus dem das Ereignis stammt. Für Deadline Cloud-Ereignisse ist dieser Wert`aws.deadline`.

`detail`

Ein JSON-Objekt, das Informationen zum Ereignis enthält. Der Service, der das Ereignis generiert, bestimmt den Inhalt dieses Feldes.

Für dieses Ereignis beinhalten diese Daten:

`farmId`

Die ID der Farm, die den Job enthält.

`queueId`

Die ID der Warteschlange, die den Job enthält.

`jobId`

Die ID des Jobs.

`previousLifecycleStatus`

Der Lebenszyklusstatus, in dem der Job beendet wird. Dieses Feld ist nicht enthalten, wenn Sie einen Job zum ersten Mal einreichen.

`lifecycleStatus`

Der Lebenszyklusstatus, in den der Job eintritt.

Ereignis zur Änderung des Status der Auftragsausführung

Ein Job besteht aus vielen Aufgaben. Jede Aufgabe hat einen Status. Der Status aller Aufgaben wird zusammengefasst, um einen Gesamtstatus für einen Job zu erhalten. Weitere Informationen finden Sie unter Job in Deadline Cloud im AWS Deadline Cloud-Benutzerhandbuch.

Ein Ereignis zur Änderung des Status der Auftragsausführung wird gesendet, wenn:

- Das kombinierte `taskRunStatus` Feld ändert sich.
- Der Job wird in die Warteschlange gestellt, es sei denn, der Job befindet sich im Status READY.

Ein Ereignis zur Änderung des Status der Auftragsausführung wird NICHT gesendet, wenn:

- Der Job wird zuerst erstellt. Um die Auftragserstellung zu überwachen, überprüfen Sie die Ereignisse zur Änderung des Joblebenszyklusstatus auf Änderungen.
- Das `taskRunStatusCounts` Feld des Jobs ändert sich, aber der Ausführungsstatus der kombinierten Jobaufgabe ändert sich nicht.

Im Folgenden finden Sie die Detailfelder für das `Job Run Status Change` Ereignis.

Die `detail-type` Felder `source` und sind unten aufgeführt, da sie spezifische Werte für Deadline Cloud-Ereignisse enthalten. Definitionen der anderen Metadatenfelder, die in allen Ereignissen enthalten sind, finden Sie unter Referenz zur Ereignisstruktur im Amazon EventBridge Benutzerhandbuch.

```
{
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Job Run Status Change",
    "source": "aws.deadline",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "aa-example-1",
    "resources": [],
```

```
    "detail": {
        "farmId": "farm-12345678900000000000000000000000",
        "queueId": "queue-12345678900000000000000000000000",
        "jobId": "job-12345678900000000000000000000000",
        "previousTaskRunStatus": "RUNNING",
        "taskRunStatus": "SUCCEEDED",
        "taskRunStatusCounts": {
            "PENDING": 0,
            "READY": 0,
            "RUNNING": 0,
            "ASSIGNED": 0,
            "STARTING": 0,
            "SCHEDULED": 0,
            "INTERRUPTING": 0,
            "SUSPENDED": 0,
            "CANCELED": 0,
            "FAILED": 0,
            "SUCCEEDED": 20,
            "NOT_COMPATIBLE": 0
       }
    }
}
```

`detail-type`

Identifiziert den Ereignistyp.

Für dieses Ereignis ist dieser Wert`Job Run Status Change`.

`source`

Identifiziert den Service, aus dem das Ereignis stammt. Für Deadline Cloud-Ereignisse ist dieser Wert`aws.deadline`.

`detail`

Ein JSON-Objekt, das Informationen zum Ereignis enthält. Der Service, der das Ereignis generiert, bestimmt den Inhalt dieses Feldes.

Für dieses Ereignis beinhalten diese Daten:

`farmId`

Die ID der Farm, die den Job enthält.

`queueId`

Die ID der Warteschlange, die den Job enthält.

`jobId`

Die ID des Jobs.

`previousTaskRunStatus`

Der Status, in dem die Aufgabe ausgeführt wird, gibt an, dass der Job beendet wird.

`taskRunStatus`

Der Status der Aufgabenausführung, in den der Job wechselt.

`taskRunStatusCounts`

Die Anzahl der Aufgaben des Jobs in jedem Status.

Schritt: Ereignis „Lebenszyklusstatus ändern“

Wenn Sie ein Ereignis erstellen oder aktualisieren, legt Deadline Cloud den Lebenszyklusstatus des Jobs fest, um den Status der letzten vom Benutzer initiierten Aktion zu beschreiben.

Ein Ereignis zur Änderung des Schrittlebenszyklusstatus wird gesendet, wenn:

- Eine Schrittaktualisierung wird gestartet (UPDATE_IN_PROGRESS).
- Ein schrittweises Update wurde erfolgreich abgeschlossen (UPDATE_SUCEEDED).
- Ein schrittweises Update ist fehlgeschlagen (UPDATE_FAILED).

Bei der ersten Erstellung des Schritts wird kein Ereignis gesendet. Um die Erstellung von Schritten zu überwachen, überprüfen Sie die Ereignisse zur Änderung des Joblebenszyklusstatus auf Änderungen.

Im Folgenden finden Sie die Detailfelder für das `Step Lifecycle Status Change` Ereignis.

Die `detail-type` Felder `source` und sind unten aufgeführt, da sie spezifische Werte für Deadline Cloud-Ereignisse enthalten. Definitionen der anderen Metadatenfelder, die in allen Ereignissen enthalten sind, finden Sie unter Referenz zur Ereignisstruktur im Amazon EventBridge Benutzerhandbuch.

```
{
```

```
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Step Lifecycle Status Change",
    "source": "aws.deadline",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "aa-example-1",
    "resources": [],
    "detail": {
        "farmId": "farm-12345678900000000000000000000000",
        "queueId": "queue-12345678900000000000000000000000",
        "jobId": "job-12345678900000000000000000000000",
        "stepId": "step-12345678900000000000000000000000",
        "previousLifecycleStatus": "UPDATE_IN_PROGRESS",
        "lifecycleStatus": "UPDATE_SUCCEEDED"
    }
}
```

`detail-type`

Identifiziert den Ereignistyp.

Für dieses Ereignis ist dieser Wert`Step Lifecycle Status Change`.

`source`

Identifiziert den Service, aus dem das Ereignis stammt. Für Deadline Cloud-Ereignisse ist dieser Wert`aws.deadline`.

`detail`

Ein JSON-Objekt, das Informationen zum Ereignis enthält. Der Service, der das Ereignis generiert, bestimmt den Inhalt dieses Feldes.

Für dieses Ereignis beinhalten diese Daten:

`farmId`

Die ID der Farm, die den Job enthält.

`queueId`

Die ID der Warteschlange, die den Job enthält.

`jobId`

Die ID des Jobs.

`stepId`

Die Kennung des aktuellen Auftragsschritts.

`previousLifecycleStatus`

Der Lebenszyklusstatus, den der Schritt verlässt.

`lifecycleStatus`

Der Lebenszyklusstatus, in den der Schritt eintritt.

Schritt: Ereignis „Status ändern“ ausführen

Jeder Schritt in einem Job besteht aus vielen Aufgaben. Jede Aufgabe hat einen Status. Die Aufgabenstatus werden kombiniert, um einen Gesamtstatus für Schritte und Jobs zu ergeben.

Ein Ereignis zur Änderung des Status eines Schrittlaufs wird gesendet, wenn:

- Die kombinierten `taskRunStatus` Änderungen.
- Der Schritt wird in eine Warteschlange gestellt, sofern sich dieser Schritt nicht im Status READY befindet.

Ein Ereignis wird nicht gesendet, wenn:

- Der Schritt wird zuerst erstellt. Um die Erstellung von Schritten zu überwachen, überprüfen Sie die Ereignisse zur Änderung des Joblebenszyklusstatus auf Änderungen.
- Der Schritt `taskRunStatusCounts` ändert sich, aber der Ausführungsstatus der kombinierten Schrittaufgabe ändert sich nicht.

Im Folgenden finden Sie die Detailfelder für das `Step Run Status Change` Ereignis.

Die `detail-type` Felder `source` und sind unten aufgeführt, da sie spezifische Werte für Deadline Cloud-Ereignisse enthalten. Definitionen der anderen Metadatenfelder, die in allen Ereignissen enthalten sind, finden Sie unter Referenz zur Ereignisstruktur im Amazon EventBridge Benutzerhandbuch.

```
{
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
```

```
    "detail-type": "Step Run Status Change",
    "source": "aws.deadline",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "aa-example-1",
    "resources": [],
    "detail": {
        "farmId": "farm-12345678900000000000000000000000",
        "queueId": "queue-12345678900000000000000000000000",
        "jobId": "job-12345678900000000000000000000000",
        "stepId": "step-12345678900000000000000000000000",
        "previousTaskRunStatus": "RUNNING",
        "taskRunStatus": "SUCCEEDED",
        "taskRunStatusCounts": {
            "PENDING": 0,
            "READY": 0,
            "RUNNING": 0,
            "ASSIGNED": 0,
            "STARTING": 0,
            "SCHEDULED": 0,
            "INTERRUPTING": 0,
            "SUSPENDED": 0,
            "CANCELED": 0,
            "FAILED": 0,
            "SUCCEEDED": 20,
            "NOT_COMPATIBLE": 0
       }
    }
}
```

`detail-type`

Identifiziert den Ereignistyp.

Für dieses Ereignis ist dieser Wert`Step Run Status Change`.

`source`

Identifiziert den Service, aus dem das Ereignis stammt. Für Deadline Cloud-Ereignisse ist dieser Wert`aws.deadline`.

`detail`

Ein JSON-Objekt, das Informationen zum Ereignis enthält. Der Service, der das Ereignis generiert, bestimmt den Inhalt dieses Feldes.

Für dieses Ereignis beinhalten diese Daten:

`farmId`

Die ID der Farm, die den Job enthält.

`queueId`

Die ID der Warteschlange, die den Job enthält.

`jobId`

Die ID des Jobs.

`stepId`

Die Kennung des aktuellen Auftragsschritts.

`previousTaskRunStatus`

Der Ausführungsstatus, den der Schritt verlässt.

`taskRunStatus`

Der Ausführungsstatus, in den der Schritt eintritt.

`taskRunStatusCounts`

Die Anzahl der Aufgaben des Schritts in jedem Status.

Ereignis „Status der Aufgabe ausführen“

Das `runStatus` Feld wird aktualisiert, wenn die Aufgabe ausgeführt wird. Ein Ereignis wird gesendet, wenn:

- Der Ausführungsstatus der Aufgabe ändert sich.
- Die Aufgabe wird in die Warteschlange gestellt, es sei denn, die Aufgabe befindet sich im Status BEREIT.

Ein Ereignis wird nicht gesendet, wenn:

- Die Aufgabe wird zuerst erstellt. Um die Aufgabenerstellung zu überwachen, überprüfen Sie die Ereignisse zur Änderung des Joblebenszyklusstatus auf Änderungen.

Im Folgenden finden Sie die Detailfelder für das `Task Run Status Change` Ereignis.

Die `detail-type` Felder `source` und sind unten aufgeführt, da sie spezifische Werte für Deadline Cloud-Ereignisse enthalten. Definitionen der anderen Metadatenfelder, die in allen Ereignissen enthalten sind, finden Sie unter Referenz zur Ereignisstruktur im Amazon EventBridge Benutzerhandbuch.

```
{
    "version": "0",
    "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "detail-type": "Task Run Status Change",
    "source": "aws.aws.deadline",
    "account": "111122223333",
    "time": "2017-12-22T18:43:48Z",
    "region": "aa-example-1",
    "resources": [],
    "detail": {
        "farmId": "farm-12345678900000000000000000000000",
        "queueId": "queue-12345678900000000000000000000000",
        "jobId": "job-12345678900000000000000000000000",
        "stepId": "step-12345678900000000000000000000000",
        "taskId": "task-12345678900000000000000000000000-0",
        "previousRunStatus": "RUNNING",
        "runStatus": "SUCCEEDED"
    }
}
```

`detail-type`

Identifiziert den Ereignistyp.

Für dieses Ereignis ist dieser Wert`Fleet Size Recommendation Change`.

`source`

Identifiziert den Service, aus dem das Ereignis stammt. Für Deadline Cloud-Ereignisse ist dieser Wert`aws.deadline`.

`detail`

Ein JSON-Objekt, das Informationen zum Ereignis enthält. Der Service, der das Ereignis generiert, bestimmt den Inhalt dieses Feldes.

Für dieses Ereignis beinhalten diese Daten:

`farmId`

Die ID der Farm, die den Job enthält.

`queueId`

Die ID der Warteschlange, die den Job enthält.

`jobId`

Die ID des Jobs.

stepId

Die Kennung des aktuellen Job-Schritts.

`taskId`

Der Bezeichner der laufenden Aufgabe.

`previousRunStatus`

Der Ausführungsstatus, den die Aufgabe verlässt.

`runStatus`

Der Ausführungsstatus, in den die Aufgabe eingeht.

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

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit der Konsole, der 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. Verwenden Sie den DescribeKeyVorgang, um das tatsächliche Datum und die Uhrzeit der Löschung des Schlüssels zu ermitteln. 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.

Nach der Abmeldung sendet der Desktop-Monitor 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.

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

- Authentifizierung mit Identitäten
- Verwalten des Zugriffs mit Richtlinien
- So funktioniert Deadline Cloud mit IAM
- Beispiele für identitätsbasierte Richtlinien für Deadline Cloud
- AWS verwaltete Richtlinien für Deadline Cloud
- Fehlerbehebung bei AWS Deadline Cloud-Identität und -Zugriff

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 darauf 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 einer Gruppe einen Namen geben 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:

```
awsdeadlinecloud
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "awsdeadlinecloud:action1",
      "awsdeadlinecloud: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
- Verwenden Sie die Deadline Cloud-Konsole
- Richtlinie zum Einreichen von Jobs an eine Warteschlange
- Richtlinie, die die Erstellung eines Lizenzendpunkts ermöglicht
- Richtlinie, die die Überwachung einer bestimmten Farmwarteschlange ermöglicht

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: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 dem Benutzer, Mitarbeiter zu erstellen, die Flottenrolle für Mitarbeiter zu übernehmen und Tags auf Mitarbeiter anzuwenden

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-WorkerHost— Änderung	Deadline Cloud hat neue Aktionen `deadline:TagResource` hinzugefügt `deadline:ListTagsForResource`, sodass Sie Tags hinzufügen und anzeigen können, die mit Mitarbeitern in Ihrer Flotte verknüpft sind.	30. Mai 2025
AWSDeadlineCloud-UserAccessFarms— Ändern 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

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 `awsdeadlinecloud:`*`GetWidget`*-Berechtigungen verfügt.

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

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `awsdeadlinecloud:`*`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 auszuführen: 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.

Konformitätsprüfung 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 Kontextschlüssel aws:SourceArnund die aws:SourceAccountglobalen Bedingungsschlüssel in Ressourcenrichtlinien zu verwenden, um die Berechtigungen einzuschränken, die der AWS Deadline Cloud 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:awsdeadlinecloud:*:`*`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` globale Bedingung verwenden können, Deadline Cloud um das Problem des verwirrten Stellvertreters zu vermeiden.

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

```
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "awsdeadlinecloud.amazonaws.com"
    },
    "Action": "awsdeadlinecloud:ActionName",
    "Resource": [
      "*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:awsdeadlinecloud:*:123456789012:*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

Zugriff AWS Deadline Cloud über einen Schnittstellenendpunkt (AWS PrivateLink)

Sie können AWS PrivateLink damit eine private Verbindung zwischen Ihrer VPC und AWS Deadline Cloud herstellen. 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.

Deadline Cloud verfügt auch über Dual-Stack-Endpunkte. Dual-Stack-Endpunkte unterstützen Anfragen über und. IPv6 IPv4

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 auch 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 vier Endpunkte für den Zugriff auf den Dienst mithilfe von AWS PrivateLink — zwei für IPv4 und zwei für. IPv6

Mitarbeiter verwenden den `scheduling.deadline.region.amazonaws.com` 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, `management.deadline.region.amazonaws.com` 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 Jobanhänge 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
```

Deadline Cloud unterstützt Dual-Stack-Endpunkte.

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 `scheduling.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).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail.
- 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 die geringsten Rechte für die Jobs der Warteschlange hat.

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 die 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 der `AssumeQueueRoleForRead` `AssumeQueueRoleForUser` ,- 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:

- Die Verwendung eines Host-Konfigurationsskripts kann die Sicherheit und den Betrieb eines Workers ändern. Eine falsche Konfiguration kann dazu führen, dass der Worker instabil ist oder nicht mehr funktioniert. Es liegt in Ihrer Verantwortung, solche Fehler zu debuggen.
- Verwenden Sie nicht denselben `jobRunAsUser` Wert für mehrere Warteschlangen, es sei denn, Aufträge, die an diese Warteschlangen gesendet werden, 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 Linux und das Konto `Administrator` Eigentümer der Worker-Agent-Programmdateien sind und diese ändern können. Windows

- Auf Linux Worker-Hosts sollten Sie erwägen, einen `umask` Override-Vorgang 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 (`/etc/hosts`aktiviert Linux und aktiviertWindows) sowie `C:\Windows\system32\etc\hosts` auf das Routing von Tabellen auf Workstations und Worker-Host-Betriebssystemen.
- 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 die Warteschlange. Windows `jobRunAsUser`
- Wechseln Sie regelmäßig die Passwörter für Ihre Warteschlange`jobRunAsUser`.
- Sorgen Sie für den Zugriff auf die Windows Kennwortgeheimnisse mit den geringsten Rechten und löschen Sie ungenutzte Geheimnisse.
- Erteilen Sie der Warteschlange nicht die `jobRunAsUser` Erlaubnis, die Befehle für den Zeitplan in der future auszuführen:
  - EinLinux, verweigern Sie diesen Konten den Zugriff auf `cron` und`at`.
  - Ist diese Windows Option aktiviert, wird diesen Konten der Zugriff auf den Windows Taskplaner verweigert.

> **Note**
>
> Weitere Informationen darüber, wie wichtig es ist, das Betriebssystem und die installierte Software regelmäßig zu patchen, finden Sie im Modell der gemeinsamen Verantwortung.

Host-Konfigurationsskript

- Die Verwendung eines Host-Konfigurationsskripts kann die Sicherheit und den Betrieb eines Workers ändern. Eine falsche Konfiguration kann dazu führen, dass der Worker instabil ist oder nicht mehr funktioniert. Es liegt in Ihrer Verantwortung, solche Fehler zu debuggen.

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 die 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 (`/etc/hosts`an Linux undmacOS, und `C:\Windows\system32\etc\hosts` anWindows) und auf das Routing von Tabellen auf Workstations und Worker-Host-Betriebssystemen.
- 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.

Überprüfen Sie die Echtheit der heruntergeladenen Software

Überprüfen Sie nach dem Herunterladen des Installationsprogramms die Echtheit Ihrer Software, um sie vor Dateimanipulationen zu schützen. Dieses Verfahren funktioniert sowohl für als auch für SystemeWindows. Linux

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 des installierten SignTool SDK. 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 dafür entscheiden, dem OpenPGP Schlüssel zu vertrauen, bearbeiten Sie den Schlüssel so, dass er vertrauenswürdig ist. gpg Gehen Sie dabei wie im folgenden Beispiel vor:

```
$ 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 Linux (Debian) auf der Registerkarte, auf der Registerkarte Linux (RPM) oder auf der Linux (AppImage) Registerkarte, die 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 verwendenLinux. AppImage Binär, führen Sie zuerst die Schritte 1 bis 3 Linux auf der Registerkarte aus 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 Linux eine.deb-Binärdatei verwenden, führen Sie zunächst die Schritte 1—3 Linux auf der Registerkarte aus.

dpkg ist das zentrale Paketverwaltungswerkzeug in den meisten debian basierten Linux Distributionen. 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, stellen Sie sicher, dass sie in der Ausgabe vorhanden `GOODSIG` ist.

Linux (RPM)

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

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.

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen in den einzelnen Versionen des AWS Deadline Cloud Developer Guide beschrieben.

Änderung	Beschreibung	Datum
Konfigurationsskripte für Worker-Hosts wurden hinzugefügt	Es wurde eine Dokumentation für die Verwendung von Worker-Host-Konfigurationsskripten hinzugefügt, die mit erhöhten Rechten ausgeführt werden. Weitere Informationen finden Sie unter Als Administrator Skripts ausführen, um Worker zu konfigurieren.	12. Mai 2025
Der Sicherheitsabschnitt zur Verwendung von AWS PrivateLink	Die Anweisungen für den Zugriff auf Deadline Cloud mithilfe AWS PrivateLink und der neuen Dual-Stack-Endpunkte wurden aktualisiert. Weitere Informationen finden Sie unter Zugriff auf Deadline Cloud über einen Schnittstellenendpunkt.	17. März 2025
Die vom Kunden verwalteten Flottenanmeldedaten wurden aktualisiert	Die Anweisungen zum Erstellen von Anmeldeinformationen für eine vom Kunden verwaltete Flotte wurden aktualisiert und bieten nun mehr Informationen zur Sicherung Ihrer Flotte. Weitere Informationen finden Sie unter	10. Februar 2025

	AWS-Anmeldeinformationen konfigurieren.	
Der Inhalt des Benutzerhandbuchs wurde neu organisiert	Inhalte, die sich auf Entwickler konzentrieren, wurden aus dem Benutzerhandbuch in das Entwicklerhandbuch verschoben: • Die Anweisungen zur Erstellung einer kundenverwalteten Flotte wurden aus dem Benutzerhandbuch in ein neues Kapitel „Kundenverwaltete Flotten“ verschoben. • Es wurde ein neues Kapitel „Softwarelizenzen verwenden“ mit Informationen zur nutzungsbasierten Lizenzierung und zur Verwendung eigener Lizenzen für vom Service und vom Kunden verwaltete Flotten erstellt. • Einzelheiten zur Überwachung mit CloudTrail CloudWatch, und wurden EventBridge aus dem Benutzerhandbuch in das Kapitel Überwachung verschoben.	6. Januar 2025

Erstellen Sie ein Conda-Paket	Es wurden Informationen zum Erstellen eines Conda-Pakets für eine Anwendung hinzugefügt. Weitere Informationen finden Sie unter Erstellen eines Conda-Pakets.	29. August 2024
Neues Handbuch	Dies ist die erste Version des Deadline Cloud Developer Guide.	26. Juli 2024

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.