Guía del usuario

AWS Nube de plazos

Version latest

AWS Nube de plazos: Guía del usuario

Table of Contents

¿Qué es Deadline Cloud? 1
Características de Deadline Cloud 1
Conceptos y terminología 2
Cómo empezar con Deadline Cloud 4
Acceder a Deadline Cloud 5
Servicios relacionados 5
Cómo funciona Deadline Cloud 6
..... 7
Permisos en Deadline Cloud 7
Soporte de software con Deadline Cloud 8
Introducción 9
Configuración de su Cuenta de AWS 9
Configura tu monitor 10
Paso 1: Configura el monitor 10
Paso 2: Defina los detalles de la granja 13
Paso 3: Defina los detalles de la cola 14
Paso 4: Defina los detalles de la flota 15
Paso 5: Configurar los requisitos de los trabajadores 16
Paso 6: Definir los niveles de acceso 17
Paso 7: Revisar y crear 17
Configura una estación de trabajo para desarrolladores 17
Paso 1: Crear una granja 18
Paso 2: Ejecute el agente de trabajo 22
Paso 3: Enviar y ejecutar trabajos 24
Paso 4: Ejecuta trabajos con archivos adjuntos 32
Paso 5: Agrega una flota gestionada por servicios 41
Paso 6: Limpiar los recursos de la granja 44
Configura el remitente 47
Paso 1: Instale el remitente de Deadline Cloud 47
Paso 2: Instale y configure Deadline Cloud monitor 55
Paso 3: Inicie el remitente de Deadline Cloud 58
Usa la granja 62
Uso del monitor 64
Comparte la URL del monitor de Deadline Cloud 64

Abre el monitor de Deadline Cloud 65
Vea los detalles de la cola y la flota 67
Vea y gestione los trabajos, los pasos y las tareas 68
Ver detalles del trabajo 69
Ver un paso 70
Ver una tarea 70
Ver registros de 71
Descarga el resultado final 73
Granjas 74
Cree una granja 74
Eliminar una granja 74
Edite una granja 75
Queues 76
Creación de una cola 76
Cree un entorno de colas 78
Entorno de Conda colas predeterminado 79
Eliminar una cola 80
Edición de una cola 81
Asocia una cola y una flota 81
Gestión de flotas 82
Flotas gestionadas por el servicio 82
Plataforma VFX 84
Flotas gestionadas por los clientes 85
Cree un CMF 85
Configuración del host de trabajo 91
Administración de acceso 96
Instale el software para los trabajos 98
Configurar credenciales de 99
Crear un AMI 101
Cree una infraestructura de flota 104
Conectarse a un punto final de licencia 114
Administración de usuarios 119
Administre los usuarios y grupos del monitor 119
Administre los usuarios y grupos de granjas, colas y flotas 121
Jobs 123
Envío de trabajos 124

Más opciones para enviar trabajos 126
Programar trabajos 128
Determine la compatibilidad de la flota 128
Escalado de flota 130
Sesiones 130
Dependencias escalonadas 132
Estados de trabajo 133
Modificación de trabajos 136
Procesando trabajos 141
Solución de problemas de trabajos 142
¿Por qué falló la creación de mi trabajo? 142
¿Por qué mi trabajo no es compatible? 143
¿Por qué está preparado mi trabajo pendiente? 143
¿Por qué falló mi trabajo? 143
¿Por qué está pendiente mi trámite? 144
Almacenamiento 145
Adjuntos de trabajo 145
Cifrado para los depósitos de S3 adjuntos a tareas 146
Administrar los adjuntos de trabajos en depósitos de S3 147
Sistema de archivos virtual 147
Almacenamiento compartido 150
Perfiles de almacenamiento en Deadline Cloud 150
Administrar los presupuestos y el uso 153
Hipótesis de costes 153
Uso del gestor de presupuestos 154
Requisito previo 155
Acceda al administrador de presupuestos 155
Creación de un presupuesto 156
Ver un presupuesto 157
Editar un presupuesto 157
Desactiva un presupuesto 158
Uso del explorador de uso 158
Requisito previo 159
Abre el explorador de uso 159
Usa el explorador de uso 158
Administración de costos 161

Mejores prácticas de administración de costos ... 162
Seguridad ... 165
Protección de datos ... 166
Cifrado en reposo ... 167
Cifrado en tránsito ... 167
Administración de claves ... 167
Privacidad del tráfico entre redes ... 177
Optar por no participar ... 178
Identity and Access Management ... 179
Público ... 179
Autenticación con identidades ... 180
Administración de acceso mediante políticas ... 184
Cómo funciona Deadline Cloud con IAM ... 187
Ejemplos de políticas basadas en identidades ... 194
AWS políticas gestionadas ... 199
Resolución de problemas ... 202
Validación de conformidad ... 204
Resiliencia ... 206
Seguridad de la infraestructura ... 206
Configuración y análisis de vulnerabilidades ... 207
Prevención de la sustitución confusa entre servicios ... 207
AWS PrivateLink ... 209
Consideraciones ... 209
Deadline Cloud puntos finales ... 210
Cree puntos finales ... 210
Prácticas recomendadas de seguridad ... 211
Protección de datos ... 212
Permisos de IAM ... 212
Ejecute trabajos como usuarios y grupos ... 213
Red ... 213
Datos de trabajo ... 214
Estructura de la granja ... 214
Colas de adjuntos de trabajos ... 215
Depósitos de software personalizados ... 217
Los trabajadores son anfitriones ... 217
Estaciones de trabajo ... 219

Supervisión 220
Iniciar sesión con CloudTrail 221
Información sobre Deadline Cloud en CloudTrail 221
Descripción de las entradas del archivo de registro de Deadline Cloud 225
Monitorear con CloudWatch 227
Actuar en función de EventBridge los acontecimientos 228
Cambio recomendado de tamaño de flota 228
Cuotas 231
AWS CloudFormation recursos 232
Deadline Cloud y AWS CloudFormation plantillas 232
Más información sobre AWS CloudFormation 232
Historial de documentos 233
AWS Glosario 234
..... ccxxxv

¿Qué es AWS Deadline Cloud?

Deadline Cloud es una Servicio de AWS solución que puede utilizar para crear y gestionar proyectos y trabajos de renderizado en instancias de Amazon Elastic Compute Cloud (Amazon EC2) directamente desde estaciones de trabajo y canales de creación de contenido digital.

Deadline Cloud proporciona interfaces de consola, aplicaciones locales, herramientas de línea de comandos y una API. Con Deadline Cloud, puede crear, administrar y monitorear granjas, flotas, trabajos, grupos de usuarios y almacenamiento. También puede especificar los requisitos de hardware, crear entornos para cargas de trabajo específicas e integrar las herramientas de creación de contenido que necesite su producción en su cartera de Deadline Cloud.

Deadline Cloud proporciona una interfaz unificada para gestionar todos tus proyectos de renderizado en un solo lugar. Puede gestionar los usuarios, asignarles proyectos y conceder permisos para los puestos de trabajo.

Temas

- Características de Deadline Cloud
- Conceptos y terminología para Deadline Cloud
- Cómo empezar con Deadline Cloud
- Acceder a Deadline Cloud
- Servicios relacionados
- Cómo funciona Deadline Cloud

Características de Deadline Cloud

Estas son algunas de las formas clave en las que Deadline Cloud puede ayudarte a ejecutar y gestionar cargas de trabajo de computación visual:

- Cree rápidamente sus granjas, colas y flotas. Supervise su estado y obtenga información sobre el funcionamiento de su granja y sus trabajos.
- Administre de forma centralizada los usuarios y grupos de Deadline Cloud y asigne permisos.
- Gestione la seguridad de inicio de sesión para los usuarios del proyecto y los proveedores de identidad externos con AWS IAM Identity Center.

- Gestione de forma segura el acceso a los recursos del proyecto con políticas y funciones AWS Identity and Access Management (IAM).
- Usa etiquetas para organizar y encontrar rápidamente los recursos del proyecto.
- Administre el uso de los recursos del proyecto y los costos estimados de su proyecto.
- Ofrezca una amplia gama de opciones de administración informática para permitir el renderizado en la nube o en persona.

Conceptos y terminología para Deadline Cloud

Para ayudarte a empezar a usar AWS Deadline Cloud, en este tema se explican algunos de sus conceptos y terminología clave.

Gestor de presupuestos

: El gestor de presupuestos forma parte del monitor de Deadline Cloud. Use el administrador de presupuestos para crear y administrar presupuestos. También puede usarlo para limitar las actividades y mantenerse dentro del presupuesto.

Biblioteca de clientes de Deadline Cloud

: La biblioteca de clientes incluye una interfaz de línea de comandos y una biblioteca para administrar Deadline Cloud. La funcionalidad incluye enviar paquetes de trabajos basados en la especificación Open Job Description a Deadline Cloud, descargar los resultados de los adjuntos de trabajos y monitorear su granja mediante la interfaz de línea de comandos.

Aplicación de creación de contenido digital (DCC)

: Las aplicaciones de creación de contenido digital (DCC) son productos de terceros con los que se crea contenido digital. Algunos ejemplos de DCC sonMaya, y. Nuke Houdini Deadline Cloud proporciona complementos integrados a los solicitantes de empleo para DCC específicos.

Granja

: Una granja es el lugar donde se encuentran los recursos de su proyecto. Se compone de colas y flotas.

Flota

: Una flota es un grupo de nodos trabajadores que realizan el renderizado. Los nodos de trabajo procesan los trabajos. Una flota se puede asociar a varias colas y una cola se puede asociar a varias flotas.

Trabajo

Un trabajo es una solicitud de renderización. Los usuarios envían trabajos. Los trabajos contienen propiedades específicas que se describen como pasos y tareas.

Adjuntos de trabajo

Un adjunto de trabajo es una función de Deadline Cloud que puedes usar para gestionar las entradas y salidas de los trabajos. Los archivos de trabajo se cargan como adjuntos al trabajo durante el proceso de renderizado. Estos archivos pueden ser texturas, modelos 3D, equipos de iluminación y otros elementos similares.

Propiedades del trabajo

Las propiedades del trabajo son ajustes que se definen al enviar un trabajo de renderizado. Algunos ejemplos incluyen el rango de fotogramas, la ruta de salida, los archivos adjuntos del trabajo, la cámara renderizable y más. Las propiedades varían en función del DCC desde el que se envía el renderizado.

Plantilla de trabajo

Una plantilla de trabajo define el entorno de ejecución y todos los procesos que se ejecutan como parte de un trabajo de Deadline Cloud.

Queue

Una cola es el lugar donde se encuentran los trabajos enviados y donde se programa su renderización. Una cola debe estar asociada a una flota para que el renderizado se realice correctamente. Una cola se puede asociar a varias flotas.

Asociación de colas y flotas

Cuando una cola está asociada a una flota, existe una asociación entre colas y flota. Use una asociación para programar a los trabajadores de una flota por los trabajos de esa cola. Puede iniciar y detener asociaciones para controlar la programación del trabajo.

Paso

Un paso es un proceso concreto que se ejecuta en el trabajo.

Fecha límite: remitente de Deadline Cloud

Un remitente de Deadline Cloud es un complemento de creación de contenido digital (DCC). Los artistas lo utilizan para enviar trabajos desde una interfaz de DCC de terceros con la que están familiarizados.

Etiquetas

Una etiqueta es una etiqueta que se puede asignar a un AWS recurso. Cada etiqueta consta de una clave y un valor opcional definido por usted.

Con las etiquetas, puedes clasificar tus AWS recursos de diferentes maneras. Por ejemplo, podría definir un conjunto de etiquetas para las instancias Amazon EC2 de su cuenta que le ayude a realizar un seguimiento del propietario y el nivel de la pila de cada instancia.

También puede clasificar AWS los recursos por propósito, propietario o entorno. Este enfoque resulta útil cuando se tienen muchos recursos del mismo tipo. Puede identificar rápidamente un recurso específico en función de las etiquetas que le haya asignado.

Tarea

Una tarea es un componente único de un paso de renderizado.

Licencias basadas en el uso (UBL)

La licencia basada en el uso (UBL) es un modelo de licencia bajo demanda que está disponible para determinados productos de terceros. Este modelo es de pago por uso y se le cobra por la cantidad de horas y minutos que utilice.

Explorador de uso

El explorador de uso es una función del monitor Deadline Cloud. Proporciona una estimación aproximada de sus costos y uso.

Entorno de trabajo

Los trabajadores pertenecen a flotas y ejecutan las tareas asignadas por Deadline Cloud para completar los pasos y trabajos. Los trabajadores almacenan los registros de las operaciones de las tareas en Amazon CloudWatch Logs. Los trabajadores también pueden usar la función de adjuntos de trabajos para sincronizar las entradas y salidas con un bucket de Amazon Simple Storage Service (Amazon S3).

Cómo empezar con Deadline Cloud

Utilice Deadline Cloud para crear rápidamente una granja de renderización con la configuración y los recursos predeterminados, como la configuración de instancias de Amazon EC2 y los depósitos de Amazon Simple Storage Service (Amazon S3).

También puede definir la configuración y los recursos al crear una granja de renderizado. Este método lleva más tiempo que el uso de la configuración y los recursos predeterminados, pero le brinda más control.

Cuando se familiarice con los conceptos y la terminología de Deadline Cloud, consulte Primeros pasos para obtener step-by-step instrucciones sobre cómo crear su granja, añadir usuarios y enlaces a información útil.

Acceder a Deadline Cloud

Puede acceder a Deadline Cloud de cualquiera de las siguientes maneras:

- Consola de Deadline Cloud: accede a la consola desde un navegador para crear una granja y sus recursos, y gestionar el acceso de los usuarios. Para más información, consulte Introducción.
- Monitor de Deadline Cloud: administre sus trabajos de renderizado, incluida la actualización de las prioridades y los estados de los trabajos. Supervise su granja y vea los registros y el estado de los trabajos. Para los usuarios con permisos de propietario, el monitor Deadline Cloud también proporciona acceso para explorar el uso y crear presupuestos. El monitor Deadline Cloud está disponible como navegador web y como aplicación de escritorio.
- AWS SDK y AWS CLI: usa AWS Command Line Interface (AWS CLI) para llamar a las operaciones de la API de Deadline Cloud desde la línea de comandos de tu sistema local. Para obtener más información, consulte Configurar una estación de trabajo para desarrolladores.

Servicios relacionados

Deadline Cloud funciona con lo siguiente: Servicios de AWS

- Amazon CloudWatch: con CloudWatch, puede monitorear sus proyectos y AWS los recursos asociados. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.
- Amazon EC2: Servicio de AWS proporciona servidores virtuales que ejecutan sus aplicaciones en la nube. Puede configurar sus proyectos para que usen instancias de Amazon EC2 para sus cargas de trabajo. Para obtener más información, consulte Instancias de Amazon EC2.
- Auto Scaling de Amazon EC2: con Auto Scaling, puede aumentar o disminuir automáticamente el número de instancias a medida que cambia la demanda de las mismas. Auto Scaling ayuda a garantizar que está ejecutando la cantidad deseada de instancias, incluso si una instancia falla. Si habilita Auto Scaling con Deadline Cloud, las instancias que se lanzan con Auto Scaling

se registran automáticamente en la carga de trabajo. Del mismo modo, las instancias que son canceladas por Auto Scaling se cancelan automáticamente del registro de la carga de trabajo. Para obtener más información, consulte la Guía del usuario de Auto Scaling de Amazon EC2.

- AWS PrivateLink— AWS PrivateLink proporciona conectividad privada entre las nubes privadas virtuales (VPC) y las redes locales, sin exponer el tráfico a la Internet pública. Servicios de AWS AWS PrivateLink facilita la conexión de servicios entre diferentes cuentas y VPC. Para obtener más información, consulte AWS PrivateLink.
- Amazon S3: Amazon S3 es un servicio de almacenamiento de objetos. Deadline Cloud utiliza depósitos de Amazon S3 para almacenar los adjuntos de trabajos.
- Centro de identidad de IAM: el centro de identidad de IAM es un Servicio de AWS lugar en el que puede proporcionar a los usuarios un acceso de inicio de sesión único a todas sus cuentas y aplicaciones asignadas desde un solo lugar. También puede gestionar de forma centralizada el acceso a varias cuentas y los permisos de usuario a todas sus cuentas AWS Organizations. Para obtener más información, consulte Preguntas frecuentes de AWS IAM Identity Center.

Cómo funciona Deadline Cloud

Con Deadline Cloud, puedes crear y gestionar proyectos y trabajos de renderizado directamente desde las estaciones de trabajo y los canales de creación de contenido digital (DCC).

Puede enviar los trabajos a Deadline Cloud mediante el AWS SDK, AWS Command Line Interface (AWS CLI) o los remitentes de trabajos de Deadline Cloud. Deadline Cloud admite la descripción de trabajo abierta (OpenJD) para la especificación de plantillas de trabajo. Para obtener más información, consulte Open Job Description en el GitHub sitio web.

Deadline Cloud proporciona ofertas de trabajo a los candidatos. Un remitente de trabajos es un complemento de DCC para enviar trabajos de renderizado desde una interfaz de DCC de terceros, como o. Maya Nuke Con un remitente, los artistas pueden enviar los trabajos de renderizado desde una interfaz de terceros a Deadline Cloud, donde se gestionan los recursos del proyecto y se supervisan los trabajos, todo en un solo lugar.

Con una granja de Deadline Cloud, puedes crear colas y flotas, gestionar los usuarios y gestionar el uso y los costes de los recursos del proyecto. Una granja se compone de colas y flotas. Una cola es el lugar donde se encuentran los trabajos enviados y se programa su procesamiento. Una flota es un grupo de nodos de trabajo que ejecutan tareas para completar los trabajos. Una cola debe estar asociada a una flota para que los trabajos se puedan procesar. Una sola flota puede admitir varias colas y una cola puede ser compatible con varias flotas.

Los trabajos constan de pasos y cada paso consta de tareas específicas. Con el monitor de Deadline Cloud, puede acceder a los estados, registros y otras métricas de solución de problemas para los trabajos, los pasos y las tareas.

Permisos en Deadline Cloud

Deadline Cloud admite lo siguiente:

- Administrar el acceso a sus operaciones de API mediante AWS Identity and Access Management (IAM)
- Administrar el acceso de los usuarios de la fuerza laboral mediante una integración con AWS IAM Identity Center

Antes de que cualquier persona pueda trabajar en un proyecto, debe tener acceso a ese proyecto y a la granja asociada. Deadline Cloud está integrado con el IAM Identity Center para gestionar la autenticación y la autorización del personal. Los usuarios se pueden añadir directamente al Centro de identidad de IAM o se puede conectar a su proveedor de identidad (IdP) Okta existente, como o. Active Directory Los administradores de TI pueden conceder permisos de acceso a usuarios y grupos en distintos niveles. Cada nivel subsiguiente incluye los permisos de los niveles anteriores. La siguiente lista describe los cuatro niveles de acceso, desde el nivel más bajo hasta el más alto:

- Visor: permiso para ver los recursos de las granjas, las colas, las flotas y los trabajos a los que tienen acceso. Un espectador no puede enviar trabajos ni realizar cambios en ellos.
- Colaborador: igual que un espectador, pero con permiso para enviar trabajos a una cola o a una granja.
- Gestor: igual que el colaborador, pero con permiso para editar los trabajos de las colas a las que tiene acceso y conceder permisos sobre los recursos a los que tiene acceso.
- Propietario: igual que el administrador, pero puede ver y crear presupuestos y ver el uso.

> **Note**
>
> Estos permisos no otorgan a los usuarios acceso a la infraestructura de Deadline Cloud AWS Management Console ni permiso para modificarla.

Los usuarios deben tener acceso a una granja antes de poder acceder a las colas y flotas asociadas. El acceso de los usuarios se asigna a las colas y a las flotas por separado dentro de una granja.

Puede añadir usuarios de forma individual o como parte de un grupo. Añadir grupos a una granja, flota o cola puede facilitar la administración de los permisos de acceso para grupos grandes de personas. Por ejemplo, si tienes un equipo que trabaja en un proyecto específico, puedes añadir a cada uno de los miembros del equipo a un grupo. A continuación, puedes conceder permisos de acceso a todo el grupo para la granja, flota o cola correspondiente.

Soporte de software con Deadline Cloud

Deadline Cloud funciona con cualquier aplicación de software que pueda ejecutarse desde una interfaz de línea de comandos y controlarse mediante valores de parámetros. Deadline Cloud admite la OpenJD especificación para describir el trabajo como trabajos con pasos de secuencias de comandos de software que se parametrizan (por ejemplo, en un rango de fotogramas) en tareas. Reúna OpenJD las instrucciones de trabajo en paquetes de tareas con las herramientas y funciones de Deadline Cloud para crear, ejecutar y licenciar los pasos desde una aplicación de software de terceros.

Los trabajos necesitan una licencia para renderizarse. Deadline Cloud ofrece licencias basadas en el uso (UBL) para una selección de licencias de aplicaciones de software que se facturan por horas en incrementos de minutos en función del uso. Con Deadline Cloud, también puedes usar tus propias licencias de software si lo deseas. Si un trabajo no puede acceder a una licencia, no se procesa y produce un error que aparece en el registro de tareas del monitor de Deadline Cloud.

Cómo empezar con Deadline Cloud

Para crear una granja en AWS Deadline Cloud, puedes usar la consola de Deadline Cloud o el AWS Command Line Interface (AWS CLI). Usa la consola para disfrutar de una experiencia guiada de creación de la granja, que incluye colas y flotas. Úsala AWS CLI para trabajar directamente con el servicio o para desarrollar tus propias herramientas que funcionen con Deadline Cloud.

Para crear una granja y usar el monitor de Deadline Cloud, configura tu cuenta en Deadline Cloud. Solo necesitas configurar la infraestructura de monitoreo de Deadline Cloud una vez por cuenta. Desde su granja, puede administrar su proyecto, incluido el acceso de los usuarios a su granja y sus recursos.

Para crear una granja sin configurar la infraestructura de monitoreo de Deadline Cloud, configura una estación de trabajo para desarrolladores para Deadline Cloud.

Para crear una granja con recursos mínimos para aceptar trabajos, selecciona Inicio rápido en la página de inicio de la consola. Configura el monitor de Deadline Cloudle guía a través de esos pasos. Estas granjas comienzan con una cola y una flota que se asocian automáticamente. Este enfoque es una forma práctica de crear granjas tipo sandbox en las que experimentar.

Temas

- Configuración de su Cuenta de AWS
- Configura el monitor de Deadline Cloud
- Configuración de una estación de trabajo para desarrolladores para Deadline Cloud
- Configura los remitentes de Deadline Cloud
- Usa la granja

Configuración de su Cuenta de AWS

Configura el tuyo Cuenta de AWS para usar AWS Deadline Cloud.

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.

2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

Cuando creas una por primera vez Cuenta de AWS, comienzas con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta.

> **Important**
>
> Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Configura el monitor de Deadline Cloud

Para empezar, tendrás que crear tu infraestructura de monitorización de Deadline Cloud y definir tu granja. También puede realizar pasos opcionales adicionales, como agregar grupos y usuarios, elegir un rol de servicio y agregar etiquetas a sus recursos.

Paso 1: Configura el monitor

El monitor Deadline Cloud que se utiliza AWS IAM Identity Center para autorizar a los usuarios. La instancia del IAM Identity Center que utilices para Deadline Cloud debe estar en la Región de AWS misma ubicación que el monitor. Si su consola utiliza una región diferente al crear el monitor, recibirá un recordatorio para cambiarse a la región del centro de identidad de IAM.

La infraestructura del monitor consta de los siguientes componentes:

- Nombre para mostrar del monitor: el nombre para mostrar del monitor es la forma en que puede identificar su monitor, por ejemplo, el AnyCompany monitor. El nombre del monitor también determina la URL del monitor.

  > **Important**
  >
  > No puede cambiar el nombre que se muestra en el monitor una vez que haya terminado de configurarlo.

- URL del monitor: puede acceder al monitor mediante la URL del monitor. La URL se basa en el nombre que se muestra en el monitor, por ejemplo, https://anycompanymonitor.awsapps.com.

  > **Important**
  >
  > No puede cambiar la URL del monitor una vez finalizada la configuración.

- Región de AWS: Región de AWSEs la ubicación física de un conjunto de centros de AWS datos. Al configurar el monitor, la región elige de forma predeterminada la ubicación más cercana a usted. Le recomendamos que cambie la región para que esté más cerca de sus usuarios. Esto reduce el retraso y mejora las velocidades de transferencia de datos. AWS IAM Identity Center debe estar activado de la Región de AWS misma manera que Deadline Cloud.

  > **Important**
  >
  > No puedes cambiar tu región una vez hayas terminado de configurar Deadline Cloud.

Complete las tareas de esta sección para configurar la infraestructura de su monitor.

Para configurar la infraestructura del monitor

1. Inicie sesión en AWS Management Consolepara iniciar la configuración de Welcome to Deadline Cloud y, a continuación, seleccione Siguiente.
2. Introduzca el nombre que se muestra en el monitor, por ejemplo**`AnyCompany Monitor`**.
3. (Opcional) Para cambiar el nombre del monitor, elija Editar URL.
4. (Opcional) Para cambiarlo Región de AWSpara que esté más cerca de sus usuarios, elija Cambiar región.

a. Elija la región que esté más próxima a la mayoría de los usuarios.

b. Elija Añadir región.

- (Opcional) Para añadir grupos y usuarios, selecciona (Opcional) Agregue grupos y usuarios.
- (Opcional) Para personalizar aún más la configuración del monitor, seleccione Ajustes adicionales.

5. Si está preparado para hacerlo Paso 2: Defina los detalles de la granja, seleccione Siguiente.

(Opcional) Agregue grupos y usuarios

Antes de completar la configuración del monitor de Deadline Cloud, puede añadir usuarios del monitor y añadirlos a un grupo.

Una vez completada la configuración, puede crear nuevos usuarios y grupos y administrar los usuarios, por ejemplo, asignándoles grupos, permisos y aplicaciones, o eliminar usuarios de su monitor.

Ajustes adicionales

La configuración de Deadline Cloud incluye ajustes adicionales. Con estos ajustes, puede ver todos los cambios que la configuración de Deadline Cloud le ha Cuenta de AWS realizado, configurar su rol de usuario supervisor y cambiar el tipo de clave de cifrado.

AWS IAM Identity Center

AWS IAM Identity Center es un servicio de inicio de sesión único basado en la nube para administrar usuarios y grupos. El IAM Identity Center también se puede integrar con el proveedor de inicio de sesión único (SSO) empresarial para que los usuarios puedan iniciar sesión con la cuenta de su empresa.

Deadline Cloud habilita el Centro de Identidad de IAM de forma predeterminada y es necesario configurar y utilizar Deadline Cloud. La instancia del IAM Identity Center que utilices para Deadline Cloud debe estar en la Región de AWS misma ubicación que el monitor. Para obtener más información, consulte Qué es AWS IAM Identity Center.

Configure la función de acceso al servicio

Un AWS servicio puede asumir un rol de servicio para realizar acciones en su nombre. Deadline Cloud requiere un rol de usuario supervisor para que los usuarios puedan acceder a los recursos de su monitor.

Puede adjuntar políticas gestionadas AWS Identity and Access Management (IAM) a la función de usuario supervisor. Las políticas permiten a los usuarios realizar determinadas acciones, como crear trabajos en una aplicación específica de Deadline Cloud. Como las aplicaciones dependen de condiciones específicas de la política administrada, si no usa las políticas administradas, es posible que la aplicación no funcione como se espera.

Puedes cambiar la función del usuario supervisor después de completar la configuración, en cualquier momento. Para obtener más información sobre los roles, consulte Roles de IAM.

Las siguientes pestañas contienen instrucciones para dos casos prácticos diferentes. Para crear y utilizar un nuevo rol de servicio, elija la pestaña Nuevo rol de servicio. Para usar un rol de servicio existente, seleccione la pestaña Rol de servicio existente.

New service role

Para crear y usar un nuevo rol de servicio

1. Seleccione Crear y utilizar un nuevo rol de servicio.
2. (Opcional) Escriba un Nombre del rol de usuario del servicio.
3. Seleccione Ver los detalles de los permisos para obtener más información sobre el rol.

Existing service role

Para usar un rol de servicio existente

1. Seleccione Utilizar un rol de servicio existente.
2. Abra la lista desplegable para elegir un rol de servicio existente.
3. (Opcional) Seleccione Ver en la consola de IAM para obtener más información sobre el rol.

Paso 2: Defina los detalles de la granja

De vuelta a la consola de Deadline Cloud, complete los siguientes pasos para definir los detalles de la granja.

1. En Detalles de la granja, agrega un nombre para la granja.
2. En Descripción, introduzca la descripción de la granja. Una descripción clara puede ayudarle a identificar rápidamente el propósito de su granja.
3. (Opcional) De forma predeterminada, sus datos se cifran con una clave que le AWS pertenece y administra para su seguridad. Puede elegir Personalizar la configuración de cifrado (avanzada) para usar una clave existente o crear una nueva que administre.

   Si elige personalizar la configuración de cifrado mediante la casilla de verificación, introduzca un AWS KMS ARN o cree uno AWS KMS nuevo seleccionando Crear nueva clave KMS.
4. (Opcional) Seleccione Añadir nueva etiqueta para añadir una o más etiquetas a su granja.
5. Seleccione una de las siguientes opciones:

   - Seleccione Saltar para revisar y Crear para revisar y crear su granja.
   - Selecciona Siguiente para continuar con los pasos opcionales adicionales.

(Opcional) Paso 3: Definir los detalles de la cola

La cola es responsable de realizar un seguimiento del progreso y programar el trabajo para sus trabajos.

1. Empezando por los detalles de la cola, introduzca un nombre para la cola.
2. En Descripción, introduzca la descripción de la cola. Una descripción clara puede ayudarle a identificar rápidamente el propósito de la cola.
3. En el caso de los adjuntos de tareas, puede crear un nuevo bucket de Amazon S3 o elegir un bucket de Amazon S3 existente. Si no tienes un bucket de Amazon S3 existente, tendrás que crear uno.

   a. Para crear un nuevo bucket de Amazon S3, seleccione Create new job bucket. Puede definir el nombre del depósito de trabajos en el campo de prefijo raíz. Te recomendamos que llames al depósito. **`deadlinecloud-job-attachments-[MONITORNAME]`**

      Solo puedes usar letras minúsculas y guiones. Sin espacios ni caracteres especiales.

   b. Para buscar y seleccionar un bucket de Amazon S3 existente, selecciona Elegir entre un bucket de Amazon S3 existente. A continuación, busque un bucket existente seleccionando Browse S3. Cuando aparezca la lista de sus depósitos de Amazon S3 disponibles, seleccione el depósito de Amazon S3 que desee utilizar para la cola.

4. Si utiliza flotas gestionadas por el cliente, seleccione Habilitar la asociación con las flotas gestionadas por el cliente.

    - En el caso de las flotas gestionadas por el cliente, añada un usuario configurado en cola y, a continuación, establezca las credenciales de POSIX o Windows. Como alternativa, puedes omitir la función de ejecución seleccionando la casilla de verificación.

5. La cola necesita permiso para acceder a Amazon S3 en su nombre. Le recomendamos que cree un nuevo rol de servicio para cada cola.

    a. Para un nuevo rol, complete los siguientes pasos.

        i. Seleccione Crear y utilizar un nuevo rol de servicio.

        ii. Introduzca un nombre de función para su función de cola o utilice el nombre de función proporcionado.

        iii. (Opcional) Añada una descripción del rol de cola.

        iv. Para ver los permisos de IAM para el rol de cola, seleccione Ver detalles del permiso.

    b. Como alternativa, puede elegir un rol de servicio existente.

6. (Opcional) Agregue variables de entorno para el entorno de colas mediante pares de nombre y valor.

7. (Opcional) Añada etiquetas a la cola mediante pares de claves y valores.

Después de introducir todos los detalles de la cola, selecciona Siguiente.

(Opcional) Paso 4: Defina los detalles de la flota

Una flota asigna trabajadores para ejecutar sus tareas de renderizado. Si necesita una flota para sus tareas de renderizado, active la casilla Crear flota.

1. Detalles de la flota

    a. Proporcione un nombre y una descripción opcional para su flota.

    b. Seleccione la forma en que deben escalarse sus recursos informáticos. La opción gestionada por el servicio permite a Deadline Cloud escalar automáticamente sus recursos de cómputo. La opción gestionada por el cliente le permite controlar su propio escalado de cómputo.

2. En la sección de opciones de instancia, elija Spot o On-Demand. Las instancias bajo demanda de Amazon EC2 ofrecen una disponibilidad más rápida y las instancias puntuales de Amazon EC2 son mejores para ahorrar costes.
3. Para escalar automáticamente el número de instancias de su flota, elija un número mínimo de instancias y un número máximo de instancias.

   Recomendamos encarecidamente establecer siempre el número mínimo de instancias para **0** evitar incurrir en costes adicionales.
4. Su flota necesita permiso para escribir CloudWatch en su nombre. Le recomendamos que cree una nueva función de servicio para cada flota.

   a. Para un nuevo rol, complete los siguientes pasos.

      i. Seleccione Crear y utilizar un nuevo rol de servicio.
      ii. Introduzca un nombre de función para su función de flota o utilice el nombre de función proporcionado.
      iii. (Opcional) Añada una descripción del rol de la flota.
      iv. Para ver los permisos de IAM para el rol de flota, selecciona Ver detalles del permiso.

   b. Como alternativa, puede usar un rol de servicio existente.
5. (Opcional) Añada etiquetas a la flota mediante pares de claves y valores.

Después de introducir todos los detalles de la flota, selecciona Siguiente.

(Opcional) Paso 5: configurar los requisitos de los trabajadores

Defina los requisitos para sus instancias de trabajadores.

1. Revise la configuración del sistema operativo (SO) y la arquitectura de la CPU para conocerla.
2. Actualice la cantidad mínima y máxima de vCPU según sus requisitos de hardware.
3. Actualice la cantidad mínima y máxima de memoria (GiB) según sus requisitos de hardware.
4. Puede filtrar los tipos de instancias permitiendo o excluyendo tipos de instancias de trabajo. En ambas opciones de filtrado, puede filtrar hasta 10 tipos de instancias de Amazon EC2.
5. En Requisitos adicionales (opcional), puede definir el volumen raíz de EBS por tamaño (GiB), IOPS y rendimiento (MiB/s).
6. Una vez establecidos todos los requisitos de trabajadores, elija Siguiente para definir el nivel de acceso de sus grupos.

(Opcional) Paso 6: Defina los niveles de acceso

Si tiene grupos conectados a su monitor, puede definir su nivel de acceso. El permiso para usar las funciones de Deadline Cloud se administra por niveles de acceso. Puede asignar diferentes niveles de acceso a grupos de usuarios.

1. Usa el menú de niveles de acceso a la granja de Deadline Cloud para seleccionar el nivel de permiso para el grupo.
2. Selecciona Siguiente para continuar y revisar todos los detalles de la granja ingresados.

Paso 7: Revisa y crea

Revisa toda la información ingresada para crear tu granja. Cuando esté listo, elija Crear granja.

El progreso de la creación de tu granja se muestra en la página Granjas. Aparece un mensaje de éxito cuando la granja está lista para usarse.

Configuración de una estación de trabajo para desarrolladores para Deadline Cloud

En este tutorial, los utilizarás AWS CloudShell para crear una granja de desarrolladores sencilla y ejecutar el agente trabajador. A continuación, podrá enviar y ejecutar un trabajo sencillo con parámetros y adjuntos, añadir una flota gestionada por el servicio y limpiar los recursos de su granja cuando haya terminado.

En las siguientes secciones, se presentan las diferentes funciones de Deadline Cloud y cómo funcionan y funcionan juntas. Seguir estos pasos resulta útil para desarrollar y probar nuevas cargas de trabajo y personalizaciones.

Temas

- Paso 1: Cree una granja de Deadline Cloud
- Paso 2: ejecuta el agente de trabajo en modo desarrollador en Deadline Cloud
- Paso 3: Envía y ejecuta trabajos con Deadline Cloud
- Paso 4: Ejecute los trabajos con los archivos adjuntos en Deadline Cloud
- Paso 5: Agrega una flota de servicios gestionados a tu granja de desarrolladores en Deadline Cloud

- Paso 6: Limpia los recursos de tu granja en Deadline Cloud

Paso 1: Cree una granja de Deadline Cloud

Para crear tu granja de desarrolladores y poner en cola los recursos en AWS Deadline Cloud, usa el AWS Command Line Interface (AWS CLI), tal y como se muestra en el siguiente procedimiento. También crearás un rol AWS Identity and Access Management (IAM) y una flota gestionada por el cliente (CMF) y asociarás la flota a tu cola. A continuación, puede configurar la granja AWS CLI y confirmar que está configurada y funcionando según lo especificado.

Puedes usar esta granja para explorar las funciones de Deadline Cloud y, a continuación, desarrollar y probar nuevas cargas de trabajo, personalizaciones e integraciones de canalizaciones.

Para crear una granja

1. Instale y configure el AWS Command Line Interface (AWS CLI), si aún no lo ha hecho. Para obtener información, consulte Instalar o actualizar a la última versión de AWS CLI.
2. Cree un nombre para su granja y añada ese nombre a`~/.bashrc`. Esto hará que esté disponible para otras sesiones terminales.

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

3. Cree el recurso de granja y añada su ID de granja a`~/.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. Cree el recurso de cola y añada su ID de cola a `~/.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. Cree un rol de IAM para la flota. Esta función proporciona a los trabajadores anfitriones de su flota las credenciales de seguridad necesarias para ejecutar los trabajos desde su lista de espera.

```
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. Cree la flota gestionada por el cliente (CMF) y añada su ID de flota a. `~/.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. Asegúrese de poder acceder a Deadline Cloud.

```
pip install deadline
```

8. Asocia el CMF a tu cola.

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

9. Para establecer la granja predeterminada en el ID de granja y la cola en el ID de cola que creó anteriormente, utilice el siguiente comando.

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

10. (Opcional) Para confirmar que la granja está configurada de acuerdo con sus especificaciones, utilice los siguientes comandos:

    - Enumere todas las granjas: **`deadline farm list`**
    - Listar todas las colas de la granja predeterminada: **`deadline queue list`**
    - Listar todas las flotas de la granja predeterminada: **`deadline fleet list`**

- Obtenga la granja predeterminada: **`deadline farm get`**
- Obtenga la cola predeterminada: **`deadline queue get`**
- Obtenga todas las flotas asociadas a la cola predeterminada: **`deadline fleet get`**

Paso 2: ejecuta el agente de trabajo en modo desarrollador en Deadline Cloud

Para poder ejecutar los trabajos que envíes a la lista de espera de tu granja de desarrolladores, debes ejecutar el agente de trabajo de AWS Deadline Cloud en modo desarrollador en un host de trabajo.

Durante el resto de este tutorial, realizarás AWS CLI operaciones en tu granja de desarrolladores mediante dos AWS CloudShell pestañas. En la primera pestaña, puede enviar trabajos. En la segunda pestaña, puede ejecutar el agente de trabajo.

> **Note**
>
> Si deja la CloudShell sesión inactiva durante más de 20 minutos, se agotará el tiempo de espera y se detendrá al agente de trabajo. Para reiniciar el agente de trabajo, siga las instrucciones del siguiente procedimiento.

Para ejecutar el agente de trabajo en modo desarrollador

1. Instale y configure el AWS Command Line Interface (AWS CLI), si aún no lo ha hecho. Para obtener información, consulte Instalar o actualizar a la última versión de AWS CLI.
2. Con la granja aún abierta en la primera CloudShell pestaña, abra una segunda CloudShell pestaña y, a continuación, cree los `demoenv-persist` directorios `demoenv-logs` y.

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

3. Descarga e instala los paquetes de agentes de trabajo de Deadline Cloud desde PyPI:

> **Note**
>
> SíWindows, es necesario que los archivos del agente estén instalados en el directorio global de paquetes de sitios de Python. Los entornos virtuales de Python no son compatibles actualmente.

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

4. Para permitir que el agente de trabajo cree los directorios temporales para las tareas en ejecución, cree un directorio:

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

5. Ejecute el agente de trabajo de Deadline Cloud en modo desarrollador con `DEV_FARM_ID` las variables `DEV_CMF_ID` que haya agregado al`~/.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
```

A medida que el agente de trabajo inicializa y, a continuación, sondea la operación de la `UpdateWorkerSchedule` API, se muestra el siguiente resultado:

```
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) ...
...
```

6. Seleccione la primera CloudShell pestaña y, a continuación, enumere los trabajadores de la flota.

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

Se muestra un resultado como el siguiente:

```
Displaying 1 of 1 workers starting at 0

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

En una configuración de producción, el agente de trabajo de Deadline Cloud requiere configurar varios usuarios y directorios de configuración como usuario administrativo en la máquina host. Puede anular esta configuración porque ejecuta los trabajos en su propia granja de desarrollo, a la que solo usted puede acceder.

Paso 3: Envía y ejecuta trabajos con Deadline Cloud

Para usar AWS Deadline Cloud para ejecutar trabajos, sigue los siguientes procedimientos. Usa la primera AWS CloudShell pestaña para enviar trabajos a tu granja de desarrolladores. Utilice la segunda CloudShell pestaña para ver el resultado del agente obrero.

Temas

- Envíe la simple_job muestra
- Envíe un anuncio simple_job con un parámetro
- Cree un paquete de trabajos simple_file_job con E/S de archivos

Envíe la simple_job muestra

Después de crear una granja y gestionar el agente obrero, puede enviar la simple_job muestra a Deadline Cloud.

Para enviar la simple_job muestra a Deadline Cloud

1. Instale y configure AWS Command Line Interface (AWS CLI), si aún no lo ha hecho. Para obtener información, consulte Instalar o actualizar a la última versión de AWS CLI.
2. Descargue el ejemplo de GitHub.

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

3. Elija la primera CloudShell pestaña y, a continuación, navegue hasta el directorio de ejemplos de paquetes de trabajos.

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

4. Envíe la simple_job muestra.

```
deadline bundle submit simple_job
```

5. Seleccione la segunda CloudShell pestaña para ver el resultado del registro sobre las llamadas`BatchGetJobEntities`, la obtención de una sesión y la ejecución de una acción de sesión.

```
...
[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**
>
> Solo se muestra el resultado del registro del agente de trabajo. Hay un registro independiente para la sesión en la que se ejecuta el trabajo.

6. Elija la primera pestaña y, a continuación, inspeccione los archivos de registro que escribe el agente de trabajo.

   a. Navegue hasta el directorio de registros del agente de trabajo y vea su contenido.

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

   b. Imprima el primer archivo de registro que cree el agente de trabajo.

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

Este archivo contiene información sobre cómo llamó a la API de Deadline Cloud para crear un recurso de trabajadores en su flota y, después, asumió la función de flota.

c. Imprima el resultado del archivo de registro cuando el agente obrero se una a la flota.

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

Este registro contiene resultados sobre todas las acciones que realiza el agente trabajador, pero no contiene resultados sobre las colas desde las que ejecuta los trabajos, excepto los ID de esos recursos.

d. Imprima los archivos de registro de cada sesión en un directorio que tenga el mismo nombre que el identificador del recurso de la cola.

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

Si el trabajo se realiza correctamente, la salida del archivo de registro será similar a la siguiente:

```
 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. Imprima la información sobre el trabajo.

   ```
   deadline job get
   ```

   Al enviar el trabajo, el sistema lo guarda como predeterminado para que no tenga que introducir el identificador del trabajo.

Envíe un anuncio simple_job con un parámetro

Puede enviar trabajos con parámetros. En el siguiente procedimiento, edite la simple_job plantilla para incluir un mensaje personalizado, envíe el simple_job archivo de registro de la sesión e imprima el mismo para ver el mensaje.

Para enviar el simple_job ejemplo con un parámetro

1. Seleccione la primera CloudShell pestaña y, a continuación, navegue hasta el directorio de ejemplos de paquetes de trabajos.

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

2. Imprima el contenido de la simple_job plantilla.

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

   La `parameterDefinitions` sección con el `Message` parámetro debería tener el siguiente aspecto:

   ```
   parameterDefinitions:
   - name: Message
     type: STRING
   ```

```
  default: Welcome to AWS Deadline Cloud!
```

3. Envíe la simple_job muestra con un valor de parámetro y espere a que el trabajo termine de ejecutarse.

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

4. Para ver el mensaje personalizado, consulte el archivo de registro de sesión más reciente.

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

Cree un paquete de trabajos simple_file_job con E/S de archivos

Un trabajo de renderizado necesita leer la definición de la escena, renderizar una imagen a partir de ella y, a continuación, guardar esa imagen en un archivo de salida. Puede simular esta acción haciendo que el trabajo calcule el hash de la entrada en lugar de renderizar una imagen.

Para crear un paquete de trabajos simple_file_job con E/S de archivos

1. Seleccione la primera CloudShell pestaña y, a continuación, navegue hasta el directorio de ejemplos del paquete de trabajos.

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

2. Haga una copia de `simple_job` con el nuevo nombre`simple_file_job`.

```
cp -r simple_job simple_file_job
```

3. Edite la plantilla de trabajo de la siguiente manera:

> **Note**
>
> Le recomendamos que utilice nano estos pasos. Si prefiere usarloVim, debe configurar su modo de pegado usando`:set paste`.

   a. Abre la plantilla en un editor de texto.

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

b. Añada lo siguiente `typeobjectType`, y `dataFlowparameterDefinitions`.

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

c. Añada el siguiente comando de `bash` script al final del archivo para leer el archivo de entrada y escribir en el archivo de salida.

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

La actualización `template.yaml` debe coincidir exactamente con lo siguiente:

```
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.runScript}}'
```

```
    embeddedFiles:
    - name: runScript
      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**
>
> Si desea ajustar el espaciado`template.yaml`, asegúrese de utilizar espacios en lugar de hendiduras.

d. Guarde el archivo y salga del editor de texto.

4. Proporcione los valores de los parámetros de los archivos de entrada y salida para enviar el simple_file_job.

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

5. Imprima la información sobre el trabajo.

```
deadline job get
```

- Verá un resultado como el siguiente:

```
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
```

- Aunque solo proporcionó rutas relativas, los parámetros tienen configurada la ruta completa. AWS CLI Une el directorio de trabajo actual a cualquier ruta que se proporcione como parámetro cuando las rutas tienen ese tipoPATH.
- El agente de trabajo que se encuentra en la otra ventana de terminal recoge y ejecuta el trabajo. Esta acción crea el `hash.txt` archivo, que puede ver con el siguiente comando.

  ```
  cat hash.txt
  ```

  Este comando imprimirá un resultado similar al siguiente.

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

Paso 4: Ejecute los trabajos con los archivos adjuntos en Deadline Cloud

Muchas granjas utilizan sistemas de archivos compartidos para compartir archivos entre los anfitriones que envían los trabajos y los que los ejecutan. Por ejemplo, en el `simple_file_job` ejemplo anterior, el sistema de archivos local se comparte entre las ventanas de AWS CloudShell terminal, que se encuentran en la pestaña uno, donde se envía el trabajo, y en la pestaña dos, donde se ejecuta el agente de trabajo.

Un sistema de archivos compartido es ventajoso cuando la estación de trabajo remitente y los hosts de trabajo se encuentran en la misma red de área local. Si almacena los datos de forma local, cerca de las estaciones de trabajo que acceden a ellos, si utiliza una granja de servidores basada en la nube, tendrá que compartir sus sistemas de archivos a través de una VPN de alta latencia o sincronizarlos en la nube. Ninguna de estas opciones es fácil de configurar ni utilizar.

AWS Deadline Cloud ofrece una solución sencilla con archivos adjuntos de trabajo, que son similares a los archivos adjuntos de correo electrónico. Con los adjuntos de trabajo, puede adjuntar datos a su trabajo. A continuación, Deadline Cloud gestiona los detalles de la transferencia y el almacenamiento de los datos de su trabajo en depósitos de Amazon Simple Storage Service (Amazon S3).

Los flujos de trabajo de creación de contenido suelen ser iterativos, lo que significa que un usuario envía los trabajos con un pequeño subconjunto de archivos modificados. Como los buckets de Amazon S3 almacenan los adjuntos de los trabajos en un almacenamiento direccionable por contenido, el nombre de cada objeto se basa en el hash de los datos del objeto y el contenido de un árbol de directorios se almacena en un formato de archivo de manifiesto adjunto a un trabajo.

Para ejecutar trabajos con trabajos adjuntos, complete los siguientes pasos.

Temas

- Añada una configuración de adjuntos de trabajos a su cola
- Enviar simple_file_job con adjuntos de trabajo
- Entender cómo se almacenan los archivos adjuntos de trabajo en Amazon S3

Añada una configuración de adjuntos de trabajos a su cola

Para habilitar los adjuntos de trabajos en su cola, añada una configuración de adjuntos de trabajos al recurso de cola de su cuenta.

Para añadir una configuración de adjuntos de trabajos a su cola

1. Instale y configure el AWS Command Line Interface (AWS CLI), si aún no lo ha hecho. Para obtener información, consulte Instalar o actualizar a la última versión de AWS CLI.
2. Seleccione la primera CloudShell pestaña y, a continuación, introduzca uno de los siguientes comandos para usar un bucket de Amazon S3 para adjuntar trabajos.
   - Si no tiene un bucket privado de Amazon S3 existente, puede crear y usar un bucket S3 nuevo.

     ```
     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}
     ```

   - Si ya tienes un bucket privado de Amazon S3, puedes usarlo *MY_BUCKET_NAME*sustituyéndolo por el nombre de tu bucket.

     ```
     DEV_FARM_BUCKET=MY_BUCKET_NAME
     ```

3. Después de crear o elegir su bucket de Amazon S3, añada el nombre del bucket `~/.bashrc` para que esté disponible para otras sesiones de terminal.

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

4. Cree un rol AWS Identity and Access Management (de IAM) para la cola.

```
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"
                }
            ]
            }'
```

5. Actualice la cola para incluir la configuración de los adjuntos de trabajos y la función de IAM.

```
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"
        }'
```

6. Confirme que ha actualizado la cola.

```
deadline queue get
```

Se muestra un resultado como el siguiente:

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

Enviar simple_file_job con adjuntos de trabajo

Cuando utilizas adjuntos de trabajo, los paquetes de trabajos deben proporcionar a Deadline Cloud suficiente información para determinar el flujo de datos del trabajo, por ejemplo, mediante PATH parámetros. En el caso desimple_file_job, editaste el `template.yaml` archivo para indicar a Deadline Cloud que el flujo de datos está en el archivo de entrada y en el archivo de salida.

Una vez que hayas añadido la configuración de adjuntos de trabajos a tu lista, puedes enviar el ejemplo de simple_file_job con los adjuntos de trabajo. Una vez hecho esto, podrá ver el registro

y el resultado de los trabajos para confirmar que el archivo con los trabajos adjuntos funciona. simple_file_job

Para enviar el paquete de trabajos simple_file_job con los trabajos adjuntos

1. Elija la primera CloudShell pestaña y, a continuación, abra el directorio. `JobBundle-Samples`
2.
```
cd ~/AmazonDeadlineCloud-DocumentationAndSamples/JobBundle-Samples
```
3. Envía simple_file_job a la lista de espera. Cuando se te pida que confirmes la carga, ingresa. **y**

```
deadline bundle submit simple_file_job \
    -p InFile=simple_job/template.yaml \
    -p OutFile=hash-jobattachments.txt
```
4. Para ver el resultado del registro de la sesión de transferencia de datos de los archivos adjuntos al trabajo, seleccione CloudShell la segunda pestaña.

```
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. Enumere las acciones de la sesión que se ejecutaron dentro de la sesión.

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

   Se muestra un resultado como el siguiente:

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

La primera acción de la sesión descargó los adjuntos del trabajo de entrada, mientras que la segunda acción ejecuta la tarea como antes y, a continuación, cargó los adjuntos del trabajo de salida.

6. Enumere el directorio de salida.

```
ls *.txt
```

Se muestra una salida como la que `hash.txt` se muestra, pero `hash-jobattachments.txt` no existe.

7. Descarga el resultado del trabajo más reciente.

```
deadline job download-output
```

8. Vea el resultado del archivo descargado.

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

Se muestra un resultado como el siguiente:

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

Entender cómo se almacenan los archivos adjuntos de trabajo en Amazon S3

Puede usar AWS Command Line Interface (AWS CLI) para cargar o descargar datos para los adjuntos de trabajos, que se almacenan en los buckets de Amazon S3. Comprender cómo Deadline Cloud almacena los adjuntos de trabajo en Amazon S3 le ayudará a desarrollar integraciones de cargas de trabajo y canalizaciones.

Para inspeccionar cómo se almacenan los adjuntos de trabajo de Deadline Cloud en Amazon S3

1. Elija la primera CloudShell pestaña y, a continuación, abra el directorio de ejemplos de paquetes de trabajos.

   ```
   cd ~/AmazonDeadlineCloud-DocumentationAndSamples/JobBundle-Samples
   ```

2. Inspeccione las propiedades del trabajo.

   ```
   deadline job get
   ```

   Se muestra un resultado como el siguiente:

   ```
   parameters:
     Message:
       string: Welcome to Amazon Deadline Cloud!
     InFile:
       path: /home/cloudshell-user/AmazonDeadlineCloud-DocumentationAndSamples/
   JobBundle-Samples/simple_job/template.yaml
     OutFile:
       path: /home/cloudshell-user/AmazonDeadlineCloud-DocumentationAndSamples/
   JobBundle-Samples/hash-jobattachments.txt
   attachments:
     manifests:
     - rootPath: /home/cloudshell-user/AmazonDeadlineCloud-DocumentationAndSamples/
   JobBundle-Samples
       rootPathFormat: posix
   ```

```
    outputRelativeDirectories:
    - .
    inputManifestPath: farm-3040c59a5b9943d58052c29d907a645d/queue-
cde9977c9f4d4018a1d85f3e6c1a4e6e/Inputs/
f46af01ca8904cd8b514586671c79303/0d69cd94523ba617c731f29c019d16e8_input.xxh128
    inputManifestHash: f95ef91b5dab1fc1341b75637fe987ee
  fileSystem: COPIED
```

El campo de adjuntos contiene una lista de estructuras de manifiesto que describen las rutas de datos de entrada y salida que utiliza el trabajo cuando se ejecuta. Observe `rootPath` la ruta del directorio local de la máquina que envió el trabajo. Para ver el sufijo de objeto de Amazon S3 que contiene un archivo de manifiesto, consulte. `inputManifestFile` El archivo de manifiesto contiene metadatos para una instantánea del árbol de directorios de los datos de entrada del trabajo.

3. Imprima de forma bonita el objeto del manifiesto de Amazon S3 para ver la estructura de directorios de entrada del trabajo.

```
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 .
```

Se muestra un resultado como el siguiente:

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

4. Cree el prefijo Amazon S3 que contiene los manifiestos de los adjuntos de los trabajos de salida y enumere el objeto debajo de él.

```
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
```

No se hace referencia directamente a los adjuntos del trabajo de salida desde el recurso del trabajo, sino que se colocan en un bucket de Amazon S3 en función de los ID de los recursos de la granja.

5. Obtenga la clave de objeto de manifiesto más reciente para el identificador de acción de sesión específico y, a continuación, imprima de forma bonita los objetos del manifiesto.

```
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 .
```

Verás las propiedades del archivo `hash-jobattachments.txt` en el resultado, como las siguientes:

```
{
     "hashAlg": "xxh128",
     "manifestVersion": "2023-03-03",
     "paths": [
     {
         "hash": "f60b8e7d0fabf7214ba0b6822e82e08b",
```

```
        "mtime": 1698785252554950,
        "path": "hash-jobattachments.txt",
        "size": 182
    }
    ],
    "totalSize": 182
}
```

Tu trabajo solo tendrá un objeto de manifiesto por cada tarea que se ejecute, pero en general es posible tener más objetos por tarea ejecutada.

6. Vea la salida de almacenamiento de Amazon S3 direccionable por contenido bajo el prefijo. `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 -
```

Se muestra un resultado como el siguiente:

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

Paso 5: Agrega una flota de servicios gestionados a tu granja de desarrolladores en Deadline Cloud

AWS CloudShell no proporciona suficiente capacidad de cómputo para probar cargas de trabajo más grandes. Tampoco está configurado para funcionar con trabajos que distribuyen las tareas en varios hosts de trabajo.

En lugar de utilizarla CloudShell, puede añadir una flota gestionada por el servicio (SMF) de Auto Scaling a su granja de desarrolladores. Un SMF proporciona suficiente capacidad de cómputo para cargas de trabajo más grandes y puede gestionar trabajos que necesiten distribuirse entre varios hosts de trabajo. El programador utilizará tanto a los trabajadores de SMF como a los de CMF para ejecutar los trabajos, a menos que cierre al trabajador de CMF.

Para añadir una flota gestionada por servicios a tu granja de desarrolladores

1. Instala y configura el AWS Command Line Interface (AWS CLI), si aún no lo has hecho. Para obtener información, consulte Instalar o actualizar a la última versión de AWS CLI.
2. Seleccione la primera AWS CloudShell pestaña y, a continuación, cree la flota gestionada por el servicio y añada su identificador de flota a `.bashrc`. Esta acción hace que esté disponible para otras sesiones de terminal.

```
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
```

3. Asocie el SMF a su cola.

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

4.

> **Note**
>
> El programador utilizará tanto a los trabajadores de SMF como a los de CMF para ejecutar los trabajos, a menos que cierre al trabajador de CMF.

Sométete a simple_file_job la cola. Cuando se te pida que confirmes la carga, ingresa**y**.

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

5. Confirme que el SMF funciona correctamente.

```
deadline fleet get
```

- El trabajador puede tardar unos minutos en empezar.
- La flota gestionada `queueFleetAssociationsStatus` por el cliente y la flota gestionada por el servicio será la flota gestionada por el cliente`ACTIVE`.
- El SMF `autoScalingStatus` cambiará de `GROWING` a`STEADY`.

Su estado será similar al siguiente:

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

6. Vea el registro del trabajo que envió. Este registro se guarda en un registro de Amazon CloudWatch Logs, no en el sistema de CloudShell archivos.

```
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
```

Paso 6: Limpia los recursos de tu granja en Deadline Cloud

Para desarrollar y probar nuevas cargas de trabajo e integraciones de canalizaciones, puedes seguir utilizando la granja de desarrolladores de Deadline Cloud que creaste para este tutorial. Si ya no necesitas tu granja de desarrolladores, puedes eliminar sus recursos, incluidos los roles de granja, flota, cola AWS Identity and Access Management (IAM) y registros en Amazon CloudWatch Logs. Tras eliminar estos recursos, tendrá que volver a empezar el tutorial para poder utilizarlos. Para obtener más información, consulte Configuración de una estación de trabajo para desarrolladores para Deadline Cloud.

Para limpiar los recursos de la granja de desarrolladores

1. Instale y configure AWS Command Line Interface (AWS CLI), si aún no lo ha hecho. Para obtener información, consulte Instalar o actualizar a la última versión de AWS CLI.
2. Selecciona la primera CloudShell pestaña y, a continuación, detiene todas las asociaciones de flotas de colas de tu cola.

```
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
```

3. Haz una lista de las asociaciones de flotas en cola.

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

Puede que tenga que volver a ejecutar el comando hasta que se muestre el resultado y`"status": "STOPPED"`, a continuación, puede continuar con el siguiente paso. Este proceso puede tardar varios minutos en completarse.

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

4. Elimine todas las asociaciones de colas y flotas de su cola.

```
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
```

5. Elimina todas las flotas asociadas a tu cola.

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

6. Elimine la cola.

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

7. Elimine la granja.

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

8. Elimina otros AWS recursos de tu granja.

   a. Elimine el rol de flota 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. Elimine la función de IAM de cola.

```
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. Elimine los grupos de CloudWatch registros de Amazon Logs. Cada cola y flota tiene su propio grupo de registros.

```
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"
```

Configura los remitentes de Deadline Cloud

Este proceso es para los administradores y artistas que desean instalar, configurar y lanzar el remitente de AWS Deadline Cloud. Un remitente de Deadline Cloud es un complemento de creación de contenido digital (DCC). Los artistas lo utilizan para enviar trabajos desde una interfaz de DCC de terceros con la que están familiarizados.

> **Note**
>
> Este proceso debe completarse en todas las estaciones de trabajo que los artistas utilizarán para enviar los renderizados.

Temas

- Paso 1: Instale el remitente de Deadline Cloud
- Paso 2: Instale y configure Deadline Cloud monitor
- Paso 3: Inicie el remitente de Deadline Cloud

Paso 1: Instale el remitente de Deadline Cloud

Las siguientes secciones lo guían por los pasos para instalar el remitente de Deadline Cloud.

Descarga el instalador del remitente

Antes de poder instalar el remitente de Deadline Cloud, debe descargar el instalador del remitente. Actualmente, el instalador del remitente de Deadline Cloud solo admite y. Windows Linux

1. Inicie sesión en la consola de Deadline Cloud AWS Management Console y ábrala.
2. En el panel de navegación lateral, selecciona Descargas.
3. Localice la sección de instalación del remitente de Deadline Cloud.
4. Selecciona el instalador para el sistema operativo de tu ordenador y, a continuación, selecciona Descargar.

(Opcional) Compruebe la autenticidad del software descargado

Para comprobar que el software que ha descargado es auténtico, utilice el siguiente procedimiento para una Windows u otraLinux.

> **Note**
>
> Puedes usar estas instrucciones para verificar primero el instalador y, después, verificar el monitor de Deadline Cloud después de descargarlo en la siguiente sección (paso 2).

Windows

Para comprobar la autenticidad de los archivos descargados, complete los siguientes pasos.

1. En el siguiente comando, *`file`* reemplácelo por el archivo que desee comprobar. Por ejemplo, ***`C:\PATH\TO\MY\`*`DeadlineCloudSubmitter-windows-x64-installer.exe`** . Además, *`signtool-sdk-version`* sustitúyalo por la versión del SignTool SDK instalada. Por ejemplo, **`10.0.22000.0`**.

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

2. Por ejemplo, puede verificar el archivo de instalación del remitente de Deadline Cloud ejecutando el siguiente comando:

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

Linux

Para comprobar la autenticidad de los archivos descargados, utilice la herramienta de línea de gpg comandos.

1. Importe la 0penPGP clave del instalador del remitente de Deadline Cloud ejecutando el siguiente comando:

```
 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. Determine si debe confiar en la 0penPGP clave. Algunos factores que se deben tener en cuenta al decidir si se debe confiar en la clave anterior son los siguientes:

- La conexión a Internet que has utilizado para obtener la clave GPG de este sitio web es segura.
- El dispositivo desde el que accedes a este sitio web es seguro.
- AWS ha tomado medidas para garantizar el alojamiento de la clave 0penPGP pública en este sitio web.

3. Si decide confiar en la OpenPGP clave, edítela de forma gpg similar a como se muestra en el ejemplo siguiente:

```
$ 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. Verifica el instalador

   Para verificar el instalador, complete los siguientes pasos:

   a. Regrese a la página de descargas de la consola de Deadline Cloud y descargue el archivo de firma del instalador del remitente de Deadline Cloud.

   b. Verifica la firma del instalador del remitente de Deadline Cloud ejecutando:

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

5. Verifica el monitor de Deadline Cloud

   > **Note**
   >
   > Puede verificar la descarga del monitor Deadline Cloud mediante archivos de firmas o métodos específicos de la plataforma. Para conocer los métodos específicos de la plataforma, consulta la Linux (DEB) Linux (AppImage) pestaña o la pestaña según el tipo de archivo descargado.

   Para verificar la aplicación de escritorio Deadline Cloud Monitor con los archivos de firma, complete los siguientes pasos:

   a. Regrese a la página de descargas de la consola Deadline Cloud, descargue el archivo.sig correspondiente y, a continuación, ejecute

   Para .deb:

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

   Para. AppImage:

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

b. Confirme que el resultado es similar al siguiente:

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

gpg: using RSA key B840C08C29A90796A071FAA5F6CD3CE6B7
```

Si el resultado contiene la fraseGood `signature from "AWS Deadline Cloud"`, significa que la firma se ha verificado correctamente y que puede ejecutar el script de instalación del monitor Deadline Cloud.

Linux (DEB)

Para verificar los paquetes que utilizan un archivo binario Linux .deb, primero complete los pasos 1 a 3 de la Linux pestaña.

dpkg es la herramienta principal de administración de paquetes en la mayoría debian de las distribuciones basadas. Linux Puede verificar el archivo.deb con la herramienta.

1. Desde la página de descargas de la consola Deadline Cloud, descargue el archivo .deb del monitor de Deadline Cloud.
2. ***<APP_VERSION>***Sustitúyalo por la versión del archivo.deb que desee verificar.

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

3. El resultado será similar al siguiente:

```
Processing deadline-cloud-monitor_1.1.1_amd64.deb... GOODSIG
_gpgbuilder B840C08C29A90796A071FAA5F6CD3C 171200
```

4. Para verificar el archivo.deb, confirme que `GOODSIG` esté presente en la salida.

Linux (AppImage)

Para verificar los paquetes que utilizan un. Linux AppImage binario, primero complete los pasos 1 a 3 de la Linux pestaña.

1. Desde la página de descargas de la consola Deadline Cloud, descarga el monitor de Deadline Cloud. AppImage archivo.
2. Para <APP_VERSION>reemplazarlo por la versión de. AppImage archivo que desee comprobar, complete los siguientes pasos:

   a. Escribe la firma del. AppImage en un archivo.sig.

   ```
   ./deadline-cloud-monitor_<APP_VERSION>_amd64.AppImage
   --appimage-signature > ./deadline-cloud-
   monitor_<APP_VERSION>_amd64_.AppImage.sig
   ```

   b. Utilice el archivo.sig generado para realizar la verificación mediante el siguiente comando.

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

   c. (Opcional) Si aparece un error de permiso denegado, utilice el siguiente comando para añadir el permiso de ejecución.

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

   d. Confirme que el resultado tiene un aspecto similar al siguiente:

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

   gpg: using RSA key B840C08C29A90796A071FAA5F6CD3CE6B7
   ```

   Si el resultado contiene la fraseGood `signature from "AWS Deadline Cloud"`, significa que la firma se ha verificado correctamente y que puede ejecutar el script de instalación del monitor Deadline Cloud.

Instala el remitente de Deadline Cloud

Puedes instalar un remitente de Deadline Cloud con Windows o. Linux Con el instalador, puede instalar los siguientes remitentes:

- Maya 2024
- Nuke 14.0 - 15.0
- Houdini 19.5

- Keyshot 12
- Licuadora 3.6
- Unreal Engine 5

Windows

1. En un explorador de archivos, navegue hasta la carpeta en la que se descargó el instalador y, a continuación, seleccione`DeadlineCloudSubmitter-windows-x64-installer.exe`.

    a. Si aparece una ventana emergente de Windows que protegió tu PC, selecciona Más información.

    b. Selecciona Ejecutar de todos modos.
2. Cuando se abra el asistente de configuración de AWS Deadline Cloud Submitter, seleccione Siguiente.
3. Elija el alcance de la instalación siguiendo uno de los siguientes pasos:
    - Para realizar la instalación solo para el usuario actual, seleccione Usuario.
    - Para realizar la instalación para todos los usuarios, elija Sistema.

      Si elige Sistema, debe salir del instalador y volver a ejecutarlo como administrador siguiendo estos pasos:

        a. Haga clic con el botón derecho en él y**`DeadlineCloudSubmitter-windows-x64-installer.exe`**, a continuación, seleccione Ejecutar como administrador.

        b. Introduzca sus credenciales de administrador y, a continuación, seleccione Sí.

        c. Elija Sistema para el alcance de la instalación.
4. Tras seleccionar el alcance de la instalación, seleccione Siguiente.
5. Vuelva a pulsar Siguiente para aceptar el directorio de instalación.
6. Seleccione el remitente integrado o el remitente que desee instalar. Nuke
7. Elija Siguiente.
8. Revise la instalación y seleccione Siguiente.
9. Vuelva a seleccionar Siguiente y, a continuación, seleccione Finalizar.

Linux

> **Note**
>
> El Nuke instalador integrado de Deadline Cloud Linux y el monitor de Deadline Cloud solo se pueden instalar en Linux distribuciones con al menos GLIBC 2.31.

1. Abra una ventana de terminal.
2. Para realizar una instalación del instalador desde el sistema, introduzca el comando **`sudo -i`** y pulse Entrar para convertirse en usuario root.
3. Navegue hasta la ubicación en la que descargó el instalador.

   Por ejemplo, **`cd /home/USER/Downloads`**.
4. Para hacer que el instalador sea ejecutable, introduzca**`chmod +x DeadlineCloudSubmitter-linux-x64-installer.run`**.
5. Para ejecutar el instalador Deadline Cloud Submitter, introduzca**`./DeadlineCloudSubmitter-linux-x64-installer.run`**.
6. Cuando se abra el instalador, siga las instrucciones que aparecen en la pantalla para completar el asistente de configuración.

Puede instalar otros remitentes que no aparecen en esta lista. Usamos las bibliotecas de Deadline Cloud para crear remitentes. Puede encontrar el código fuente de estas bibliotecas y de los remitentes en la organización GitHubaws-Deadline.

Paso 2: Instale y configure Deadline Cloud monitor

Puede instalar la aplicación de escritorio Deadline Cloud Monitor con Windows oLinux.

Windows

1. Si aún no lo has hecho, inicia sesión en la consola de Deadline Cloud AWS Management Console y ábrela.
2. En el panel de navegación izquierdo, selecciona Descargas.
3. En la sección Monitor de Deadline Cloud, selecciona el archivo para el sistema operativo de tu ordenador.
4. Para descargar el monitor de Deadline Cloud, selecciona Descargar.

Linux

Para instalar el monitor Deadline Cloud AppImage en distribuciones RPM

1. Descarga la última versión del monitor AppImage de Deadline Cloud.
2. Para crear el AppImage ejecutable, introduzca**`chmod a+x deadline-cloud-monitor_<APP_VERSION>_amd64.AppImage`**.
3. Para configurar la ruta correcta del certificado SSL, introduzca**`sudo ln -sf /etc/ssl/certs/ca-bundle.crt /etc/ssl/certs/ca-certificates.crt`**.

Para instalar el monitor Deadline Cloud en las AppImage distribuciones de Debian

1. Descarga la última versión del monitor de Deadline Cloud. AppImage
2.
> **Note**
>
> Este paso es para Ubuntu 22 y versiones posteriores. Para otras versiones de Ubuntu, omite este paso.

   Para instalar libfuse2, introduzca **`sudo apt udpate`**

   `sudo apt install libfuse2`.
3. Para crear el AppImage ejecutable, introduzca. **`chmod a+x deadline-cloud-monitor_<APP_VERSION>_amd64.AppImage`**

Para instalar el paquete Debian de Deadline Cloud monitorea en las distribuciones de Debian

1. Descargue el paquete Debian más reciente de Deadline Cloud para monitorizar.
2.
> **Note**
>
> Este paso es para Ubuntu 22 y versiones posteriores. Para otras versiones de Ubuntu, omite este paso.

   Para instalar libssl1.1, introduzca **`wget http://nz2.archive.ubuntu.com/ubuntu/pool/main/o/openssl/libssl1.<APP_VERSION>.1f-1ubuntu2.22_amd64.deb`**

sudo dpkg -i libssl1.*<APP_VERSION>*.1f-1ubuntu2.22_amd64.deb.

3. Para instalar el paquete Debian para monitorear Deadline Cloud, introduzca **sudo apt update**

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

4. Si la instalación falla en paquetes que tienen dependencias insatisfechas, corrija los paquetes dañados y ejecuta los siguientes comandos.

   sudo apt --fix-missing update

   sudo apt update

   sudo apt install -f

Una vez finalizada la descarga, puede comprobar la autenticidad del software descargado. Consulte Verificar la autenticidad del software descargado en el paso 1.

Tras descargar el monitor de Deadline Cloud y comprobar la autenticidad, utilice el siguiente procedimiento para configurar el monitor de Deadline Cloud.

Para configurar el monitor de Deadline Cloud

1. Abre el monitor de Deadline Cloud.
2. Cuando se le pida que cree un nuevo perfil, complete los siguientes pasos.

   a. Introduzca la URL de su monitor en la entrada URL, que tiene el siguiente aspecto **https://*MY-MONITOR*.deadlinecloud.amazonaws.com/**

   b. Introduzca un nombre de perfil.

   c. Seleccione Crear perfil.

      Se ha creado su perfil y sus credenciales ahora se comparten con cualquier software que utilice el nombre de perfil que creó.

3. Después de crear el perfil de monitor de Deadline Cloud, no podrás cambiar el nombre del perfil ni la URL del estudio. Si necesitas hacer cambios, haz lo siguiente en su lugar:

   a. Elimine el perfil. En el panel de navegación izquierdo, selecciona Deadline Cloud monitor, Settings y Delete.

b. Cree un perfil nuevo con los cambios que desee.

4. En el panel de navegación izquierdo, usa la opción >Deadline Cloud monitor para hacer lo siguiente:

   - Cambia el perfil del monitor de Deadline Cloud para iniciar sesión en otro monitor.
   - Activa el inicio de sesión automático para no tener que introducir la URL de tu monitor en las siguientes aperturas del monitor de Deadline Cloud.

5. Cierre la ventana del monitor de Deadline Cloud. Sigue ejecutándose en segundo plano y sincroniza tus credenciales cada 15 minutos.
6. Para cada aplicación de creación de contenido digital (DCC) que vaya a utilizar en sus proyectos de renderizado, siga estos pasos:

   a. Desde el remitente de Deadline Cloud, abra la configuración de la estación de trabajo de Deadline Cloud.
   b. En la configuración de la estación de trabajo, seleccione el perfil que creó en el monitor de Deadline Cloud. Sus credenciales de Deadline Cloud ahora se comparten con este DCC y sus herramientas deberían funcionar como se espera.

Paso 3: Inicie el remitente de Deadline Cloud

Las siguientes secciones lo guían por los pasos para lanzar el complemento de presentación de Deadline Cloud enBlender,Nuke, Maya y. Houdini

Para lanzar el remitente de Deadline Cloud en Blender

> **Note**
>
> Support for Blender se proporciona mediante el Conda entorno de flotas gestionadas por el servicio. Para obtener más información, consulte Entorno de Conda colas predeterminado.

1. Abra Blender.
2. Abra una Blender escena con las dependencias que existen en el directorio raíz de los activos.
3. En el menú Render, seleccione el cuadro de diálogo Deadline Cloud.

   a. Si aún no se ha autenticado en el remitente de Deadline Cloud, el estado de las credenciales muestra NEEDS_LOGIN.

b. Seleccione Iniciar sesión.

c. Aparece una ventana del navegador de inicio de sesión. Inicie sesión con sus credenciales de usuario.

d. Elija Permitir. Ya ha iniciado sesión y el estado de las credenciales aparecerá como AUTENTICADO.

4. Seleccione Submit (Enviar).

Para iniciar el remitente de Deadline Cloud en Foundry Nuke

> **Note**
>
> Support for Nuke se proporciona mediante el Conda entorno de flotas gestionadas por el servicio. Para obtener más información, consulte Entorno de Conda colas predeterminado.

1. Abra Nuke.
2. Abra un Nuke script con las dependencias que existen en el directorio raíz de los activos.
3. Selecciona Thinkbox y, a continuación, selecciona Enviar a Deadline Cloud para iniciar el remitente.

   a. Si aún no te has autenticado en el remitente de Deadline Cloud, el estado de las credenciales aparecerá como NEEDS_LOGIN.

   b. Seleccione Iniciar sesión.

   c. En la ventana del navegador de inicio de sesión, inicie sesión con sus credenciales de usuario.

   d. Elija Permitir. Ya ha iniciado sesión y el estado de las credenciales aparecerá como AUTENTICADO.

4. Seleccione Submit (Enviar).

Para iniciar el remitente de Deadline Cloud en Maya

> **Note**
>
> Support Maya y Arnold for Maya(MtoA) se proporciona mediante el Conda entorno para flotas gestionadas por servicios. Para obtener más información, consulte Entorno de Conda colas predeterminado.

1. Abra Maya.
2. Configure su proyecto y abra un archivo que se encuentre en el directorio raíz de los activos.
3. Elija Windows → Configuración/Preferencias → Administrador de complementos.
4. Busque Submitter. DeadlineCloud
5. Para cargar el complemento de envío de Deadline Cloud, selecciona Cargado.
    a. Si aún no te has autenticado en el remitente de Deadline Cloud, el estado de las credenciales aparecerá como NEEDS_LOGIN.
    b. Seleccione Iniciar sesión.
    c. Aparece una ventana del navegador de inicio de sesión. Inicie sesión con sus credenciales de usuario.
    d. Elija Permitir. Ahora ha iniciado sesión y el estado de las credenciales aparece como AUTENTICADO.
6. (Opcional) Para cargar el complemento de envío de Deadline Cloud cada vez que lo abrasMaya, selecciona Cargar automáticamente.
7. Selecciona la estantería Deadline Cloud y, a continuación, selecciona el botón verde para iniciar el remitente.

Para iniciar el remitente de Deadline Cloud en Houdini

> **Note**
>
> Support for Houdini se proporciona mediante el Conda entorno de flotas gestionadas por el servicio. Para obtener más información, consulte Entorno de Conda colas predeterminado.

1. Abra Houdini.

2. En el editor de red, seleccione /out network.
3. Pulse la tecla Tab y entre**deadline**.
4. Selecciona la opción Deadline Cloud y conéctala a tu red actual.
5. Haga doble clic en el nodo Deadline Cloud.

Para iniciar el remitente de Deadline Cloud en KeyShot

Esto supone que ya has descargado Deadline Cloud y PySide 2.

1. Copie o vincule el archivo Deadline-cloud-for-keyshot/keyshot_script/submit to AWS Deadline Cloud.py a la carpeta de scripts. KeyShot

   Por ejemploWindows, en, la ubicación de la carpeta de scripts sería. **C:/Users/*USER*/Documents/KeyShot 12/Scripts**
2. Establezca las siguientes variables de entorno.

   a. Establezca la variable de entorno **DEADLINE_PYTHON** como la ruta a la instalación de Python donde se encuentran deadline-cloud y PySide 2.

      Por ejemploWindows, si usa Python 3.10, el comando podría ser**set DEADLINE_PYTHON=C:/Users/*USER*/AppData/Local/Programs/Python/Python310/python**.

   b. Establezca la variable de entorno **DEADLINE_KEYSHOT** como la ruta a la carpeta keyshot_submitter.

      Por ejemplo, si la fuente está en el escritorioWindows, el comando podría estar activado. **set DEADLINE_KEYSHOT=C:/Users/*USER*/Desktop/deadline-cloud-for-keyshot/src/deadline/keyshot_submitter**
3. Con las variables de entorno configuradas, inicie KeyShot.
4. Para iniciar el remitente KeyShot, seleccione Scripting console Windows, Submit to AWS Deadline Cloud y Ejecutar.

Para lanzar el remitente de Deadline Cloud en Unreal Engine

Esto supone que ya has descargado Deadline Cloud.

1. Crea o abre la carpeta que utilizas para tus Unreal Engine proyectos.

2. Abre la línea de comandos y ejecuta los siguientes comandos:

   - `git clone https://github.com/aws-deadline/deadline-cloud-for-unreal-engine`
   - `cd deadline-cloud-for-unreal/test_projects`
   - `git lfs fetch –all`
3. Para descargar el complementoUnreal Engine, abra la carpeta Unreal Engine del proyecto e inicie deadline-cloud-forunreal/test_projects/pull_ue_plugin.bat.

   Esto coloca los archivos del plugin en C:// LocalProjectsUnrealDeadlineCloudTestUnrealDeadlineCloudService/Plugins/.
4. Para descargar el remitente, abra la carpeta y ejecútelo. UnrealDeadlineCloudService **`deadline-cloud-forunreal/ test_projects/Plugins/ UnrealDeadlineCloudService/install_unreal_submitter.bat`**
5. Para iniciar el remitente desdeUnreal Engine, complete los siguientes pasos:

   a. Seleccione Edición > Configuración del proyecto.

   b. En la barra de búsqueda, ingrese **`movie render pipeline`**.

   c. Ajusta los siguientes ajustes de Movie Render Pipeline:

      i. Para Default Remote Executor, introduzca**`MoviePipelineDeadlineCloudRemote Executor`**.

      ii. En Default Executor Job, introduzca **`MoviePipelineDeadlineCloudExecutorJob`**

      iii. Para las clases de configuración de trabajo predeterminadas, elija el signo más y, a continuación, introduzca**`DeadlineCloudRenderStepSetting`**.

   Con estos ajustes, puedes elegir el plugin Deadline Cloud entreUnreal Engine.

Usa la granja

Si ha seguido todas las instrucciones de introducción, ha configurado todo lo necesario para empezar a enviar los trabajos desde su estación de trabajo local a su granja y, a continuación, supervisar esos trabajos y recursos. Para obtener más información sobre cómo enviar todo tipo de trabajos o supervisarlos, consulte los temas relacionados que aparecen a continuación.

- Trabajos

- Uso del monitor

Uso del monitor Deadline Cloud

El monitor AWS Deadline Cloud le proporciona una visión general de sus trabajos de computación visual. Puede usarlo para monitorear y administrar los trabajos, ver la actividad de los trabajadores en las flotas, realizar un seguimiento de los presupuestos y el uso, y descargar los resultados de un trabajo.

Cada cola tiene un monitor de trabajos que muestra el estado de los trabajos, los pasos y las tareas. El monitor proporciona formas de administrar los trabajos directamente desde el monitor. Puede realizar cambios de priorización, cancelar trabajos y volver a ponerlos en cola.

El monitor de Deadline Cloud tiene una tabla que muestra el estado resumido de un trabajo, o puedes seleccionar un trabajo para ver los registros de tareas detallados que ayudan a solucionar los problemas relacionados con un trabajo.

Puedes usar el monitor de Deadline Cloud para descargar los resultados a la ubicación de tu estación de trabajo que se especificó cuando se creó el trabajo.

El monitor Deadline Cloud también te ayuda a controlar el uso y gestionar los costes. Para obtener más información, consulte Administrar los presupuestos y el uso de Deadline Cloud.

Temas

- Comparte la URL del monitor de Deadline Cloud
- Abre el monitor de Deadline Cloud
- Consulta los detalles de las colas y la flota en Deadline Cloud
- Vea y gestione los trabajos, los pasos y las tareas en Deadline Cloud
- Vea los detalles del trabajo en Deadline Cloud
- Ver un paso en Deadline Cloud
- Ver una tarea en Deadline Cloud
- Vea los registros en Deadline Cloud
- Descarga el resultado final en Deadline Cloud

Comparte la URL del monitor de Deadline Cloud

Cuando configuras el servicio Deadline Cloud, de forma predeterminada creas una URL que abre el monitor de Deadline Cloud de tu cuenta. Usa esta URL para abrir el monitor en tu navegador o en

tu escritorio. Comparta la URL con otros usuarios para que puedan acceder al monitor de Deadline Cloud.

Antes de que un usuario pueda abrir el monitor de Deadline Cloud, debes concederle acceso. Para conceder el acceso, añada el usuario a la lista de usuarios autorizados del monitor o agréguelo a un grupo con acceso al monitor. Para obtener más información, consulte Administrar usuarios en Deadline Cloud.

Para compartir la URL del monitor

1. Abre la consola de Deadline Cloud.
2. En Comenzar, selecciona Ir al panel de Deadline Cloud.
3. En el panel de navegación, elija Panel.
4. En la sección Resumen de la cuenta, selecciona Detalles de la cuenta.
5. Copia la URL y envíala de forma segura a cualquier persona que necesite acceder al monitor de Deadline Cloud.

Abre el monitor de Deadline Cloud

Puedes abrir el monitor de Deadline Cloud de cualquiera de las siguientes maneras:

- Consola: inicia sesión en la consola de Deadline Cloud AWS Management Console y ábrela.
- Web: ve a la URL del monitor que creaste al configurar Deadline Cloud.
- Supervisar: utilice el monitor de escritorio de Deadline Cloud.

Al utilizar la consola, debe poder iniciar sesión AWS con una AWS Identity and Access Management identidad y, a continuación, iniciar sesión en el monitor con AWS IAM Identity Center las credenciales. Si solo tiene las credenciales del IAM Identity Center, debe iniciar sesión con la URL del monitor o la aplicación de escritorio.

Para abrir el monitor de Deadline Cloud (web)

1. Con un navegador, abre la URL del monitor que creaste al configurar Deadline Cloud.
2. Inicia sesión con tus credenciales de usuario.

Para abrir el monitor de Deadline Cloud (consola)

1. Abre la consola de Deadline Cloud.
2. En el panel de navegación, selecciona Granjas.
3. Seleccione una granja y, a continuación, elija Administrar trabajos para abrir la página de monitoreo de Deadline Cloud.
4. Inicia sesión con tus credenciales de usuario.

Para abrir el monitor de Deadline Cloud (escritorio)

1. Abre la consola de Deadline Cloud.

   -o bien-

   Abre el monitor web de Deadline Cloud desde la URL del monitor.
2. • En la consola de Deadline Cloud, haga lo siguiente:
     1. En el monitor, selecciona Ir al panel de Deadline Cloud y, a continuación, selecciona Descargas en el menú de la izquierda.
     2. En el monitor de Deadline Cloud, elige la versión de monitor para tu escritorio.
     3. Elija Descargar.
   • En el monitor web de Deadline Cloud, haga lo siguiente:
     • En el menú de la izquierda, selecciona Configuración de estación de trabajo. Si el elemento de configuración de la estación de trabajo no está visible, usa la flecha para abrir el menú de la izquierda.
     • Elija Descargar.
     • En Seleccione un sistema operativo, elija su sistema operativo.
3. Descarga el monitor Deadline Cloud para escritorio.
4. Después de descargar e instalar el monitor, ábralo en su computadora.

   • Si es la primera vez que abre el monitor de Deadline Cloud, debe proporcionar la URL del monitor y crear un nombre de perfil. A continuación, inicia sesión en el monitor con tus credenciales de Deadline Cloud.
   • Después de crear un perfil, abra el monitor seleccionando un perfil. Puede que tengas que introducir tus credenciales de Deadline Cloud.

Consulta los detalles de las colas y la flota en Deadline Cloud

Puedes usar el monitor de Deadline Cloud para ver la configuración de las colas y las flotas de tu granja. También puede usar el monitor para ver una lista de los trabajos en cola o de los trabajadores de una flota.

Debe tener `VIEWING` permiso para ver los detalles de las colas y la flota. Si no aparecen los detalles, ponte en contacto con tu administrador para obtener los permisos correctos.

Para ver los detalles de la cola

1. Abre el monitor de Deadline Cloud.
2. En la lista de granjas, elija la granja que contenga la cola que le interese.
3. En la lista de colas, elija una cola para mostrar sus detalles. Para comparar la configuración de dos o más colas, active más de una casilla de verificación.
4. Para ver una lista de los trabajos de la cola, elija el nombre de la cola en la lista de colas o en el panel de detalles.

Si el monitor ya está abierto, puede seleccionar la cola en la lista de colas del panel de navegación izquierdo.

Ver los detalles de la flota

1. Abre el monitor de Deadline Cloud.
2. En la lista de granjas, elija la granja que contenga la flota que le interese.
3. En Recursos agrícolas, selecciona Flotas.
4. En la lista de flotas, selecciona una flota para ver sus detalles. Para comparar la configuración de dos o más flotas, seleccione más de una casilla de verificación.
5. Para ver una lista de los trabajadores de la flota, elija el nombre de la flota en la lista de flotas o en el panel de detalles.

Si el monitor ya está abierto, puede seleccionar la flota en la lista de flotas del panel de navegación izquierdo.

Vea y gestione los trabajos, los pasos y las tareas en Deadline Cloud

Cuando seleccionas una cola, la sección de supervisión de trabajos del monitor de Deadline Cloud te muestra los trabajos de esa cola, los pasos del trabajo y las tareas de cada paso. Cuando seleccionas un trabajo, un paso o una tarea, puedes usar el menú Acciones para gestionar cada uno de ellos.

Para abrir el monitor de trabajos, siga los pasos para ver una cola y, a continuaciónConsulta los detalles de las colas y la flota en Deadline Cloud, seleccione el trabajo, el paso o la tarea con los que desea trabajar.

Para los trabajos, los pasos y las tareas, puede hacer lo siguiente:

- Cambie el estado a Se ha vuelto a poner en cola, se ha realizado correctamente, ha fallado o se ha cancelado.
- Descargue el resultado procesado del trabajo, paso o tarea.
- Copie el ID del trabajo, paso o tarea.

Para el trabajo seleccionado, puede:

- Archivar el trabajo.
- Modifique las propiedades del trabajo, por ejemplo, cambiando la priorización o viendo las dependencias paso a paso.
- Vea detalles adicionales mediante los parámetros del trabajo.

Para obtener más información, consulte Vea los detalles del trabajo en Deadline Cloud.

Para cada paso, puede:

- Ver las dependencias del paso. Las dependencias de un paso deben completarse antes de que se ejecute el paso.

Para obtener más detalles, consulte Ver un paso en Deadline Cloud.

Para cada tarea, puede:

- Ver los registros de la tarea.
- Ver los parámetros de la tarea.

Para obtener más información, consulte Ver una tarea en Deadline Cloud.

Vea los detalles del trabajo en Deadline Cloud

La página de supervisión de trabajos del monitor de Deadline Cloud le proporciona lo siguiente:

- Una visión general del progreso de un trabajo.
- Una vista de los pasos y las tareas que componen el trabajo.

Seleccione un trabajo de la lista para ver una lista de los pasos del trabajo y, a continuación, elija un paso de la lista de pasos para ver las tareas del trabajo. Después de elegir un elemento, puede usar el menú Acciones de ese elemento para ver los detalles.

Para ver los detalles del trabajo

1. Siga los pasos para ver una cola enConsulta los detalles de las colas y la flota en Deadline Cloud.
2. En el panel de navegación, selecciona la cola a la que enviaste tu trabajo.
3. Seleccione un trabajo mediante uno de los siguientes métodos:

    a. En la lista de trabajos, seleccione un trabajo para ver sus detalles.

    b. En el campo de búsqueda, introduzca cualquier texto asociado al trabajo, como el nombre del trabajo o el usuario que lo creó. En los resultados que aparecen, seleccione el trabajo que desee ver.

Los detalles de un trabajo incluyen los pasos del trabajo y las tareas de cada paso. Puede utilizar el menú Acciones para hacer lo siguiente:

- Cambie el estado del trabajo.
- Vea y modifique las propiedades de un trabajo. Puede ver las dependencias entre los pasos del trabajo y cambiar la prioridad del trabajo. Por lo general, los trabajos con una prioridad más alta se completan antes.
- Vea los parámetros del trabajo que se establecieron cuando se envió el trabajo.

- Descarga el resultado de un trabajo. Al descargar el resultado de un trabajo, contiene todo el resultado generado por los pasos y las tareas del trabajo.

Ver un paso en Deadline Cloud

Usa el monitor de AWS Deadline Cloud para ver los pasos de tus trabajos de procesamiento. En el monitor de tareas, la lista de pasos muestra la lista de pasos que componen el trabajo seleccionado. Al seleccionar un paso, la lista de tareas muestra las tareas del paso.

Para ver un paso

1. Siga los pasos que se indican Vea los detalles del trabajo en Deadline Cloud para ver una lista de trabajos.
2. Seleccione un trabajo en la lista Jobs (Trabajos).
3. Seleccione un paso de la lista de pasos.

Puede utilizar el menú Acciones para hacer lo siguiente:

- Cambie el estado del paso.
- Descarga el resultado del paso. Al descargar el resultado de un paso, contiene todo el resultado generado por las tareas del paso.
- Vea las dependencias de un paso. La tabla de dependencias muestra una lista de los pasos que deben completarse antes de que comience el paso seleccionado y una lista de los pasos que están esperando a que se complete este paso.

Ver una tarea en Deadline Cloud

Usa el monitor de AWS Deadline Cloud para ver las tareas de tus trabajos de procesamiento. En el monitor de tareas, la lista de tareas muestra las tareas que componen el paso seleccionado en la lista de pasos.

Para ver una tarea

1. Siga los pasos que se indican Vea los detalles del trabajo en Deadline Cloud para ver una lista de trabajos.
2. Seleccione un trabajo en la lista Jobs (Trabajos).

3. Seleccione un paso de la lista de pasos.
4. Seleccione una tarea de la lista de tareas.

Puede utilizar el menú Acciones para hacer lo siguiente:

- Cambie el estado de la tarea.
- Ver los registros de tareas. Para obtener más información, consulte Vea los registros en Deadline Cloud.
- Vea los parámetros que se establecieron cuando se creó la tarea.
- Descarga el resultado de la tarea. Al descargar el resultado de una tarea, solo contiene el resultado generado por la tarea seleccionada.

Vea los registros en Deadline Cloud

Los registros te proporcionan información detallada sobre el estado y el procesamiento de las tareas. En el monitor de AWS Deadline Cloud, puede ver los dos tipos de registros siguientes:

- Los registros de sesión detallan el cronograma de las acciones, que incluyen:
  - Acciones de configuración, como la sincronización de los archivos adjuntos y la carga del entorno de software
  - Ejecutar una tarea o un conjunto de tareas
  - Acciones de cierre, como cerrar el entorno de un trabajador

  Una sesión incluye el procesamiento de al menos una tarea y puede incluir varias tareas. Los registros de sesión también muestran información sobre el tipo de instancia, la vCPU y la memoria de Amazon Elastic Compute Cloud (Amazon EC2). Los registros de sesión también incluyen un enlace al registro del trabajador utilizado en la sesión.
- Los registros de los trabajadores proporcionan detalles del cronograma de las acciones que un trabajador procesa durante su ciclo de vida. Los registros de los trabajadores pueden contener información sobre varias sesiones.

Puede descargar los registros de sesión y de trabajo para examinarlos sin conexión.

Para ver los registros de las sesiones

1. Siga los pasos que se indican Vea los detalles del trabajo en Deadline Cloud para ver una lista de trabajos.
2. Seleccione un trabajo en la lista Jobs (Trabajos).
3. Seleccione un paso de la lista de pasos.
4. Seleccione una tarea de la lista de tareas.
5. En el menú Acciones, selecciona Ver registros.

La sección Cronogramas muestra un resumen de las acciones de la tarea. Para ver más tareas ejecutadas en la sesión y ver las acciones de cierre de la sesión, seleccione Ver los registros de todas las tareas.

Para ver los registros de los trabajadores de una tarea

1. Siga los pasos que se indican Vea los detalles del trabajo en Deadline Cloud para ver una lista de trabajos.
2. Seleccione un trabajo en la lista Jobs (Trabajos).
3. Seleccione un paso de la lista de pasos.
4. Seleccione una tarea de la lista de tareas.
5. En el menú Acciones, selecciona Ver registros.
6. Selecciona Información de sesión.
7. Selecciona Ver registro de trabajadores.

Para ver los registros de los trabajadores a partir de los detalles de la flota

1. Siga los pasos Consulta los detalles de las colas y la flota en Deadline Cloud que se indican para ver una flota.
2. Seleccione un identificador de trabajador de la lista de trabajadores.
3. En el menú Acciones, selecciona Ver los registros de los trabajadores.

Descarga el resultado final en Deadline Cloud

Una vez finalizado un trabajo, puedes usar el monitor de AWS Deadline Cloud para descargar los resultados a tu estación de trabajo. El archivo de salida se guarda con el nombre y la ubicación que especificó al crear el trabajo.

Los archivos de salida se almacenan indefinidamente. Para reducir los costes de almacenamiento, considere la posibilidad de crear una configuración de S3 Lifecycle para el bucket de Amazon S3 de su cola. Para obtener más información, consulte Administrar el ciclo de vida de almacenamiento en la Guía del usuario de Amazon Simple Storage Service.

Para descargar el resultado final de un trabajo, paso o tarea

1. Siga los pasos que se indican Vea los detalles del trabajo en Deadline Cloud para ver una lista de trabajos.
2. Seleccione el trabajo, el paso o la tarea cuyos resultados desee descargar.
   - Si selecciona un trabajo, puede descargar todos los resultados de todas las tareas de todos los pasos de ese trabajo.
   - Si selecciona un paso, puede descargar todos los resultados de todas las tareas de ese paso.
   - Si selecciona una tarea, puede descargar el resultado de esa tarea individual.
3. En el menú Acciones, selecciona Descargar la salida.
4. El resultado se descargará en la ubicación establecida cuando se envió el trabajo.

> **Note**
>
> Actualmente, la descarga de resultados mediante el menú solo se admite para Windows yLinux. Si tiene un elemento de menú Descargar resultados Mac y elige el elemento de menú Descargar resultados, aparecerá una ventana con el AWS CLI comando que puede utilizar para descargar el resultado renderizado.

Granjas Deadline Cloud

Una granja es un contenedor de colas que administran trabajos y flotas de recursos informáticos que realizan tareas.

Temas

- Cree una granja
- Eliminar una granja
- Edite una granja

Cree una granja

1. En la consola de Deadline Cloud, selecciona Ir al panel de control.
2. En la sección Granjas del panel de Deadline Cloud, selecciona Acciones → Crear granja.
    - Como alternativa, en el panel lateral izquierdo, selecciona Granjas y otros recursos y, a continuación, selecciona Crear granja.
3. Añade un nombre a tu granja.
4. En Descripción, introduzca la descripción de la granja. Una descripción clara puede ayudarle a identificar rápidamente el propósito de su granja.
5. (Opcional) De forma predeterminada, sus datos se cifran con una clave que le AWS pertenece y administra para su seguridad. Puede elegir Personalizar la configuración de cifrado (avanzada) para usar una clave existente o crear una nueva que administre.

    Si elige personalizar la configuración de cifrado mediante la casilla de verificación, introduzca un AWS KMS ARN o cree uno AWS KMS nuevo seleccionando Crear nueva clave KMS.
6. (Opcional) Seleccione Añadir nueva etiqueta para añadir una o más etiquetas a su granja.
7. Selecciona Crear granja. Tras la creación, aparecerá tu granja.

Eliminar una granja

1. En el panel de Deadline Cloud, selecciona Granjas y otros recursos.
2. En la lista de granjas, selecciona la granja o las granjas que deseas eliminar y, a continuación, selecciona Eliminar.

Edite una granja

1. En el panel de Deadline Cloud, selecciona Granjas y otros recursos.
2. En la lista de granjas, selecciona la granja o las granjas que deseas eliminar y, a continuación, selecciona Editar.
3. En la ventana de edición que aparece, cambie el nombre o la descripción de la granja y, a continuación, seleccione Guardar cambios.

Colas de Deadline Cloud

Una cola es un recurso de granja que administra y procesa los trabajos.

Para trabajar con colas, ya debe tener un monitor y una granja configurados.

Temas

- Creación de una cola
- Cree un entorno de colas
- Eliminar una cola
- Edición de una cola
- Asocia una cola y una flota

Creación de una cola

1. En el panel de la consola de Deadline Cloud, selecciona la granja para la que quieres crear una cola.

   - Como alternativa, en el panel lateral izquierdo, selecciona Granjas y otros recursos y, a continuación, selecciona la granja para la que quieres crear una cola.
2. En la pestaña Colas, selecciona Crear cola.
3. Introduce un nombre para la cola.
4. En Descripción, introduzca la descripción de la cola. Una descripción le ayuda a identificar el propósito de la cola.
5. Para los adjuntos de tareas, puede crear un nuevo bucket de Amazon S3 o elegir un bucket de Amazon S3 existente.

   a. Para crear un nuevo bucket de Amazon S3

      i. Seleccione Crear un nuevo grupo de trabajos.

      ii. Introduzca un nombre para el depósito. Te recomendamos ponerle un nombre al depósito`deadlinecloud-job-attachments-[MONITORNAME]`.

      iii. Introduce un prefijo raíz para definir o cambiar la ubicación raíz de la cola.

   b. Para elegir un bucket de Amazon S3 existente

i. Seleccione Elegir un bucket de S3 existente > Explorar S3.

ii. Seleccione el depósito de S3 para su cola en la lista de depósitos disponibles.

6. (Opcional) Para asociar la cola a una flota gestionada por el cliente, selecciona Habilitar la asociación con flotas gestionadas por el cliente.

7. Si habilita la asociación con flotas gestionadas por el cliente, debe completar los siguientes pasos.

> **Important**
>
> Recomendamos encarecidamente especificar los usuarios y grupos para la funcionalidad de ejecución automática. Si no lo hace, se degradará la seguridad de su granja, ya que los trabajadores pueden hacer todo lo que el agente del trabajador puede hacer. Para obtener más información sobre los posibles riesgos de seguridad, consulte Ejecutar trabajos como usuarios y grupos.

a. Para Ejecutar como usuario:

Para proporcionar las credenciales de los trabajos de la cola, seleccione Usuario configurado en cola.

O bien, para dejar de configurar sus propias credenciales y ejecutar los trabajos como usuario del agente de trabajo, seleccione el usuario del agente de trabajo.

b. (Opcional) En Ejecutar como credenciales de usuario, introduzca un nombre de usuario y un nombre de grupo para proporcionar las credenciales de los trabajos de la cola.

Si utiliza una Windows flota, debe crear un AWS Secrets Manager secreto que contenga la contraseña del usuario Ejecutar como usuario. Sigue estas instrucciones para crear el secreto. Sustituya *`jobuser`* por el nombre del`jobRunAsUser`.

i. Abra PowerShell o una línea de comandos como administrador.

ii. Cree el usuario.

```
net user jobuser /add
```

iii. Establezca la contraseña.

```
net user jobuser *
```

iv. Cree un perfil local y un directorio principal para el usuario. Ejecute el siguiente comando e introduzca la contraseña del usuario cuando se le solicite.

```
runas /profile /user:jobuser "cmd.exe /C"
```

8. Requerir un presupuesto ayuda a gestionar los costes de la cola. Seleccione No requerir un presupuesto o Exigir un presupuesto.
9. La cola necesita permiso para acceder a Amazon S3 en su nombre. Puede crear una nueva función de servicio o utilizar una función de servicio existente. Si no tienes un rol de servicio existente, crea y usa uno nuevo.

    a. Para usar un rol de servicio existente, selecciona Elegir un rol de servicio y, a continuación, selecciona un rol en el menú desplegable.

    b. Para crear un nuevo rol de servicio, selecciona Crear y usar un nuevo rol de servicio y, a continuación, ingresa el nombre y la descripción del rol.
10. (Opcional) Para agregar variables de entorno para el entorno de colas, elija Agregar nueva variable de entorno y, a continuación, escriba un nombre y un valor para cada variable que agregue.
11. (Opcional) Seleccione Añadir nueva etiqueta para añadir una o más etiquetas a la cola.
12. Para crear un entorno de Conda colas predeterminado, mantén la casilla de verificación seleccionada. Para obtener más información sobre los entornos de colas, consulte Crear un entorno de colas. Si va a crear una cola para una flota gestionada por el cliente, desactive la casilla de verificación.
13. Elija Crear cola.

Cree un entorno de colas

Un entorno de colas es un conjunto de variables de entorno y comandos que configuran a los trabajadores de una flota. Puede utilizar los entornos de colas para proporcionar aplicaciones de software, variables de entorno y otros recursos a los trabajos de la cola.

Al crear una cola, tiene la opción de crear un entorno de colas predeterminadoConda. Este entorno proporciona a las flotas gestionadas por servicios acceso a paquetes para aplicaciones y

renderizadores de DCC asociados. Para obtener más información, consulte Entorno de Conda colas predeterminado.

Puede añadir entornos de colas mediante la consola o editando directamente la plantilla json o YAML. Este procedimiento describe cómo crear un entorno con la consola.

1. Para añadir un entorno de colas a una cola, navegue hasta la cola y seleccione la pestaña Entornos de colas.
2. Seleccione Acciones y, a continuación, Crear una nueva con formulario.
3. Introduzca un nombre y una descripción para el entorno de colas.
4. Seleccione Añadir nueva variable de entorno y, a continuación, introduzca un nombre y un valor para cada variable que añada.
5. (Opcional) Introduzca una prioridad para el entorno de colas. La prioridad indica el orden en que se ejecutará este entorno de colas en el trabajador. Los entornos de colas de mayor prioridad se ejecutarán primero.
6. Seleccione Crear entorno de colas.

Entorno de Conda colas predeterminado

Al crear una cola asociada a una flota gestionada por un servicio, tiene la opción de añadir un entorno de colas predeterminado que permita descargar e instalar paquetes en un entorno virtual Condapara sus trabajos.

Condaproporciona paquetes de los canales. Un canal es un lugar donde se almacenan los paquetes. Deadline Cloud proporciona un canal que aloja paquetes compatibles con las aplicaciones y renderizadores de DCC de los socios. `deadline-cloud` Los paquetes son:

- Blender
  - `blender=3.6`
  - `blender-openjd`
- Houdini
  - `houdini=19.5`
  - `houdini-openjd`
- Maya
  - `maya=2024`

  - `maya-mtoa=2024.5.3`
  - `maya-openjd`
- Bomba nuclear
  - `nuke=15`
  - `nuke-openjd`

Al enviar un trabajo a una cola con el Conda entorno predeterminado, el entorno añade dos parámetros al trabajo. Estos parámetros especifican los Conda paquetes y los canales que se van a utilizar para configurar el entorno del trabajo antes de procesar las tareas. Los parámetros son:

- `CondaPackages`— una lista separada por espacios de las especificaciones de los paquetes que coinciden, como `blender=3.6` o. `numpy>1.22` El valor predeterminado está vacío para omitir la creación de un entorno virtual.
- `CondaChannels`— una lista de Condacanales separados por espacios`deadline-cloud`, como`conda-forge`, `os3://DOC-EXAMPLE-BUCKET/conda/channel`. El canal predeterminado es `deadline-cloud` un canal disponible para las flotas gestionadas por el servicio que proporciona aplicaciones de DCC y renderizadores asociados.

Cuando utilizas un remitente integrado para enviar un trabajo a Deadline Cloud desde tu DCC, el remitente rellena el valor del parámetro en función de la solicitud de DCC y del `CondaPackages` remitente. Por ejemplo, si utilizas Blender, el parámetro se establece en. `CondaPackage` `blender=3.6.* blender-openjd=0.4.*`

Eliminar una cola

> **Warning**
>
> No puedes recuperar los trabajos de una cola si la eliminas. Al eliminar la cola, también se eliminan los trabajos de esa cola.

1. En el panel de Deadline Cloud, selecciona Granjas y otros recursos.
2. En la lista de granjas, selecciona la granja que contiene la cola que deseas eliminar.
3. Seleccione la cola y, a continuación, elija Eliminar.

4. En la ventana de confirmación, elija Delete. Se eliminarán la cola y todos los trabajos de la cola.

Edición de una cola

1. En el panel de Deadline Cloud, selecciona Granjas y otros recursos.
2. En la lista de granjas, selecciona la granja que contiene la cola que deseas editar.
3. Seleccione la cola y, a continuación, elija Editar.
4. Puede editar el nombre, la descripción, las necesidades presupuestarias, la opción Ejecutar como usuario y el rol de servicio asignado. También puede asociar una flota existente a su cola.
5. Elija Guardar cambios.

Asocia una cola y una flota

1. Seleccione la cola que desee asociar a una flota.
2. Para seleccionar una flota y asociarla a tu cola, selecciona Asociar flotas.
3. Selecciona el menú desplegable Seleccionar flotas. Aparece una lista de las flotas disponibles.
4. En la lista de flotas disponibles, seleccione la casilla de verificación situada junto a la flota o las flotas que desee asociar a su cola.
5. Elija Asociar. El estado de la asociación de flotas ahora debería ser Asociada.

Gestione las flotas de Deadline Cloud

En esta sección, se explica cómo gestionar las flotas gestionadas por servicios (SMF) y las flotas gestionadas por los clientes (CMF) para Deadline Cloud.

Puedes configurar dos tipos de flotas de Deadline Cloud:

- Las flotas gestionadas por el servicio son flotas de trabajadores que tienen la configuración predeterminada proporcionada por este servicio, Deadline Cloud. Estos ajustes predeterminados están diseñados para ser eficientes y rentables.
- Las flotas gestionadas por el cliente (CMF) son flotas de trabajadores que usted administra. Una CMF puede residir en la AWS infraestructura, en las instalaciones o en un centro de datos compartido. Una CMF proporciona el control y la responsabilidad totales de la flota. Esto incluye el aprovisionamiento, las operaciones, la administración y el desmantelamiento de los trabajadores de la flota.

Temas

- Gestione las flotas gestionadas por el servicio Deadline Cloud
- Gestione las flotas gestionadas por los clientes de Deadline Cloud

Gestione las flotas gestionadas por el servicio Deadline Cloud

Las flotas gestionadas por servicios son flotas de trabajadores que tienen la configuración predeterminada proporcionada por Deadline Cloud. Estos ajustes predeterminados están diseñados para ser eficientes y rentables.

1. Para crear una flota gestionada por servicios (SMF), navegue hasta la granja en la que desee crear la flota.
2. Selecciona la pestaña Flotas.
3. Elija Create fleet (Crear flota).
4. Introduzca un nombre para su flota.
5. Escriba una descripción en Description. Una descripción clara puede ayudarle a identificar rápidamente el propósito de su flota.
6. Seleccione el tipo de flota gestionada por el servicio.

7. Elija la opción de mercado de instancias puntuales o bajo demanda para su flota. Las instancias puntuales son una capacidad sin reservas que puede utilizar a un precio reducido, pero las solicitudes bajo demanda pueden interrumpirlas. Las instancias bajo demanda tienen un precio por segundo, pero no tienen un compromiso a largo plazo y no se interrumpirán. De forma predeterminada, las flotas utilizan instancias puntuales.
8. Opcional: defina el número máximo de instancias para escalar la flota de modo que haya capacidad disponible para los trabajos de la cola. Le recomendamos que deje el número mínimo de instancias establecido **`0`** para garantizar que la flota libere todas las instancias cuando no haya ningún trabajo en cola.
9. Para acceder al servicio de su flota, seleccione un rol existente o cree uno nuevo. Un rol de servicio proporciona credenciales a las instancias de la flota, lo que les otorga permiso para procesar los trabajos, y a los usuarios del monitor, para que puedan leer la información de registro.
10. Elija Siguiente.
11. Introduzca las CPU virtuales mínimas y máximas que necesita para su flota.
12. Introduzca la memoria mínima y máxima que necesita para su flota.
13. Opcionalmente, puede optar por permitir o excluir tipos de instancias específicos de su flota para asegurarse de que solo esos tipos de instancias se usen en esta flota.
14. Opcional: puede especificar el tamaño del volumen gp3 de Amazon Elastic Block Store (Amazon EBS) que se adjuntará a los trabajadores de esta flota. Para obtener más información, consulte la guía del usuario de EBS.
15. Elija Siguiente.
16. Opcional: Defina requisitos de personal personalizados que definan las características de esta flota y que puedan combinarse con los requisitos de hospedaje personalizados que se especifican en las solicitudes de trabajo. Un ejemplo es un tipo de licencia concreto si planea conectar su flota a su propio servidor de licencias.
17. Elija Siguiente.
18. Opcional Para asociar su flota a una cola, seleccione una cola en el menú desplegable. Si la cola está configurada con el entorno de Conda colas predeterminado, su flota recibirá automáticamente paquetes compatibles con las aplicaciones y renderizadores de DCC de los socios. Para obtener una lista de los paquetes proporcionados, consulte. Entorno de Conda colas predeterminado
19. Elija Siguiente.

20. Opcional: para añadir una etiqueta a su flota, seleccione Añadir nueva etiqueta y, a continuación, introduzca la clave y el valor de esa etiqueta.
21. Elija Siguiente.
22. Revisa la configuración de tu flota y, a continuación, selecciona Crear flota. Tras la creación, aparecerá tu flota.

Compatibilidad con el VFX Reference Platform

VFX Reference PlatformEs una plataforma objetivo común para la industria de los efectos visuales. Para utilizar la instancia Amazon EC2 de flota gestionada por servicios estándar que ejecuta Amazon Linux 2023 con un software compatible con VFX Reference Platform la, debe tener en cuenta las siguientes consideraciones al utilizar una flota gestionada por servicios.

Se actualiza anualmente. VFX Reference Platform Estas consideraciones a la hora de utilizar una AL2023, incluidas las flotas gestionadas por el servicio Deadline Cloud, se basan en las plataformas de referencia del año natural (CY) de 2022 a 2024. Para obtener más información, consulte VFX Reference Platform.

> **Note**
>
> Si va a crear un custom Amazon Machine Image (AMI) para una flota gestionada por el cliente, puede añadir estos requisitos al preparar la instancia de Amazon EC2.

Para utilizar el software VFX Reference Platform compatible en una instancia Amazon EC2 AL2023, tenga en cuenta lo siguiente:

- La versión glibc instalada con el AL2023 es compatible para su uso en tiempo de ejecución, pero no para la creación de software compatible con el CY2024 o versiones anteriores. VFX Reference Platform
- Python 3.9 y 3.11 se proporcionan con la flota gestionada por el servicio, lo que la hace compatible con VFX Reference Platform CY2022 y CY2024. Python 3.7 y 3.10 no se proporcionan en la flota gestionada por el servicio. El software que los requiera debe proporcionar la instalación de Python en la cola o en el entorno de trabajo.
- Algunos componentes de la biblioteca Boost que se proporcionan en la flota de servicios gestionados son de la versión 1.75, que no es compatible con la. VFX Reference Platform Si

su aplicación usa Boost, debe proporcionar su propia versión de la biblioteca para garantizar la compatibilidad.

- La actualización 3 de Intel TBB se incluye en la flota de servicios gestionados. Es compatible con los modelos VFX Reference Platform CY2022, CY2023 y CY2024.
- La flota gestionada por el VFX Reference Platform servicio no proporciona otras bibliotecas con versiones especificadas en el. Debe proporcionar a la biblioteca cualquier aplicación que se utilice en una flota gestionada por un servicio. Para obtener una lista de bibliotecas, consulte la plataforma de referencia.

Gestione las flotas gestionadas por los clientes de Deadline Cloud

En esta sección se explica cómo gestionar una flota gestionada por el cliente (CMF) para Deadline Cloud.

Los CMF son flotas de trabajadores que usted administra. Una CMF puede residir en la AWS infraestructura, en las instalaciones o en un centro de datos compartido. Una CMF proporciona el control y la responsabilidad totales de la flota. Esto incluye el aprovisionamiento, las operaciones, la administración y el desmantelamiento de los trabajadores de la flota.

Temas

- Cree una flota gestionada por el cliente
- Instalación y configuración del host de trabajo
- Administre el acceso a los secretos de los usuarios de trabajos de Windows
- Instalar y configurar el software necesario para los trabajos
- Configuración de AWS credenciales
- Crear un Amazon Machine Image
- Cree una infraestructura de flota con un grupo de Auto Scaling de Amazon EC2
- Connect las flotas gestionadas por el cliente a un punto final de licencia

Cree una flota gestionada por el cliente

Para crear una flota gestionada por el cliente (CMF), complete los siguientes pasos.

Deadline Cloud console

Para usar la consola de Deadline Cloud para crear una flota gestionada por el cliente

1. Abre la consola de Deadline Cloud.
2. Selecciona Farms. Aparece una lista de las granjas disponibles.
3. Seleccione el nombre de la granja en la que desea trabajar.
4. Seleccione la pestaña Flotas.
5. Elija Create fleet (Crear flota).
6. Introduzca un nombre para su flota.
7. (Opcional) Introduzca una descripción para su flota.
8. Seleccione Gestionado por el cliente para el tipo de flota.
9. Seleccione un tipo de Auto Scaling. Para obtener más información, consulte Uso EventBridge para gestionar eventos de Auto Scaling.

   - Sin escalado: está creando una flota local y quiere excluirse de Deadline Cloud Auto Scaling.
   - Recomendaciones de escalado: está creando una flota de Amazon Elastic Compute Cloud (Amazon EC2).
10. Seleccione el acceso al servicio de su flota.

    a. Te recomendamos que utilices la opción Crear y usar una nueva función de servicio para cada flota para controlar los permisos de forma más pormenorizada. Esta opción está seleccionada de forma predeterminada.

    b. También puede usar un rol de servicio existente seleccionando Elegir un rol de servicio.
11. Revisa tus selecciones y, a continuación, selecciona Siguiente.
12. Seleccione un sistema operativo para su flota. Todos los trabajadores de una flota deben tener un sistema operativo común.
13. Seleccione la arquitectura de la CPU del host.
14. Seleccione los siguientes requisitos de hardware para los anfitriones de trabajadores de esta flota.

    a. Seleccione los requisitos mínimos y máximos de hardware de vCPU y memoria para satisfacer las demandas de carga de trabajo de sus flotas.

    b. (Opcional) Seleccione el requisito de GPU e introduzca las GPU mínimas y máximas.
15. Revisa tus selecciones y, a continuación, selecciona Siguiente.
16. (Opcional) Defina los requisitos de los trabajadores personalizados.
17. En el menú desplegable, seleccione una o más colas para asociarlas a la flota.

> **Note**
>
> Recomendamos asociar una flota únicamente a las colas que estén todas en el mismo límite de confianza. Esto garantiza un límite de seguridad sólido entre los trabajos que se ejecutan en el mismo trabajador.

18. Revise las asociaciones de colas y, a continuación, seleccione Siguiente.
19. (Opcional) Para el entorno de colas de Conda predeterminado, crearemos un entorno para su cola en el que se instalarán los paquetes de Conda solicitados por los trabajos.

> **Note**
>
> El entorno de colas de Conda se utiliza para instalar los paquetes de Conda solicitados por los trabajos. Por lo general, debe desmarcar el entorno de colas de Conda en las colas asociadas a los CMF, ya que los CMF no tendrán instalados los comandos de Conda necesarios de forma predeterminada.

20. (Opcional) Añada etiquetas a su CMF. Para obtener más información, consulte Etiquetar AWS los recursos.
21. Revise la configuración de su flota y realice los cambios que considere oportunos.
22. Elija Create fleet (Crear flota).
23. Selecciona la pestaña Flotas y, a continuación, anota el ID de la flota.

AWS CLI

Para utilizarla AWS CLI para crear una flota gestionada por el cliente

1. Abre el. AWS CLI
2. Editar `fleet-trust-policy.json`.

    a. Añada la siguiente política de IAM y sustituya el texto en *cursiva por* su ID de AWS cuenta y su ID de granja de Deadline Cloud.

```
{
    "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. Guarde los cambios.

3. Editar `create-cmf-fleet.json`.

a. Añada la siguiente política de IAM.

```
{
    "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. Guarde los cambios.

4. Añada una función de IAM para que la usen los trabajadores de su flota.

```
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. Editar `create-fleet-request.json`.

a. Añada la siguiente política de IAM y sustituya el texto en cursiva por los valores de su CMF.

> **Note**
>
> *Puede encontrar el ROLE_ARN en.* `create-cmf-fleet.json`
> Para el *OS_FAMILY*, debe elegir una de las siguientes opciones: o. `linux` `macos` `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. Guarde los cambios.

6. Crea tu flota.

```
aws deadline create-fleet --cli-input-json file://create-fleet-request.json
```

Instalación y configuración del host de trabajo

Un anfitrión de trabajo se refiere a una máquina host que ejecuta un servidor de Deadline Cloud. En esta sección se explica cómo configurar el host de trabajo y configurarlo para sus necesidades específicas. Cada host de trabajo ejecuta un programa denominado agente de trabajo. El agente trabajador es responsable de:

- Gestionar el ciclo de vida del trabajador.
- Sincronizar el trabajo asignado, su progreso y sus resultados.
- Supervisión del trabajo en ejecución.
- Reenviar los registros a los destinos configurados.

Le recomendamos que utilice el agente de trabajo de Deadline Cloud proporcionado. El agente de trabajo es de código abierto y te recomendamos que solicites funciones, pero también puedes desarrollarlo y personalizarlo para adaptarlo a tus necesidades.

Para completar las tareas de las siguientes secciones, necesitará lo siguiente:

Linux

- Una instancia Linux basada en Amazon Elastic Compute Cloud (Amazon EC2). Recomendamos Amazon Linux 2023.
- `sudo`privilegios.
- Python 3.9 o superior.

Windows

- Una instancia Windows basada en Amazon Elastic Compute Cloud (Amazon EC2). RecomendamosWindows Server 2022.
- Acceso de administrador al anfitrión del trabajador
- Python 3.9 o superior instalado para todos los usuarios

Crear y configurar un entorno virtual de Python

Puede crear un entorno virtual de Python Linux si ha instalado Python 3.9 o superior y lo ha colocado en suPATH.

Para crear y activar un entorno virtual de Python

1. Abra el AWS CLI.
2. Cree y active un entorno virtual de Python.

```
python3 -m venv /opt/deadline/worker
source /opt/deadline/worker/bin/activate
pip install --upgrade pip
```

Instale el agente de trabajo de Deadline Cloud

Una vez que hayas configurado tu Python y creado un entorno virtualLinux, instala los paquetes Python del agente de trabajo de Deadline Cloud.

Para instalar los paquetes de Python del agente de trabajo

1. Abra un terminal.
   a. LinuxActivado, abra una terminal como `root` usuario (o utilice`sudo`/`su`)
   b. ActivadoWindows, abre una línea de comandos o una PowerShell terminal de administrador.
2. Descarga e instala los paquetes de agentes de trabajo de Deadline Cloud desde PyPI:

> **Note**
>
> SíWindows, los archivos del agente deben estar instalados en el directorio global de paquetes de sitios de Python. Los entornos virtuales de Python no son compatibles actualmente.

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

Configure el agente de trabajo de Deadline Cloud

Puede configurar los ajustes del agente de trabajo de Deadline Cloud de tres maneras. Le recomendamos que utilice el sistema operativo configurado anteriormente`install-deadline-worker`.

Argumentos de línea de comandos: puede especificar argumentos al ejecutar el agente de trabajo de Deadline Cloud desde la línea de comandos. Algunos ajustes de configuración no están disponibles a través de los argumentos de la línea de comandos. Para ver todos los argumentos de la línea de comandos disponibles, introduzca `deadline-worker-agent --help` para ver todos los argumentos de la línea de comandos disponibles.

Variables de entorno: puede configurar el agente de trabajo de Deadline Cloud configurando la variable de entorno que comience por`DEADLINE_WORKER_`. Por ejemplo, se puede utilizar `export DEADLINE_WORKER_VERBOSE=true` para configurar la salida del agente de trabajo en verbosa. Para obtener más ejemplos e información, consulte `/etc/amazon/deadline/worker.toml.example` en Linux o `C:\ProgramData\Amazon\Deadline\Config\worker.toml.example` en. Windows

Archivo de configuración: al instalar el agente de trabajo, se crea un archivo de configuración ubicado `/etc/amazon/deadline/worker.toml` en Linux o `C:\ProgramData\Amazon\Deadline\Config\worker.toml` onWindows. El agente de trabajo carga este archivo de configuración cuando se inicia. Puede usar el archivo de configuración de ejemplo (`/etc/amazon/deadline/worker.toml.example`activado Linux o `C:\ProgramData\Amazon\Deadline\Config\worker.toml.example` activadoWindows) para adaptar el archivo de configuración del agente de trabajo predeterminado a sus necesidades específicas.

Por último, le recomendamos que habilite el apagado automático para el agente trabajador. Esto permite que la flota de trabajadores se amplíe cuando sea necesario y se cierre cuando finalice el trabajo de renderizado. El escalado automático ayuda a garantizar que solo utilice los recursos cuando sea necesario.

Para habilitar el apagado automático

Como **`root`** usuario:

- Instale el agente de trabajo con los parámetros**`--allow-shutdown`**.

Linux

Introduzca:

```
/opt/deadline/worker/bin/install-deadline-worker \
  --farm-id FARM_ID \
  --fleet-id FLEET_ID \
  --region REGION \
  --allow-shutdown
```

Windows

Ingresa:

```
install-deadline-worker ^
  --farm-id FARM_ID ^
  --fleet-id FLEET_ID ^
  --region REGION ^
  --allow-shutdown
```

Cree usuarios y grupos de trabajos

En esta sección se describe la relación de usuario y grupo necesaria entre el usuario agente y la `jobRunAsUser` definida en sus colas.

El agente de trabajo de Deadline Cloud debe funcionar como un usuario dedicado a un agente específico en el host. Debe configurar la `jobRunAsUser` propiedad de las colas de Deadline Cloud para que los trabajadores ejecuten las tareas de cola como un usuario y un grupo específicos del sistema operativo. Esto significa que puedes controlar los permisos de sistema de archivos compartidos que tienen tus trabajos. También proporciona un importante límite de seguridad entre sus trabajos y el usuario del agente de trabajo.

Linuxusuarios y grupos del trabajo

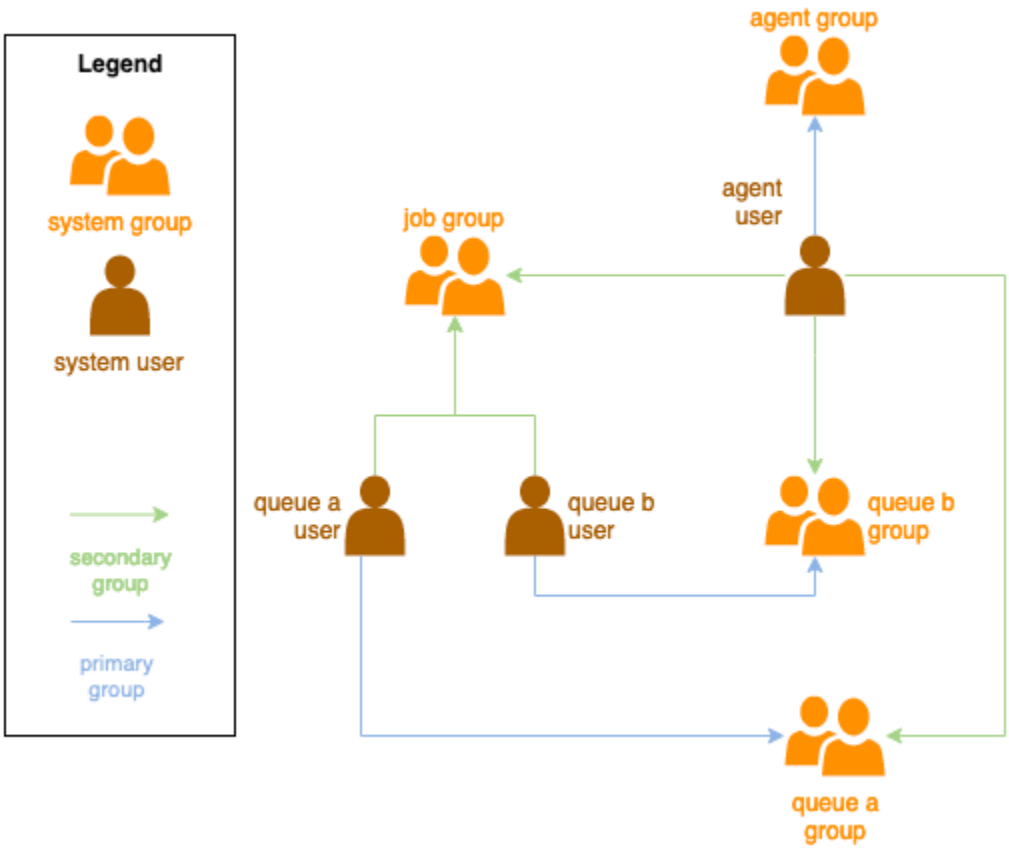
Para configurar su agente-usuario`jobRunAsUser`, asegúrese de cumplir los siguientes requisitos:

- Hay un grupo para cada uno `jobRunAsUser` y es el grupo principal para el grupo correspondiente. `jobRunAsUser`

- El agente-usuario pertenece al grupo principal de las colas en `jobRunAsUser` las que el trabajador obtiene trabajo. Como prácticas recomendadas de seguridad, recomendamos que se trate de un grupo secundario del agente-usuario. Este grupo compartido permite al agente de trabajo hacer que los archivos estén disponibles para el trabajo mientras se está ejecutando.
- A `jobRunAsUser` no pertenece al grupo principal del agente-usuario. Para conocer las mejores prácticas de seguridad:
  - Los archivos confidenciales escritos por el agente trabajador son propiedad del grupo principal del agente.
  - Si a `jobRunAsUser` pertenece a este grupo, es posible que los trabajos que se envíen a la cola del trabajador tengan acceso a los archivos que escribe el agente de trabajo.
- La AWS región predeterminada debe coincidir con la región de la granja a la que pertenece el trabajador. Para obtener más información, consulte Ajustes de configuración y archivos de credenciales.

  Esto debería aplicarse a:
  - El agente-usuario
  - Todas las `jobRunAsUser` cuentas en cola del trabajador
- El agente-usuario puede ejecutar `sudo` comandos como. `jobRunAsUser`

El siguiente diagrama ilustra la relación entre el usuario agente y los `jobRunAsUser` usuarios y grupos de las colas asociadas a la flota.



Usuarios de Windows

Para utilizar un Windows usuario como`jobRunAsUser`, debe cumplir los siguientes requisitos:

- Deben existir todos `jobRunAsUser` los usuarios de la cola.
- Sus contraseñas deben coincidir con el valor del secreto especificado en el campo de la `JobRunAsUser` cola. Para obtener instrucciones, consulte el paso 7 deCreación de una cola.
- El usuario-agente debe poder iniciar sesión como esos usuarios.

Administre el acceso a los secretos de los usuarios de trabajos de Windows

Al configurar una cola con Windows`jobRunAsUser`, debe especificar un secreto de AWS Secrets Manager. Se espera que el valor de este secreto sea un objeto codificado en JSON del siguiente formato:

```
{
    "password": "JOB_USER_PASSWORD"
```

```
}
```

Para que los trabajadores puedan ejecutar los trabajos tal y como está configurada la cola`jobRunAsUser`, la función de IAM de la flota debe tener permisos para obtener el valor del secreto. Si el secreto se cifra con una clave de KMS gestionada por el cliente, la función de IAM de la flota también debe tener permisos para descifrarlo mediante la clave de KMS.

Se recomienda encarecidamente seguir el principio del mínimo privilegio para estos secretos. Esto significa que el acceso para obtener el valor secreto de una cola → → debería ser: `jobRunAsUser` `windows` `passwordArn`

- se otorga a un rol de flota cuando se crea una asociación de cola y flota entre la flota y la cola
- se revoca de un rol de flota cuando se elimina una asociación de cola y flota entre la flota y la cola

Además, el secreto de AWS Secrets Manager que contiene la `jobRunAsUser` contraseña debe eliminarse cuando ya no se utilice.

Conceda acceso a una contraseña secreta

Las flotas de Deadline Cloud necesitan acceder a la `jobRunAsUser` contraseña almacenada en la contraseña secreta de la cola cuando se asocian la cola y la flota. Recomendamos utilizar la política de recursos de AWS Secrets Manager para conceder acceso a las funciones de la flota. Si sigues estrictamente esta directriz, es más fácil determinar qué roles de flota tienen acceso al secreto.

Para conceder acceso al secreto

1. Abra el secreto en la consola de AWS Secret Manager.
2. En la sección «Permisos de recursos», añada una declaración de política con el siguiente formato:

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    // ...
    {
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "FLEET_ROLE_ARN"
      },
```

```
      "Action" : "secretsmanager:GetSecretValue",
      "Resource" : "*"
    }
    // ...
  ]
}
```

Revocar el acceso a una contraseña secreta

Cuando una flota ya no necesite acceder a una cola, elimine el acceso a la contraseña secreta de la cola. `jobRunAsUser` Recomendamos utilizar la política de recursos de AWS Secrets Manager para conceder acceso a las funciones de la flota. Si sigues estrictamente esta directriz, es más fácil determinar qué roles de flota tienen acceso al secreto.

Para revocar el acceso al secreto

1. Abra el secreto en la consola de AWS Secret Manager.
2. En la sección Permisos de recursos, elimine la declaración de política del formulario:

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    // ...
    {
      "Effect" : "Allow",
      "Principal" : {
        "AWS" : "FLEET_ROLE_ARN"
      },
      "Action" : "secretsmanager:GetSecretValue",
      "Resource" : "*"
    }
    // ...
  ]
}
```

Instalar y configurar el software necesario para los trabajos

Después de configurar el agente de trabajo de Deadline Cloud, puede preparar el anfitrión del trabajador con cualquier software necesario para ejecutar los trabajos.

Cuando envías un trabajo a una cola con un asociado`jobRunAsUser`, el trabajo se ejecuta como ese usuario. Todos los comandos deben estar disponibles en el nombre `PATH` de ese usuario.

En Linux, puede especificar el valor `PATH` para un usuario en una de las siguientes opciones:

- su `~/.bashrc` o `~/.bash_profile`
- archivos de configuración del sistema, como `/etc/profile.d/*` y `/etc/profile`
- scripts de inicio de shell:`/etc/bashrc`.

En Windows, puede especificar el `PATH` para un usuario en una de las siguientes opciones:

- sus variables de entorno específicas del usuario
- las variables de entorno de todo el sistema

Instale adaptadores para herramientas de creación de contenido digital

Deadline Cloud proporciona aplicaciones de creación de contenido digital (DCC) con soporte de integración propio. Para utilizar estas integraciones en una flota gestionada por el cliente, debe instalar el software DCC y los adaptadores.

Para instalar los adaptadores DCC en una flota gestionada por el cliente

1. Abra el terminal A.
    a. En Linux, abre un terminal como `root` usuario (o usa`sudo`/`su`)
    b. En Windows, abra una línea de comandos o una PowerShell terminal de administrador.
2. Instale los paquetes de adaptadores de Deadline Cloud.

```
pip install deadline deadline-cloud-for-maya deadline-cloud-for-nuke deadline-
cloud-for-blender
```

Configuración de AWS credenciales

En esta sección se explica cómo configurar AWS las credenciales.

Esta fase inicial del ciclo de vida del trabajador se está iniciando. En esta fase, el software de agente obrero crea un trabajador en la flota y obtiene AWS las credenciales del rol de la flota para seguir operando.

AWS credentials for Amazon EC2

Para configurar AWS las credenciales de Amazon EC2

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. Seleccione Funciones en el panel de navegación y, a continuación, Crear función.
3. Seleccione el AWS servicio.
4. Seleccione EC2 como servicio o caso de uso y, a continuación, seleccione Siguiente.
5. Adjunte la política `AWSDeadlineCloud-WorkerHost` AWS gestionada.

On-premise AWS credentials

Para configurar AWS las credenciales locales

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. Seleccione Funciones en el panel de navegación y, a continuación, Crear función.
3. Seleccione Cuenta de AWSy, a continuación, seleccione Siguiente.
4. Adjunta la política `AWSDeadlineCloud-WorkerHost` AWS gestionada.
5. Genere claves secretas y de acceso de AWS IAM para el usuario de IAM:
    a. Para ver IAM Role Anywhere, consulte IAM Roles Anywhere.
    b. Para conocer la forma más segura de configurar las credenciales en el host, consulte Obtención de credenciales de seguridad temporales de AWS Identity and Access Management Roles Anywhere.
    c. También puede utilizar la CLI como autenticación alternativa. Para obtener más información, consulte Autenticación con credenciales de usuario de IAM.
6. Guarde estas claves en el archivo de AWS credenciales del agente-usuario del sistema de archivos del host de trabajo.
    a. En Linux, se encuentra en `~/.aws/credentials`
    b. En Windows, se encuentra en `%USERPROFILE%\.aws\credentials`

> **Note**
>
> Solo debe poder acceder a las credenciales el nombre de usuario del sistema operativo (`deadline-worker-agent`) que instaló el agente de trabajo.

```
# Replace keys below
[default]
aws_access_key_id=ACCESS_KEY_ID
aws_secret_access_key=SECRET_ACCESSS_KEY
```

7. Cambie el `deadline-worker-agent` propietario y los permisos.

> **Note**
>
> Si cambió el nombre de usuario del sistema operativo (`deadline-worker-agent`) al instalar el agente de trabajo, utilice ese nombre en su lugar.

Crear un Amazon Machine Image

Para crear un Amazon Machine Image (AMI) para usarlo en una flota gestionada por el cliente (CMF) de Amazon Elastic Compute Cloud (Amazon EC2), complete las tareas de esta sección. Debe crear una instancia de Amazon EC2 antes de continuar. Para obtener más información, consulte Lance your instance en la Guía del usuario de Amazon EC2 para instancias de Linux.

> **Important**
>
> Al crear y, se AMI crea una instantánea de los volúmenes adjuntos a la instancia de Amazon EC2. Todo el software instalado en la instancia se conserva en las instancias, que se reutilizan al lanzar instancias desde. AMI Recomendamos adoptar una estrategia de parches y actualizar periódicamente los nuevos AMI con el software actualizado antes de aplicarlos a su flota.

Prepare la instancia de Amazon EC2

Antes de crear unaAMI, debe eliminar el estado de trabajo. El estado obrero persiste entre el lanzamiento del agente obrero. Si este estado persiste enAMI, todas las instancias que se lancen desde él compartirán el mismo estado.

También le recomendamos que elimine todos los archivos de registro existentes. Los archivos de registro pueden permanecer en una instancia de Amazon EC2 cuando prepare la AMI. La eliminación de estos archivos minimiza la confusión a la hora de diagnosticar un posible problema en las flotas de trabajadores que utilizan la AMI.

También debe habilitar el servicio del sistema de agentes de trabajo para que el agente de trabajo de Deadline Cloud se lance cuando se inicie Amazon EC2.

Por último, le recomendamos que active el apagado automático del agente de trabajo. Esto permite que la flota de trabajadores se amplíe cuando sea necesario y se cierre cuando finalice el trabajo de renderizado. Este escalado automático ayuda a garantizar que solo utilice los recursos según sea necesario.

Para preparar la instancia de Amazon EC2

1. Abra la consola de Amazon EC2.
2. Lance una instancia de Amazon EC2. Para obtener más información, consulte Lance your instance.
3. Configure el host para que se conecte a su proveedor de identidad (IdP) y, a continuación, monte cualquier sistema de archivos compartido que necesite.
4. Sigue los tutoriales paraInstale el agente de trabajo de Deadline Cloud, luegoConfigure el agente de trabajo, y. Cree usuarios y grupos de trabajos
5. Si está preparando un software AMI basado en Amazon Linux 2023 para ejecutar software compatible con la plataforma de referencia VFX, necesitará actualizar varios requisitos. Para obtener más información, consulte Compatibilidad con el VFX Reference Platform.
6. Abra un terminal.
    a. En Linux, abra un terminal como `root` usuario (o utilice`sudo`/`su`)
    b. En Windows, abra una línea de comandos o una PowerShell terminal de administrador.
7. Asegúrese de que el servicio de trabajo no esté en ejecución y esté configurado para iniciarse al arrancar:

a. En Linux, ejecute

```
systemctl stop deadline-worker
systemctl enable deadline-worker
```

b. En Windows, ejecute

```
sc.exe stop DeadlineWorker
sc.exe config DeadlineWorker start= auto
```

8. Elimine el estado del trabajador.

a. En Linux, ejecute

```
rm -rf /var/lib/deadline/*
```

b. En Windows, ejecute

```
del /Q /S %PROGRAMDATA%\Amazon\Deadline\Cache\*
```

9. Elimine los archivos de registro.

a. En Linux, ejecute

```
rm -rf /var/log/amazon/deadline/*
```

b. En Windows, ejecute

```
del /Q /S %PROGRAMDATA%\Amazon\Deadline\Logs\*
```

10. En Windows, se recomienda ejecutar la aplicación Amazon EC2Launch Settings que se encuentra en el menú Inicio para completar la preparación final del host y el cierre de la instancia.

> **Note**
>
> DEBE elegir Apagar sin Sysprep y nunca apagar con Sysprep. Si se cierra con Sysprep, todos los usuarios locales quedarán inutilizables. Para obtener más información,

consulte la sección Antes de empezar del tema Crear una AMI personalizada de la Guía del usuario para instancias de Windows.

Cree el AMI

Para construir el AMI

1. Abra la consola de Amazon EC2.
2. Seleccione Instances en el panel de navegación y, a continuación, seleccione su instancia.
3. Seleccione Estado de la instancia y, a continuación, Detenga la instancia.
4. Una vez detenida la instancia, selecciona Acciones.
5. Selecciona Imagen y plantillas y, a continuación, Crear imagen.
6. Ingresa un nombre de imagen.
7. (Opcional) Introduce una descripción para la imagen.
8. Elija Crear imagen.

Cree una infraestructura de flota con un grupo de Auto Scaling de Amazon EC2

En esta sección se explica cómo crear una flota de Auto Scaling de Amazon EC2.

Utilice la plantilla AWS CloudFormation YAML que aparece a continuación para crear un grupo de Auto Scaling (Auto Scaling) de Amazon EC2, una Amazon Virtual Private Cloud (Amazon VPC) con dos subredes, un perfil de instancia y un rol de acceso a la instancia. Son necesarios para lanzar la instancia mediante Auto Scaling en las subredes.

Deberías revisar y actualizar la lista de tipos de instancias para adaptarla a tus necesidades de renderización.

Para crear una flota de Auto Scaling de Amazon EC2

1. Abra la AWS CloudFormation consola en https://console.aws.amazon.com/cloudformation.
2. Cree una CloudFormation plantilla con los parámetros `Farm ID`Fleet ID, y`AMI ID`.

```
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 launcing 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 workers in 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
```

3. Tras crear las funciones de IAM, debe tener en cuenta lo siguiente:

   - Las credenciales del rol de IAM asociadas a la instancia Amazon EC2 del trabajador están disponibles para todos los procesos que se ejecutan en ese trabajador, incluidos los trabajos. El trabajador debe tener el mínimo de privilegios para operar: y `deadline:CreateWorker` `deadline:AssumeFleetRoleForWorker.`
   - El agente de trabajo obtiene las credenciales para la función de cola y las configura para que las utilice en la ejecución de trabajos. El rol del perfil de instancia de Amazon EC2 no debe incluir los permisos que necesitan sus trabajos.

Amplíe automáticamente su flota de Amazon EC2 con la función de recomendación de escalado de Deadline Cloud

Deadline Cloud aprovecha un grupo de Auto Scaling (Auto Scaling) de Amazon EC2 para escalar automáticamente la flota gestionada por el cliente (CMF) de Amazon EC2. Debe configurar el modo de flota e implementar la infraestructura requerida en su cuenta para que su flota se escale automáticamente. La infraestructura que implementaste funcionará en todas las flotas, por lo que solo tendrás que configurarla una vez.

El flujo de trabajo básico consiste en configurar el modo de flota para que se escale automáticamente y, a continuación, Deadline Cloud enviará un EventBridge evento para esa flota cada vez que cambie el tamaño de la flota recomendado (un evento contiene el identificador de la flota, el tamaño de la flota recomendado y otros metadatos). Dispondrá de una EventBridge regla para filtrar los eventos relevantes y dispondrá de una Lambda para consumirlos. La Lambda se integrará con Amazon EC2 `AutoScalingGroup` Auto Scaling para escalar automáticamente la flota de Amazon EC2.

Configure el modo de flota en **`EVENT_BASED_AUTO_SCALING`**

Configura tu modo de flota para`EVENT_BASED_AUTO_SCALING`. Para ello, puede utilizar la consola o utilizar la AWS CLI para llamar directamente a la `UpdateFleet` API `CreateFleet` o. Una vez configurado el modo, Deadline Cloud comienza a enviar EventBridge eventos cada vez que cambia el tamaño de flota recomendado.

- Ejemplo de `UpdateFleet` comando:

```
aws deadline update-fleet \
  --farm-id FARM_ID \
  --fleet-id FLEET_ID \
  --configuration file://configuration.json
```

- Ejemplo de `CreateFleet` comando:

```
aws deadline create-fleet \
  --farm-id FARM_ID \
  --display-name "Fleet name" \
  --max-worker-count 10 \
  --configuration file://configuration.json
```

El siguiente es un ejemplo del `configuration.json` uso en los comandos CLI anteriores (`--configuration file://configuration.json`).

- Para activar Auto Scaling en su flota, debe configurar el modo en`EVENT_BASED_AUTO_SCALING`.
- Estos `workerCapabilities` son los valores predeterminados que se asignaron al CMF cuando lo creó. Puede cambiar estos valores si necesita aumentar los recursos disponibles para su CMF.

Después de configurar el modo de flota, Deadline Cloud comienza a emitir eventos de recomendación sobre el tamaño de la flota para esa flota.

```
{
    "customerManaged": {
        "mode": "EVENT_BASED_AUTO_SCALING",
        "workerCapabilities": {
            "vCpuCount": {
                "min": 1,
                "max": 4
            },
            "memoryMiB": {
                "min": 1024,
                "max": 4096
            },
            "osFamily": "linux",
            "cpuArchitectureType": "x86_64",
        }
```

```
    }
}
```

Implemente la pila de Auto Scaling mediante la AWS CloudFormation plantilla

Puede configurar una EventBridge regla para filtrar los eventos, una Lambda para consumir los eventos y controlar Auto Scaling y una cola SQS para almacenar los eventos sin procesar. Utilice la siguiente AWS CloudFormation plantilla para implementar todo en una pila. Una vez que hayas desplegado los recursos correctamente, puedes enviar un trabajo y la flota se ampliará automáticamente.

```
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
```

Connect las flotas gestionadas por el cliente a un punto final de licencia

El servidor de licencias basado en el uso de AWS Deadline Cloud (Deadline Cloud) ofrece licencias bajo demanda para determinados productos de terceros. Esto le permite pagar sobre la marcha. Solo cambiarás por el tiempo que utilices.

El servidor de licencias basado en el uso de Deadline Cloud se puede utilizar con cualquier tipo de flota siempre que los trabajadores de Deadline Cloud puedan comunicarse con el servidor de licencias. Esto se configura automáticamente en las flotas gestionadas por el servicio. Esta configuración solo es necesaria para las flotas gestionadas por el cliente.

Para crear el servidor de licencias, necesita lo siguiente:

- Un grupo de seguridad para la VPC de su granja que permite el tráfico de licencias de terceros.
- Un rol AWS Identity and Access Management (IAM) con una política adjunta que permite el acceso a las operaciones de punto final de licencia de Deadline Cloud.

Temas

- Paso 1: Crear un grupo de seguridad
- Paso 2: Configure el punto final de la licencia
- Paso 3: Conectar una aplicación de renderizado a un punto final

Paso 1: Crear un grupo de seguridad

Utilice la consola Amazon VPC (https://console.aws.amazon.com/vpc/) para crear un grupo de seguridad para la VPC de su granja. Configure el grupo de seguridad para permitir las siguientes reglas de entrada:

- Autodesk Maya y Arnold: 2701 - 2702, TCP, IPv4
- Autodesk 3ds Max: 2704, TCP, IPv4
- Foundry Nuke: 6101, TCP, IPv4
- SideFX Houdini, Mantra y Karma: 1715 - 1717, TCP, IPv4

El origen de cada regla de entrada es el grupo de seguridad de los trabajadores de la flota.

Para obtener más información sobre la creación de un grupo de seguridad, consulte Crear un grupo de seguridad en la guía del usuario de Amazon Virtual Private Cloud.

Paso 2: Configure el punto final de la licencia

Un punto final de licencia proporciona acceso a los servidores de licencias para productos de terceros. Las solicitudes de licencia se envían al punto final de la licencia. El punto final las dirige al servidor de licencias correspondiente. El servidor de licencias rastrea los límites de uso y los derechos. Se aplica un cargo por cada punto de conexión de licencia que cree. Para obtener más información, consulte Precios de Amazon VPC.

Puede crear el punto de conexión de su licencia desde el AWS Command Line Interface con los permisos adecuados. Para conocer la política requerida para crear un punto de enlace de licencia, consulte Política para permitir la creación de un punto de enlace de licencia.

Puede usar el AWS CloudShell (https://console.aws.amazon.com/cloudshell/) o cualquier otro AWS CLI entorno para configurar el punto final de la licencia mediante los siguientes AWS Command Line Interface comandos.

1. Cree el punto final de la licencia. Sustituya el ID del grupo de seguridad, el ID de subred y el ID de VPC por los valores que creó anteriormente. Si usa varias subredes, sepárelas con espacios.

```
aws deadline create-license-endpoint \
  --security-group-id SECURITY_GROUP_ID \
  --subnet-ids SUBNET_ID1 SUBNET_ID2 \
  --vpc-id VPC_ID
```

2. Confirme que el punto final se creó correctamente con el siguiente comando. Recuerde el nombre DNS del punto final de la VPC.

```
aws deadline get-license-endpoint \
  --license-endpoint-id LICENSE_ENDPOINT_ID
```

3. Consulte una lista de los productos medidos disponibles:

```
aws deadline list-available-metered-products
```

4. Añada los productos con contador al punto final de la licencia con el siguiente comando.

```
aws deadline put-metered-product \
--license-endpoint-id LICENSE_ENDPOINT_ID \
--product-id PRODUCT_ID
```

Puede eliminar un producto de un punto final de licencia con el `remove-metered-product` comando:

```
aws deadline remove-metered-product \
  --license-endpoint-id LICENSE_ENDPOINT_ID \
  --productId PRODUCT_ID
```

Puede eliminar un punto final de licencia con el `delete-license-endpoint` comando:

```
aws deadline delete-license-endpoint \
 --license-endpoint-id LICENSE_ENDPOINT_ID
```

Paso 3: Conectar una aplicación de renderizado a un punto final

Una vez configurado el punto final de la licencia, las aplicaciones lo utilizan de la misma manera que lo hacen con un servidor de licencias de terceros. Por lo general, se configura el servidor de licencias para la aplicación estableciendo una variable de entorno u otro ajuste del sistema, como una clave de registro de Microsoft Windows, en un puerto y una dirección del servidor de licencias.

Para obtener el nombre DNS del punto de conexión de la licencia, utilice el siguiente AWS CLI comando.

```
aws deadline get-license-endpoint
```

O bien, puede utilizar la consola de Amazon VPC (https://console.aws.amazon.com/vpc/) para identificar el punto de enlace de VPC creado por la API de Deadline Cloud en el paso anterior.

Ejemplos de configuraciones

Example — Autodesk Maya y Arnold

Defina la variable de entorno `ADSKFLEX_LICENSE_FILE` en:

```
2702@VPC_Endpoint_DNS_Name:2701@VPC_Endpoint_DNS_Name
```

> **Note**
>
> En el Windows caso de los trabajadores, utilice un punto y coma (;) en lugar de dos puntos (:) para separar los puntos finales.

Example — Autodesk 3ds Max

Defina la variable `ADSKFLEX_LICENSE_FILE` de entorno en:

```
2704@VPC_Endpoint_DNS_Name
```

Example — Foundry Nuke

Defina la variable de entorno en `foundry_LICENSE 6101@`*`VPC_Endpoint_DNS_Name`* Para comprobar que las licencias funcionan correctamente, puede ejecutar Nuke en una terminal:

```
~/nuke/Nuke14.0v5/Nuke14.0 -x
```

Example — SideFX, Houdini, Mantra y Karma

Ejecute el siguiente comando:

```
/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;"
```

Para comprobar que las licencias funcionan correctamente, puede renderizar una escena de Houdini mediante este comando:

```
/opt/hfs19.5.640/bin/hython ~/forpentest.hip -c "hou.node('/out/mantra1').render()"
```

Administrar usuarios en Deadline Cloud

AWS Deadline Cloud se usa AWS IAM Identity Center para administrar usuarios y grupos. IAM Identity Center es un servicio de inicio de sesión único basado en la nube que se puede integrar con su proveedor de inicio de sesión único (SSO) empresarial. Con la integración, los usuarios pueden iniciar sesión con la cuenta de su empresa.

Deadline Cloud habilita el Centro de Identidad de IAM de forma predeterminada y es necesario configurar y utilizar Deadline Cloud. Para obtener más información, consulte Administrar su fuente de identidad.

El propietario de su organización AWS Organizations es responsable de administrar los usuarios y grupos que tienen acceso a su monitor de Deadline Cloud. Puede crear y gestionar estos usuarios y grupos mediante el Centro de Identidad de IAM o la consola de Deadline Cloud. Para obtener más información, consulte ¿Qué es AWS Organizations?

Puede crear y eliminar usuarios y grupos que pueden usar el monitor para administrar granjas, colas y flotas mediante la consola de Deadline Cloud. Al añadir un usuario a Deadline Cloud, este debe restablecer su contraseña mediante el Centro de identidad de IAM antes de poder acceder.

Temas

- Administre los usuarios y grupos del monitor
- Administre los usuarios y grupos de granjas, colas y flotas

Administre los usuarios y grupos del monitor

El propietario de una organización puede usar la consola de Deadline Cloud para administrar los usuarios y grupos que tienen acceso al monitor de Deadline Cloud. Puede elegir entre los usuarios y grupos existentes del IAM Identity Center o puede añadir nuevos usuarios y grupos desde la consola.

1. Inicie sesión en la consola de Deadline Cloud AWS Management Console y ábrala. En la página principal, en la sección Cómo empezar, selecciona Configurar Deadline Cloud o Ir al panel de control.
2. En el panel de navegación izquierdo, selecciona Administración de usuarios. De forma predeterminada, está seleccionada la pestaña Grupos.

En función de la acción que se vaya a realizar, elija la pestaña Grupos o la pestaña Usuarios.

Monitor groups

Creación de un grupo

1. Elija Crear grupo.
2. Introduzca un nombre de grupo. El nombre debe ser único entre los grupos de la organización de su centro de identidad de IAM.

Para eliminar un grupo

1. Seleccione el grupo que desee eliminar.
2. Elija Eliminar.
3. En el cuadro de diálogo de confirmación, selecciona Eliminar grupo.

> **Note**
>
> Va a eliminar el grupo del Centro de identidades de IAM. Los miembros del grupo ya no pueden iniciar sesión en Deadline Cloud ni acceder a los recursos de la granja.

Monitor users

Para agregar usuarios

1. Elija la pestaña Users.
2. Elija Agregar usuarios.
3. Introduzca el nombre, la dirección de correo electrónico y el nombre de usuario del nuevo usuario.
4. Si lo desea, elija uno o más grupos del IAM Identity Center a los que añadir el nuevo usuario.
5. Seleccione Enviar invitación para enviar al nuevo usuario un correo electrónico con instrucciones para unirse a su organización del Centro de Identidad de IAM.

Para eliminar un usuario

1. Seleccione el usuario que desee eliminar del monitor.
2. Elija Eliminar.

3. En el cuadro de diálogo de confirmación, seleccione Eliminar usuario.

> **Note**
>
> Va a eliminar el usuario del Centro de identidades de IAM. El usuario ya no puede iniciar sesión en el monitor de Deadline Cloud ni acceder a los recursos de la granja.

Administre los usuarios y grupos de granjas, colas y flotas

1. Si aún no lo has hecho, inicia sesión en la consola de Deadline Cloud AWS Management Console y ábrela.
2. En el panel de navegación izquierdo, selecciona Granjas y otros recursos.
3. Seleccione la granja que desee administrar. Elija el nombre de la granja para abrir la página de detalles. Puede buscar la granja mediante la barra de búsqueda.
4. Para gestionar una cola o una flota, selecciona la pestaña Colas o Flotas y, a continuación, selecciona la cola o la flota que quieres gestionar.
5. Seleccione la pestaña Gestión de acceso. De forma predeterminada, está seleccionada la pestaña Grupos. Para administrar los usuarios, mueve el botón a Usuarios.

En función de la acción que se vaya a realizar, selecciona la pestaña Grupos o la pestaña Usuarios.

Para ver las definiciones de los niveles de acceso, consulte Permisos.

Groups

Cómo añadir grupos:

1. Seleccione el conmutador Grupos.
2. Elija Añadir grupo.
3. En el menú desplegable, selecciona los grupos que deseas añadir.
4. Para el nivel de acceso grupal, elige una de las siguientes opciones:
   - Espectador
   - Colaborador
   - Gestor

- Propietario

5. Elija Añadir.

Cómo eliminar grupos:

1. Seleccione los grupos que desee eliminar.
2. Elija Eliminar.
3. En el diálogo de confirmación, elija Remove.

Users

Para agregar usuarios

1. Para añadir un usuario, selecciona Añadir usuario.
2. En el menú desplegable, selecciona los usuarios que deseas añadir a tu granja.
3. Para el nivel de acceso de los usuarios, elige una de las siguientes opciones:
   - Espectador
   - Colaborador
   - Gestor
   - Propietario
4. Elija Añadir. Los usuarios se añaden a su granja.

Cómo eliminar usuarios:

1. Seleccione el usuario que desee eliminar.
2. En el cuadro de diálogo de confirmación de eliminación, seleccione Eliminar. A continuación, se elimina al usuario de la granja seleccionada.

También puede añadir o eliminar permisos de granja para usuarios y grupos mediante la consola del IAM Identity Center en https://console.aws.amazon.com/singlesignon/.

Empleos en Deadline Cloud

Un trabajo es un conjunto de instrucciones que AWS Deadline Cloud utiliza para programar y ejecutar el trabajo con los trabajadores disponibles. Cuando creas un trabajo, eliges la granja y la cola a las que quieres enviar el trabajo. También proporciona un archivo JSON o YAML que contiene las instrucciones para que los trabajadores las procesen. Deadline Cloud acepta plantillas de trabajo que siguen la especificación Open Job Description (OpenJD) para describir los trabajos. Para obtener más información, consulte la documentación de descripción del puesto de trabajo abierto en el GitHub sitio web.

Un trabajo consiste en:

- Pasos: define el script que se ejecutará en los trabajadores. Los pasos pueden tener requisitos como una memoria mínima para el trabajador u otros pasos que deban completarse primero. Cada paso tiene una o más tareas.
- Tareas: unidad de trabajo que se envía a un trabajador para que la lleve a cabo. Una tarea es una combinación del guion de un paso y de los parámetros, como el número de fotograma, que se utilizan en el guion. El trabajo estará completo cuando se hayan completado todas las tareas de todos los pasos.
- Entornos: configura y desmonta las instrucciones que se comparten en varios pasos o tareas.

Puede crear un trabajo de cualquiera de las siguientes maneras:

- Usa un remitente de Deadline Cloud.
- Cree un paquete de trabajos y utilice la interfaz de línea de comandos de Deadline Cloud (CLI de Deadline Cloud).
- Usa el AWS SDK.
- Usa el AWS Command Line Interface (AWS CLI).

Un remitente es un complemento para su software de creación de contenido digital (DCC) que gestiona la creación de un trabajo en la interfaz de su software de DCC. Después de crear el trabajo, utilizas el remitente para enviarlo a Deadline Cloud para su procesamiento. Entre bastidores, el remitente crea una plantilla de trabajo de OpenJD que describe el trabajo. Al mismo tiempo, carga los archivos de sus activos en un bucket de Amazon Simple Storage Service (Amazon S3). Para

reducir el tiempo que se tarda en enviar los archivos, solo se envían a Amazon S3 los archivos que han cambiado desde la última vez que los cargó.

Para crear tus propios scripts y canalizaciones para enviar trabajos a Deadline Cloud, puedes usar la CLI de Deadline Cloud, el AWS SDK o las operaciones de llamada AWS CLI para crear, obtener, ver y enumerar trabajos. En los siguientes temas se explica cómo utilizar la CLI de Deadline Cloud.

La CLI de Deadline Cloud se instala junto con el remitente de Deadline Cloud. Para obtener más información, consulte Configura los remitentes de Deadline Cloud.

Temas

- Envío de trabajos con la CLI de Deadline Cloud
- Programar trabajos en Deadline Cloud
- Estados de trabajo en la CLI de Deadline Cloud
- Modificación de trabajos en Deadline Cloud
- Cómo procesa Deadline Cloud los trabajos
- Solución de problemas de trabajos en Deadline

Envío de trabajos con la CLI de Deadline Cloud

Para enviar un trabajo mediante la interfaz de línea de comandos de Deadline Cloud (CLI de Deadline Cloud), utilice el `deadline bundle submit` comando.

Los trabajos se envían a las colas. Si aún no has configurado una granja y una cola, usa la consola de Deadline Cloud (https://console.aws.amazon.com/https://console.aws.amazon.com/deadlinecloud/home) para configurar una granja y una cola y ver el ID de la granja y la cola. Para obtener más información, consulte Definir los detalles de la granja y Definir los detalles de la cola.

Para configurar la granja y la cola predeterminadas para la CLI de Deadline Cloud, utilice el siguiente comando. Al establecer los valores predeterminados, puede usar los comandos CLI de Deadline Cloud sin especificar una granja o una cola. En el siguiente ejemplo, sustituya *farmId* y *queueId* por su propia información:

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

Para especificar los pasos y las tareas de un trabajo, cree una plantilla de trabajo de OpenJD. Para obtener más información, consulte Esquemas de plantillas [Versión: 2023-09] en el repositorio de especificaciones de Open Job Description. GitHub

El siguiente ejemplo es una plantilla de trabajo de YAML. Define un trabajo con dos pasos y cinco tareas por paso.

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

Para crear un trabajo, cree una nueva carpeta con el nombre `sample_job` y guarde el archivo de plantilla en la nueva carpeta como`template.yaml`. Envía el trabajo con el siguiente comando CLI de Deadline Cloud:

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

La respuesta del comando contiene un identificador para el trabajo. Recuerde el identificador para poder comprobar el estado del trabajo más adelante.

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

Existen opciones adicionales que puede utilizar al enviar un trabajo. Para obtener más información, consulte Más opciones para enviar trabajos con la CLI de Deadline Cloud.

Más opciones para enviar trabajos con la CLI de Deadline Cloud

El comando CLI de `deadline bundle submit` Deadline Cloud proporciona opciones que puede usar para especificar información adicional para un trabajo. Los siguientes ejemplos muestran como:

- Especifique los parámetros que se utilizan al procesar la plantilla de trabajo.
- Adjunte archivos y carpetas de un entorno compartido a un trabajo.
- Establezca el número máximo de errores en las tareas antes de que se cancele un trabajo.
- Establece el número máximo de reintentos para una tarea.

Parámetros del flujo de trabajo

La `parameters` opción establece el valor de un parámetro de trabajo al crear el trabajo. La plantilla de trabajo define el campo y la `parameters` opción establece el valor. Un parámetro puede tener un valor por defecto. Si se especifica un valor para el parámetro, el valor especificado anula el valor predeterminado.

La siguiente plantilla de trabajo define el `TestParameter` campo:

```
name: Sample Job With Job Parameter
parameterDefinitions:
- default: test
  name: TestParameter
  type: STRING
specificationVersion: jobtemplate-2023-09
```

```
steps:
- description: step description
  name: MyStep
  parameterSpace:
    taskParameterDefinitions:
    - name: var
      range: 1-5
      type: INT
  script:
    actions:
      onRun:
        args:
        - '1'
        command: /usr/bin/sleep
```

El siguiente comando establece el valor de como «Hello AWS»: `TestParameter`

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

Perfiles de almacenamiento

Los perfiles de almacenamiento ayudan a compartir archivos entre trabajadores con diferentes sistemas operativos. Cree un perfil de almacenamiento mediante la consola de Deadline Cloud. A continuación, utilice el `storage-profile-id` parámetro para utilizar el perfil de almacenamiento. Para obtener más información, consulte Almacenamiento compartido en Deadline Cloud.

Para configurar el perfil de almacenamiento para los envíos de trabajos, mediante la CLI de Deadline Cloud, utilice el siguiente comando para establecer el parámetro de `storage-profile-id` configuración:

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

Número máximo de tareas fallidas

La `max-failed-tasks-count` opción establece el número máximo de tareas que pueden fallar antes de que falle todo el trabajo y se marquen todas las tareas restantes`CANCELED`. El valor predeterminado es 100.

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

Número máximo de reintentos de tareas fallidas

La `max-retries-per-task` opción establece el número máximo de veces que se debe volver a intentar una tarea antes de que se produzca un error. Cuando se vuelve a intentar una tarea, se pone en ese estado. `READY` El valor predeterminado es 5.

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

Programar trabajos en Deadline Cloud

Una vez creado un trabajo, AWS Deadline Cloud lo programa para que se procese en una o más de las flotas asociadas a una cola. La flota que procesa una tarea en particular se elige en función de las capacidades configuradas para la flota y los requisitos del anfitrión de un paso específico.

Los trabajos se programan en orden de prioridad, de mayor a menor. Cuando dos trabajos tienen la misma prioridad, el trabajo más antiguo se programa primero.

En las siguientes secciones se proporcionan detalles del proceso de programación de un trabajo.

Determine la compatibilidad de la flota

Una vez creado un trabajo, Deadline Cloud compara los requisitos de alojamiento para cada paso del trabajo con las capacidades de las flotas asociadas a la cola a la que se envió el trabajo. Si una flota cumple con los requisitos de hospedaje, el trabajo pasa a manos del `READY` estado.

Si algún paso del trabajo tiene requisitos que una flota asociada a la cola no puede cumplir, el estado del paso se establece en. `NOT_COMPATIBLE` Además, el resto de los pasos del trabajo se cancelan.

Las capacidades de una flota se establecen a nivel de flota. Incluso si un trabajador de una flota cumple con los requisitos del trabajo, no se le asignarán tareas del trabajo si su flota no cumple con los requisitos del trabajo.

La siguiente plantilla de trabajo tiene un paso que especifica los requisitos de anfitrión para el paso:

```
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
```

Este trabajo se puede programar para una flota con las siguientes capacidades:

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

Este trabajo no se puede programar para una flota con ninguna de las siguientes capacidades:

```
{
    "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.
```

Escalado de flota

Cuando se asigna un trabajo a una flota gestionada por servicio compatible, la flota se escala automáticamente. La cantidad de trabajadores de la flota fluctúa en función de la cantidad de tareas disponibles para la flota.

Cuando se asigna un trabajo a una flota gestionada por el cliente, es posible que ya existan trabajadores o que se puedan crear mediante el escalado automático basado en eventos. Para obtener más información, consulte Uso EventBridge para gestionar eventos de autoescalado en la Guía del usuario de Auto Scaling de Amazon EC2.

Sesiones

Las tareas de un trabajo se dividen en una o más sesiones. Los trabajadores dirigen las sesiones para configurar el entorno, ejecutar las tareas y, a continuación, desmantelar el entorno. Cada sesión se compone de una o más acciones que el trabajador debe realizar.

A medida que un trabajador completa las acciones de la sección, se le pueden enviar acciones de sesión adicionales. El trabajador reutiliza los entornos existentes y los adjuntos de trabajo en la sesión para completar las tareas de manera más eficiente.

Los adjuntos de trabajo los crea el remitente que utilizas, como parte de tu paquete de trabajos CLI de Deadline Cloud. También puede crear adjuntos de trabajo mediante la `--attachments` opción del `create-job` AWS CLI comando. Los entornos se definen en dos lugares: los entornos de cola adjuntos a una cola específica y los entornos de pasos de tareas definidos en la plantilla de trabajo.

Hay cuatro tipos de acciones de sesión:

- `syncInputJobAttachments`— Descarga los archivos adjuntos al trabajo de entrada para el trabajador.

- `envEnter`— Realiza las `onEnter` acciones de un entorno.
- `taskRun`— Realiza las onRun acciones de una tarea.
- `envExit`— Realiza las `onExit` acciones para un entorno.

La siguiente plantilla de trabajo tiene un entorno escalonado. Tiene una `onEnter` definición para configurar el entorno escalonado, una onRun definición que define la tarea que se va a ejecutar y una `onExit` definición para desmantelar el entorno escalonado. Las sesiones creadas para este trabajo incluirán una `envEnter` acción, una o más `taskRun` acciones y, a continuación, una `envExit` acción.

```
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 }}
```

Dependencias escalonadas

Deadline Cloud permite definir las dependencias entre los pasos, de modo que un paso espere a que se complete otro paso antes de empezar. Puedes definir más de una dependencia para un paso. Un paso con una dependencia no se programa hasta que todas sus dependencias estén completas.

Si la plantilla de trabajo define una dependencia circular, el trabajo se rechaza y su estado se establece en. `CREATE_FAILED`

La siguiente plantilla de trabajo crea un trabajo en dos pasos. `StepB`depende de`StepA`. `StepB`solo se ejecuta después de que `StepA` se complete correctamente.

Una vez creado el trabajo, `StepA` se encuentra en el `READY` estado y `StepB` se encuentra en el `PENDING` estado. Una vez `StepA` finalizado, `StepB` pasa al `READY` estado. Si `StepA` falla o `StepA` se cancela, `StepB` pasa al `CANCELED` estado.

Puede establecer una dependencia en varios pasos. Por ejemplo, si `StepC` depende de ambos `StepA` pasos`StepB`, `StepC` no empezará hasta que finalicen los otros dos pasos.

```
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!
```

Estados de trabajo en la CLI de Deadline Cloud

En este tema se describe cómo utilizar la interfaz de línea de comandos de AWS Deadline Cloud (CLI de Deadline Cloud) para ver el estado de un trabajo o paso. Si desea utilizar el monitor de Deadline Cloud para ver el estado de los trabajos o pasos, consulteVea y gestione los trabajos, los pasos y las tareas en Deadline Cloud.

Puede ver el estado de un trabajo mediante el comando CLI de `deadline job get --job-id` Deadline Cloud. La respuesta a los comandos incluye el estado del trabajo o paso y el número de tareas en cada estado de procesamiento.

Al enviar un trabajo por primera vez, el estado es`CREATE_IN_PROGRESS`. Si el trabajo supera las comprobaciones de validación, su estado cambia a`CREATE_COMPLETE`. Si no, el estado cambia a`CREATE_FAILED`.

Algunas de las posibles razones por las que un trabajo puede fallar en las comprobaciones de validación son las siguientes:

- La plantilla de trabajo no sigue la especificación de OpenJD.
- El trabajo contiene demasiados pasos.
- El trabajo contiene demasiadas tareas en total.

Para ver las cuotas del número máximo de pasos y tareas de un trabajo, utilice la consola Service Quotas. Para obtener más información, consulte Cuotas para Deadline Cloud.

También puede haber un error de servicio interno que impida la creación de un trabajo. Si esto ocurre, el código de estado del trabajo es `INTERNAL_ERROR` y el campo del mensaje de estado proporciona una explicación más detallada.

Use el siguiente comando CLI de Deadline Cloud para ver los detalles de un trabajo. En el siguiente ejemplo, *`jobID`*sustitúyalo por tu propia información:

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

La respuesta del `deadline job get` comando es la siguiente:

```
jobId: jobId
name: Sample Job
lifecycleStatus: CREATE_COMPLETE
lifecycleStatusMessage: Job creation completed successfully
priority: 50
createdAt: 2024-03-26 18:11:19.065000+00:00
createdBy: Test User
startedAt: 2024-03-26 18:12:50.710000+00:00
taskRunStatus: STARTING
```

```
taskRunStatusCounts:
  PENDING: 0
  READY: 5
  RUNNING: 0
  ASSIGNED: 0
  STARTING: 0
  SCHEDULED: 0
  INTERRUPTING: 0
  SUSPENDED: 0
  CANCELED: 0
  FAILED: 0
  SUCCEEDED: 0
  NOT_COMPATIBLE: 0
maxFailedTasksCount: 100
maxRetriesPerTask: 5
```

Cada tarea de un trabajo o paso tiene un estado. Los estados de las tareas se combinan para proporcionar un estado general de los trabajos y los pasos. El número de tareas en cada estado se indica en el `taskRunStatusCounts` campo de la respuesta.

El estado de un trabajo o paso depende del estado de sus tareas. El estado lo determinan las tareas que tienen estos estados, en orden. Los estados de los pasos se determinan de la misma manera que el estado del trabajo.

En la siguiente lista se describen los estados:

`NOT_COMPATIBLE`

El trabajo no es compatible con la granja porque no hay flotas que puedan completar una de las tareas del trabajo.

`RUNNING`

Uno o más trabajadores están ejecutando tareas desde el trabajo. Mientras haya al menos una tarea en ejecución, la tarea estará marcada`RUNNING`.

`ASSIGNED`

A uno o más trabajadores se les asignan tareas del trabajo como siguiente acción. El entorno, si lo hay, está configurado.

`STARTING`

Uno o más trabajadores están configurando el entorno para ejecutar las tareas.

`SCHEDULED`

Las tareas del trabajo se programan para uno o más trabajadores como la siguiente acción del trabajador.

`READY`

Al menos una tarea del trabajo está lista para ser procesada.

`INTERRUPTING`

Se está interrumpiendo al menos una tarea del trabajo. Se pueden producir interrupciones al actualizar manualmente el estado del trabajo. También puede ocurrir en respuesta a una interrupción debida a cambios en el precio spot de Amazon Elastic Compute Cloud (Amazon EC2).

`FAILED`

Una o más tareas del trabajo no se completaron correctamente.

`CANCELED`

Se han cancelado una o más tareas del trabajo.

`SUSPENDED`

Se ha suspendido al menos una tarea del trabajo.

`PENDING`

Una tarea del trabajo está esperando la disponibilidad de otro recurso.

`SUCCEEDED`

Todas las tareas del trabajo se procesaron correctamente.

Modificación de trabajos en Deadline Cloud

Puede usar los siguientes `update` comandos AWS Command Line Interface (AWS CLI) para modificar la configuración de un trabajo o para establecer el estado objetivo de un trabajo, paso o tarea:

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

- `aws deadline update-task`

En los siguientes ejemplos de `update` comandos, sustituya cada uno *`user input placeholder`*por su propia información.

También puede usar el monitor de Deadline Cloud para modificar la configuración de un trabajo. Para obtener más información, consulte Vea y gestione los trabajos, los pasos y las tareas en Deadline Cloud.

Example — Volver a poner en cola un trabajo

Todas las tareas del trabajo cambian al `READY` estado, a menos que haya dependencias entre pasos. Los pasos con dependencias cambian a uno `READY` o a `PENDING` medida que se restauran.

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

Example — Cancelar un trabajo

Todas las tareas del trabajo que no tienen el estado `SUCCEEDED` o `FAILED` están marcadas`CANCELED`.

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

Example — Marcar un trabajo fallido

Todas las tareas del trabajo que tienen ese estado `SUCCEEDED` permanecen sin cambios. Todas las demás tareas están marcadas`FAILED`.

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

```
--target-task-run-status FAILED
```

Example — Marcar un trabajo como exitoso

Todas las tareas del trabajo se trasladan al SUCCEEDED estado.

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

Example — Suspender un trabajo

Las tareas del trabajo en el FAILED estado SUCCEEDEDCANCELED, o no cambian. Todas las demás tareas están marcadasSUSPENDED.

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

Example — Cambiar la prioridad de un trabajo

Actualiza la prioridad de un trabajo para cambiar el orden en que está programado. Por lo general, los trabajos de mayor prioridad se programan primero.

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

Example — Cambiar el número de tareas fallidas permitidas

Actualiza el número máximo de tareas fallidas que puede tener el trabajo antes de que se cancelen las tareas restantes.

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

```
--queue-id queueID \
--job-id jobID \
--max-failed-tasks-count 200
```

Example — Cambia el número de reintentos de tareas permitidos

Actualiza el número máximo de reintentos de una tarea antes de que se produzca un error en la tarea. Una tarea que ha alcanzado el número máximo de reintentos no se puede volver a poner en cola hasta que se aumente este valor.

```
aws deadline update-job \
--farm-id farmID \
--queue-id queueID \
--job-id jobID \
--max-retries-per-task 10
```

Example — Archivar un trabajo

Actualiza el estado del ciclo de vida del trabajo a`ARCHIVED`. Los trabajos archivados no se pueden programar ni modificar. Solo puede archivar un trabajo que se encuentre en el `SUSPENDED` estado `FAILEDCANCELED`,`SUCCEEDED`, o.

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

Example — Volver a poner en cola un paso

Todas las tareas del paso cambian al `READY` estado, a menos que haya dependencias entre pasos. Las tareas de los pasos con dependencias cambian a uno `READY` o `PENDING` varios pasos y la tarea se restaura.

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

Example — Cancelar un paso

Todas las tareas del paso que no tienen el estado `SUCCEEDED` o `FAILED` están marcadas`CANCELED`.

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

Example — Marcar un paso como fallido

Todas las tareas del paso que tienen ese estado `SUCCEEDED` permanecen sin cambios. Todas las demás tareas están marcadas`FAILED`.

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

Example — Marcar un paso como exitoso

Todas las tareas del paso están marcadas`SUCCEEDED`.

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

Example — Suspender un paso

Las tareas del paso en el `FAILED` estado `SUCCEEDED``CANCELED`, o no cambian. Todas las demás tareas están marcadas`SUSPENDED`.

```
aws deadline update-step \
--farm-id farmID \
--queue-id queueID \
```

```
--job-id jobID \
--step-id stepID \
--target-task-run-status SUSPENDED
```

Example — Cambiar el estado de una tarea

Al utilizar el comando CLI de `update-task` Deadline Cloud, la tarea cambia al estado especificado.

```
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
```

Cómo procesa Deadline Cloud los trabajos

Para procesar un trabajo, AWS Deadline Cloud utiliza la plantilla de trabajo Open Job Description (OpenJD) para determinar los recursos necesarios. Deadline Cloud selecciona a un trabajador adecuado para un escalón de entre las flotas asociadas a tu lista de espera. El trabajador seleccionado cumple con todos los atributos de capacidad necesarios para el paso.

A continuación, Deadline Cloud envía instrucciones a los trabajadores para que configuren una sesión para el paso. El software necesario para el paso debe estar disponible en la instancia de trabajo para que se ejecute el trabajo. El servicio puede abrir sesiones para varios trabajadores si la configuración de escalado de la flota tiene capacidad.

Puede configurar el software en un Amazon Machine Image (AMI) o su empleado puede cargar el software en tiempo de ejecución desde un repositorio o un administrador de paquetes. Puede usar entornos de colas, trabajos o escalones para implementar el software que prefiera.

El servicio Deadline Cloud utiliza la plantilla OpenJD para determinar los pasos necesarios para el trabajo y las tareas necesarias para cada paso. Algunos pasos dependen de otros, por lo que Deadline Cloud determina el orden en el que se deben completar los pasos. Luego, Deadline Cloud envía las tareas de cada paso a los trabajadores para que las procesen. Cuando finaliza una tarea, el servicio envía otra tarea en la misma sesión o el trabajador puede iniciar una nueva sesión.

Puede realizar un seguimiento del progreso del trabajo en el monitor de Deadline Cloud, en la interfaz de línea de comandos de Deadline Cloud (CLI de Deadline Cloud) o en AWS CLI. Para

obtener más información sobre el uso del monitor, consulteUso del monitor Deadline Cloud. Para obtener más información sobre el uso de la CLI de Deadline Cloud, consulteEstados de trabajo en la CLI de Deadline Cloud.

Una vez finalizadas todas las tareas de cada paso, el trabajo estará completo y el resultado estará listo para descargarse en su estación de trabajo. Incluso si el trabajo no ha finalizado, el resultado de cada paso y tarea que haya finalizado está disponible para su descarga.

Deadline Cloud elimina los trabajos 120 días después de su envío. Cuando se elimina un trabajo, también se eliminan todos los pasos y tareas asociados al trabajo. Si necesita volver a ejecutar el trabajo, vuelva a enviar la plantilla de OpenJD correspondiente al trabajo.

Solución de problemas de trabajos en Deadline

Para obtener información sobre los problemas más comunes con los trabajos en AWS Deadline Cloud, consulta los siguientes temas.

Temas

- ¿Por qué falló la creación de mi trabajo?
- ¿Por qué mi trabajo no es compatible?
- ¿Por qué está preparado mi trabajo pendiente?
- ¿Por qué falló mi trabajo?
- ¿Por qué está pendiente mi trámite?

¿Por qué falló la creación de mi trabajo?

Algunas de las posibles razones por las que un trabajo puede fallar en las comprobaciones de validación son las siguientes:

- La plantilla de trabajo no sigue la especificación de OpenJD.
- El trabajo contiene demasiados pasos.
- El trabajo contiene demasiadas tareas en total.
- Se ha producido un error de servicio interno que impide la creación del trabajo.

Para ver las cuotas del número máximo de pasos y tareas de un trabajo, utilice la consola Service Quotas. Para obtener más información, consulte Cuotas para Deadline Cloud.

¿Por qué mi trabajo no es compatible?

Los motivos más comunes por los que los trabajos no son compatibles con las colas son los siguientes:

- No hay ninguna flota asociada a la cola a la que se envió el trabajo. Abre el monitor de Deadline Cloud y comprueba que la cola tenga flotas asociadas. Para obtener más información sobre cómo ver las colas, consulte. Consulta los detalles de las colas y la flota en Deadline Cloud
- El trabajo tiene requisitos de alojamiento que ninguna de las flotas asociadas a la cola cumple. Para comprobarlo, compare la `hostRequirements` entrada de la plantilla de trabajo con la configuración de las flotas de su granja. Asegúrese de que una de las flotas cumpla con los requisitos del anfitrión. Para obtener más información sobre la compatibilidad de la flota, consulte. Determine la compatibilidad de la flota Para ver la configuración de la flota, consulteConsulta los detalles de las colas y la flota en Deadline Cloud.

¿Por qué está preparado mi trabajo pendiente?

Las posibles razones por las que su trabajo parece estar estancado en el `READY` estado incluyen las siguientes:

- El número máximo de trabajadores para las flotas asociadas a la cola se establece en cero. Para comprobarlo, consulte. Consulta los detalles de las colas y la flota en Deadline Cloud
- Hay un trabajo de mayor prioridad en la cola. Para comprobarlo, consulteConsulta los detalles de las colas y la flota en Deadline Cloud.
- Para las flotas administradas por el cliente, compruebe la configuración de escalado automático. Para obtener más información, consulte Amplíe automáticamente su flota de Amazon EC2 con la función de recomendación de escalado de Deadline Cloud.

¿Por qué falló mi trabajo?

Un trabajo puede fallar por muchas razones. Para buscar el problema, abre el monitor de Deadline Cloud y selecciona el trabajo que no funciona. Elija una tarea que haya fallado y, a continuación, consulte los registros de la tarea. Para ver instrucciones, consulte Vea los registros en Deadline Cloud.

- Si ve errores de licencia o si aparece una marca de agua que se debe a que el software no tiene una licencia válida, asegúrese de que el usuario pueda conectarse al servidor de licencias

necesario. Para obtener más información, consulte Connect las flotas gestionadas por el cliente a un punto final de licencia.

¿Por qué está pendiente mi trámite?

Los pasos pueden permanecer en el `PENDING` estado cuando una o más de sus dependencias no estén completas. Puedes comprobar el estado de las dependencias mediante el monitor de Deadline Cloud. Para ver instrucciones, consulte Ver un paso en Deadline Cloud.

Almacenamiento de archivos para Deadline Cloud

Los trabajadores deben tener acceso a las ubicaciones de almacenamiento que contienen los archivos de entrada necesarios para procesar un trabajo y a las ubicaciones que almacenan la salida. AWS Deadline Cloud ofrece dos opciones de ubicaciones de almacenamiento:

- Con los adjuntos de trabajo, Deadline Cloud transfiere los archivos de entrada y salida de tus trabajos entre una estación de trabajo y los trabajadores de Deadline Cloud. Para habilitar las transferencias de archivos, Deadline Cloud utiliza un depósito de Amazon Simple Storage Service (Amazon S3) en su cuenta. Cuenta de AWS

  Cuando utilizas adjuntos de trabajo con una flota de servicios gestionados, puedes configurar un sistema de archivos virtual (VFS) en tu red privada virtual (VPN). De este modo, los trabajadores pueden cargar los archivos solo cuando los necesiten.
- Con el almacenamiento compartido, utiliza el uso compartido de archivos con su sistema operativo para proporcionar acceso a los archivos.

  Al utilizar el almacenamiento compartido multiplataforma, puede crear un perfil de almacenamiento para que los trabajadores puedan mapear la ruta de acceso a los archivos entre dos sistemas operativos diferentes.

Temas

- Adjuntos de trabajo en Deadline Cloud
- Almacenamiento compartido en Deadline Cloud

Adjuntos de trabajo en Deadline Cloud

Los adjuntos de trabajo te permiten transferir archivos de un lado a otro entre tu estación de trabajo y AWS Deadline Cloud. Con los adjuntos de trabajo, no necesita configurar manualmente un bucket de Amazon S3 para sus archivos. En su lugar, cuando creas una cola con la consola de Deadline Cloud, eliges el depósito para tus adjuntos de trabajo.

La primera vez que envíes un trabajo a Deadline Cloud, todos los archivos del trabajo se transfieren a Deadline Cloud. Para envíos posteriores, solo se transfieren los archivos que han cambiado, lo que ahorra tiempo y ancho de banda.

Una vez finalizado el procesamiento, puede descargar el resultado desde la página de detalles del trabajo o mediante el `deadline job download-output` comando CLI de Deadline Cloud.

Puede usar el mismo depósito de S3 para varias colas. Defina un prefijo raíz diferente para cada cola a fin de organizar los archivos adjuntos en el depósito.

Al crear una cola con la consola, puede elegir un rol existente AWS Identity and Access Management (IAM) o hacer que la consola cree un rol nuevo. Si la consola crea el rol, establece los permisos para acceder al bucket especificado para la cola. Si eliges un rol existente, debes concederle permisos para acceder al bucket de S3.

Cifrado para los depósitos de S3 adjuntos a tareas

De forma predeterminada, los archivos adjuntos de los trabajos se cifran automáticamente en su bucket de S3. Este enfoque ayuda a proteger su información contra el acceso no autorizado. No necesita hacer nada para cifrar sus archivos con las claves proporcionadas por Deadline Cloud. Para obtener más información, consulte Amazon S3 ahora cifra automáticamente todos los objetos nuevos en la Guía del usuario de Amazon S3.

Puede utilizar su propia AWS Key Management Service clave gestionada por el cliente para cifrar el depósito de S3 que contiene los adjuntos de sus trabajos. Para ello, debe modificar la función de IAM de la cola asociada al bucket para permitir el acceso al. AWS KMS key

Para abrir el editor de políticas de IAM para la función de cola

1. Inicie sesión en la consola de Deadline Cloud AWS Management Console y ábrala. En la página principal, en la sección Cómo empezar, selecciona Ver granjas.
2. En la lista de granjas, elija la granja que contiene la cola que desee modificar.
3. En la lista de colas, elija la cola que desee modificar.
4. En la sección de detalles de la cola, elija la función de servicio para abrir la consola de IAM correspondiente a la función de servicio.

A continuación, complete el siguiente procedimiento.

Para actualizar la política de roles con permiso para AWS KMS

1. En la lista de políticas de permisos, elija la política para el rol.
2. En la sección Permisos definidos en esta política, elija Editar.

3. Elija Agregar nueva instrucción.
4. Copia y pega la siguiente política en el editor. Cambia la *RegionaccountID*, y *keyID*por tus propios valores.

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

5. Elija Siguiente.
6. Revisa los cambios de la política y, cuando estés de acuerdo, selecciona Guardar cambios.

Administrar los adjuntos de trabajos en depósitos de S3

Deadline Cloud almacena los archivos adjuntos de trabajo necesarios para su trabajo en un depósito de S3. Estos archivos se acumulan con el paso del tiempo, lo que aumenta los costes de Amazon S3. Para reducir los costos, puede aplicar una configuración del ciclo de vida de S3 a su bucket de S3. Esta configuración puede eliminar automáticamente los archivos del bucket. Como el bucket de S3 está en su cuenta, puede optar por modificar o eliminar la configuración del ciclo de vida de S3 en cualquier momento. Para obtener más información, consulte Ejemplos de configuración del ciclo de vida de S3 en la Guía del usuario de Amazon S3.

Si busca una solución de administración de buckets de S3 más detallada, puede configurar los objetos Cuenta de AWS para que caduquen en un bucket de S3 en función de la última vez que se accedió a ellos. Para obtener más información, consulte el artículo sobre la caducidad de los objetos de Amazon S3 en función de la fecha del último acceso para reducir los costes en el blog de AWS arquitectura.

Sistema de archivos virtual Deadline Cloud

El soporte del sistema de archivos virtual para adjuntar trabajos en AWS Deadline Cloud permite que el software cliente de los trabajadores se comunique directamente con Amazon Simple Storage

Service. Los trabajadores pueden cargar los archivos solo cuando los necesitan, en lugar de descargarlos todos antes de procesarlos. Los archivos se almacenan de forma local. Este enfoque evita descargar los activos utilizados más de una vez varias veces. Todos los archivos se eliminan una vez finalizado el trabajo.

- El sistema de archivos virtual proporciona un aumento significativo del rendimiento para perfiles de trabajo específicos. En general, los subconjuntos más pequeños del total de archivos con flotas de trabajadores más grandes muestran los mayores beneficios. Un número reducido de archivos con menos trabajadores tiene tiempos de procesamiento aproximadamente equivalentes.
- El soporte para sistemas de archivos virtuales solo está disponible para Linux los trabajadores de las flotas gestionadas por el servicio.
- El sistema de archivos virtual Deadline Cloud admite las siguientes operaciones, pero no es compatible con POSIX:
  - Archivo`create`,`delete`,`open`,`close`,`read`,`write`,,`append`,`truncate`,`rename`,`move`,`copy`, `statfsync`, y `falloc`
  - Directorio`create`, `deleterename`,`move`,`copy`, y `stat`
- El sistema de archivos virtual está diseñado para reducir la transferencia de datos y mejorar el rendimiento cuando las tareas solo acceden a una parte de un conjunto de datos grande, y no está optimizado para todas las cargas de trabajo. Debe probar su carga de trabajo antes de ejecutar trabajos de producción.

Habilite la compatibilidad con VFS

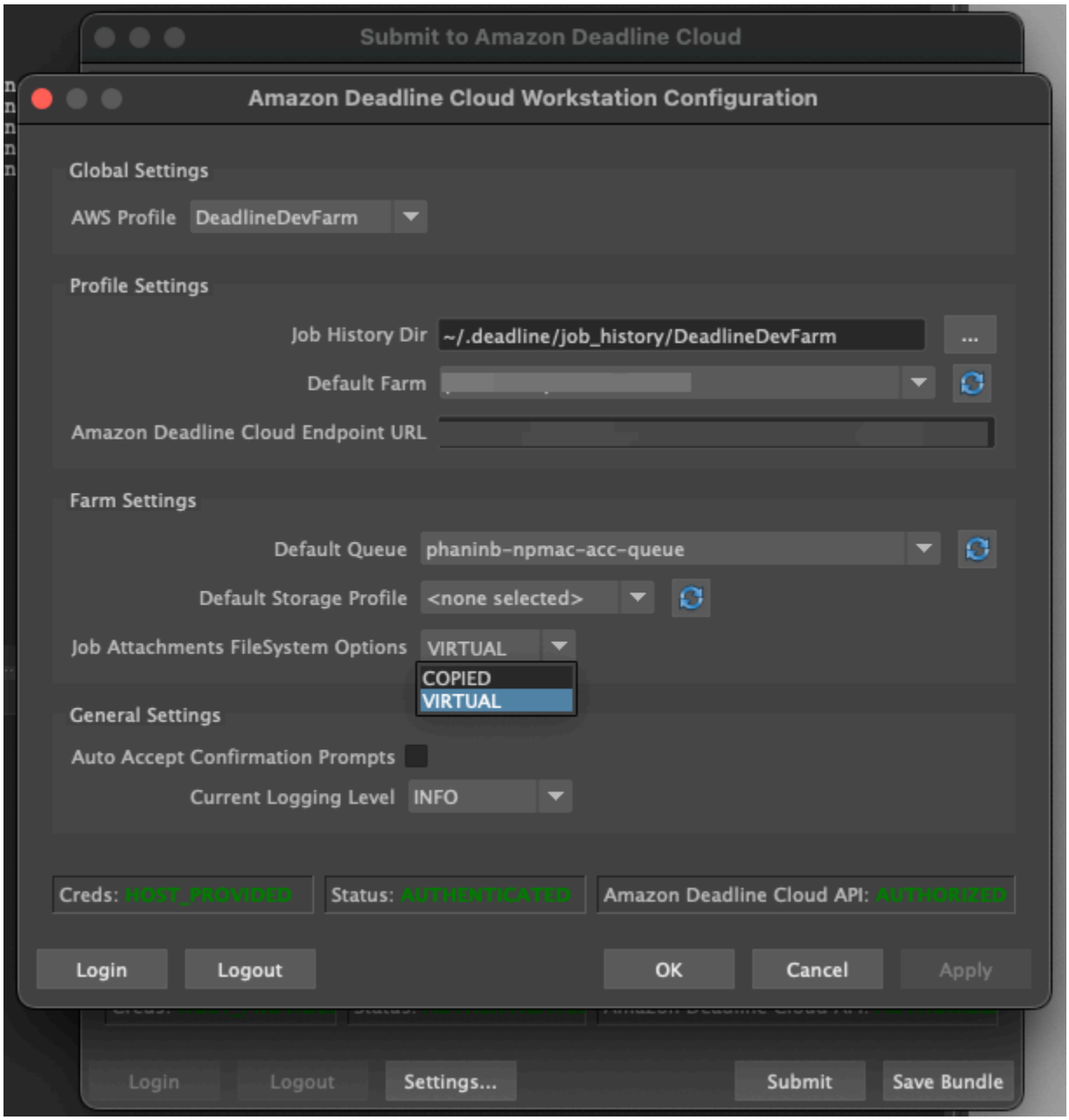
La compatibilidad con sistemas de archivos virtuales (VFS) está habilitada para cada trabajo. Un trabajo recurre al marco predeterminado de adjuntos de trabajos en los siguientes casos:

- El perfil de una instancia de trabajador no admite un sistema de archivos virtual.
- Los problemas impiden iniciar el proceso del sistema de archivos virtual.
- No se puede montar el sistema de archivos virtual.

Para habilitar la compatibilidad con el sistema de archivos virtual mediante el remitente

1. Al enviar un trabajo, pulse el botón Configuración para abrir el panel de configuración de la estación de trabajo AWS Deadline Cloud.

2. En el menú desplegable de opciones del sistema de archivos adjuntos de trabajos, elija VIRTUAL.



3. Para guardar los cambios, pulse Aceptar.

Para habilitar la compatibilidad con el sistema de archivos virtual mediante AWS CLI

- Utilice el siguiente comando al enviar un trabajo guardado:

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

Para comprobar que el sistema de archivos virtual se ha iniciado correctamente para una tarea concreta, revise sus registros en Amazon CloudWatch Logs. Busque los siguientes mensajes:

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

Si el registro contiene el siguiente mensaje, la compatibilidad con el sistema de archivos virtual está deshabilitada:

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

Solución de problemas: soporte para sistemas de archivos virtuales

Puede ver los registros de su sistema de archivos virtual mediante el monitor de Deadline Cloud. Para ver instrucciones, consulte Vea los registros en Deadline Cloud.

Los registros del sistema de archivos virtual también se envían al grupo de CloudWatch registros que está asociado a la cola compartida con la salida del agente de trabajo.

Almacenamiento compartido en Deadline Cloud

Para usar el almacenamiento compartido, los trabajadores usan el sistema de intercambio de archivos del sistema operativo para acceder a un espacio de almacenamiento compartido para la entrada y salida de sus trabajos.

El método real que utilice para compartir archivos depende del sistema operativo y de la forma en que implemente el almacenamiento compartido en la red. Usted es responsable de configurar el uso compartido de archivos y de garantizar que satisfaga sus necesidades.

Si utiliza una solución para compartir archivos entre sistemas, puede utilizar perfiles de almacenamiento para mapear las ubicaciones de los archivos entre Linux los distintos sistemas de Windows archivos.

Perfiles de almacenamiento en Deadline Cloud

Un perfil de almacenamiento te permite configurar granjas mediante almacenamiento compartido multiplataforma. Un perfil de almacenamiento mapea las rutas entre los sistemas operativos para los trabajos procesados en trabajadores con un sistema operativo diferente al de la estación de trabajo desde la que se enviaron.

Los perfiles de almacenamiento son necesarios cuando se utiliza una flota gestionada por el cliente con una combinación de sistemas operativos entre estaciones de trabajo y trabajadores. Los perfiles de almacenamiento no son compatibles con las flotas gestionadas por el servicio.

Tras crear un perfil de almacenamiento, debe conceder acceso a las colas y flotas que utilizan el perfil.

Para crear un perfil de almacenamiento

1. Abre la consola de Deadline Cloud.
2. En Comenzar, selecciona Ir al panel de Deadline Cloud.
3. Elige una granja y, a continuación, selecciona la pestaña Perfiles de almacenamiento.
4. Selecciona Crear perfil de almacenamiento.
5. Elija un sistema operativo en el menú desplegable.
6. Proporcione un nombre para el perfil. Un nombre claro le ayuda a elegir el perfil de almacenamiento que se utilizará al enviar los trabajos.
7. Para el nombre de la ruta, introduzca la ubicación raíz de los datos del trabajo en la estación de trabajo desde la que envía los trabajos.
8. Elija un tipo de almacenamiento:
   - Local se refiere a las ubicaciones de los archivos que no comparten el trabajador y la estación de trabajo. Se cargan como archivos adjuntos de trabajo.
   - Compartido se refiere al almacenamiento que comparten el trabajador y la estación de trabajo. Los archivos del almacenamiento compartido no se cargan como adjuntos de trabajo.
9. Proporcione una ruta de ubicación del sistema de archivos. Este es el directorio raíz de los datos de su trabajo.
10. Seleccione Crear.

Tras crear un perfil de almacenamiento, debe modificar las colas y las flotas gestionadas por los clientes para utilizar el nuevo perfil. Para permitir el acceso a un perfil de almacenamiento, utilice el siguiente procedimiento después de completar el procedimiento anterior.

Para permitir que las colas y las flotas gestionadas por los clientes utilicen un perfil de almacenamiento

1. Seleccione la pestaña Colas o Flotas.

2. Elija la cola o la flota que desee modificar.
3. Seleccione Modificar perfiles de almacenamiento.
4. Seleccione el perfil de almacenamiento que desee permitir y las ubicaciones del sistema de archivos de ese perfil.
5. Elija Guardar cambios.

Administrar los presupuestos y el uso de Deadline Cloud

El administrador de presupuesto y el explorador de uso de AWS Deadline Cloud son herramientas de administración de costos que proporcionan el costo aproximado de usar Deadline Cloud en función de la información disponible sobre las variables de costo. Las herramientas de gestión de costes no garantizan el importe adeudado por el uso real de Deadline Cloud y otros AWS servicios.

Para ayudarte a gestionar los costes de Deadline Cloud, puedes utilizar las siguientes funciones:

- Gestor de presupuestos: con el gestor de presupuestos de Deadline Cloud, puedes crear y editar presupuestos para ayudarte a gestionar los costes del proyecto.
- Explorador de uso: con el explorador de uso de Deadline Cloud, puedes ver cuántos AWS recursos se utilizan y los costos estimados de esos recursos.

Hipótesis de costes

El cálculo básico que utilizan las herramientas de gestión de costes de Deadline Cloud es:

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

- El tiempo de ejecución es la suma de todas las tareas de un trabajo, desde la hora de inicio hasta la hora de finalización.
- La tasa de cómputo viene determinada por los precios de AWS Deadline Cloud para las flotas con servicios gestionados. En el caso de las flotas gestionadas por los clientes, la tarifa de cálculo se estima en 1 dólar por hora de trabajo.
- La tarifa de licencia viene determinada por el precio base de la licencia de Deadline Cloud. Los niveles adicionales no están incluidos. Para obtener más información sobre los precios de las licencias, consulta los precios de AWS Deadline Cloud.

La estimación de costos de las herramientas de administración de costos de Deadline Cloud puede variar de sus costos reales por varios motivos. Las razones más comunes incluyen:

- Los recursos propiedad del cliente y sus precios. Puede optar por utilizar sus propios recursos, ya sea desde AWS o desde fuera de las instalaciones o de otros proveedores de nube. Los costos reales de estos recursos no se calculan.
- Costes de los trabajadores inactivos. En el caso de las flotas con un recuento mínimo de instancias superior a cero, los trabajadores inactivos no se tienen en cuenta en los cálculos.
- Créditos promocionales, descuentos y acuerdos de precios personalizados. Las herramientas de administración de costos no tienen en cuenta los créditos promocionales, los acuerdos de precios privados ni otros descuentos. Es posible que reúna los requisitos para obtener otros descuentos que no forman parte de la estimación.
- Almacenamiento de activos. El almacenamiento de activos no está incluido en las estimaciones de costo y uso.
- Cambios en el precio. AWS ofrece pay-as-you-go precios para la mayoría de los servicios. Los precios pueden cambiar con el tiempo. Las herramientas de gestión de costes son las que utilizan la mayoría de up-to-date los precios disponibles públicamente, pero es posible que se produzcan retrasos tras los cambios.
- Impuestos. Las herramientas de gestión de costes no incluyen los impuestos que se aplican a la compra del servicio.
- Redondeo. La herramienta de gestión de costes realiza un redondeo matemático de los datos de precios.
- Moneda. Las estimaciones de costos se realizan en dólares estadounidenses. Los tipos de cambio globales varían con el tiempo. Si convierte las estimaciones a una base de divisa diferente en el tipo de cambio actual, los cambios en el tipo de cambio afectarán a la estimación.
- Licencias externas. Si eliges usar licencias preadquiridas (trae tu propia licencia), las herramientas de administración de costos de Deadline Cloud no pueden contabilizar este costo.

Uso del gestor de presupuestos de Deadline Cloud

El gestor de presupuestos de Deadline Cloud te ayuda a controlar el gasto en un recurso determinado, como una cola, una flota o una granja. Puedes crear importes y límites presupuestarios y establecer acciones automatizadas para ayudar a reducir o detener los gastos adicionales con respecto al presupuesto.

En las siguientes secciones, se indican los pasos para utilizar el gestor de presupuestos de Deadline Cloud.

Temas

- Requisito previo
- Acceda al administrador de presupuestos
- Creación de un presupuesto
- Ver un presupuesto
- Editar un presupuesto
- Desactiva un presupuesto

Requisito previo

Para utilizar el gestor de presupuestos de Deadline Cloud, debes tener un nivel de `OWNER` acceso. Para conceder el `OWNER` permiso, sigue los pasos que se indicanAdministrar usuarios en Deadline Cloud.

Acceda al administrador de presupuestos

Para acceder al administrador de presupuestos de Deadline Cloud, utilice el siguiente procedimiento.

1. Inicie sesión en la consola de Deadline Cloud AWS Management Console y ábrala.
2. Selecciona Ver granjas.
3. Localice la granja sobre la que desee obtener información y, a continuación, seleccione Administrar trabajos. El monitor de Deadline Cloud se abre en una pestaña nueva.
4. En el monitor de Deadline Cloud, en el panel de navegación izquierdo, selecciona Presupuestos.

La página de resumen del gestor de presupuestos muestra una lista de los presupuestos activos e inactivos:

- Los presupuestos activos se comparan con el recurso seleccionado (una cola).
- Los presupuestos inactivos han caducado o han sido cancelados por un usuario y ya no permiten hacer un seguimiento de los costes con respecto a los límites de este presupuesto.

Después de elegir un presupuesto, la página de resumen del presupuesto contiene información básica sobre el presupuesto. La información proporcionada incluye el nombre del presupuesto, el estado, los recursos, el porcentaje restante, el importe restante, el presupuesto total, la fecha de inicio y la fecha de finalización.

Creación de un presupuesto

Para crear un presupuesto, utilice el siguiente procedimiento.

1. Si aún no lo ha hecho, inicie sesión en la consola de Deadline Cloud AWS Management Console, abra la consola de Deadline Cloud, elija una granja y, a continuación, elija Administrar trabajos.
2. En la página del administrador de presupuestos, selecciona Crear presupuesto.
3. En la sección de detalles, introduce un nombre de presupuesto para el presupuesto.
4. (Opcional) En el campo de descripción, introduce una descripción breve y clara del presupuesto.
5. En Recurso, elija el menú desplegable de colas para buscar y seleccionar la cola para la que desea crear un presupuesto.
6. En Período, establece la fecha de inicio y finalización del presupuesto siguiendo estos pasos:

   a. En Fecha de inicio, introduzca la primera fecha del seguimiento del presupuesto en formato AAAA/MM/DD, o bien elija el icono del calendario y seleccione una fecha.

      La fecha de inicio predeterminada es la fecha en que se creó el presupuesto.

   b. En Fecha de finalización, introduzca la última fecha del seguimiento del presupuesto en formato AAAA/MM/DD o elija el icono del calendario y seleccione una fecha.

      La fecha de finalización predeterminada es de 120 días a partir de la fecha de inicio.
7. En Importe presupuestario, introduzca el importe en dólares del presupuesto.
8. (Opcional) Le recomendamos que cree alertas de límite. En la sección Limitar las acciones, puedes implementar acciones automatizadas que se produzcan cuando queden importes específicos en el presupuesto. Para ello, siga los pasos que se describen a continuación:

   a. Selecciona Añadir nueva acción.

   b. En Importe restante, introduce el importe en dólares con el que deseas iniciar la acción.

   c. En el menú desplegable Acción, elige la acción que desees. Las acciones incluyen:

      - Interrumpir después de terminar el trabajo actual: todo el trabajo que se esté ejecutando en ese momento cuando se alcance el importe límite seguirá ejecutándose (e incurrirá en costes) hasta su finalización.
      - Interrumpir inmediatamente el trabajo: todo el trabajo se cancela inmediatamente cuando se alcanza el importe límite.

d. Para crear alertas de límite adicionales, selecciona Añadir nueva acción y repite los dos pasos anteriores.

9. Seleccione Crear presupuesto. Aparece la página del administrador de presupuestos. El presupuesto recién creado aparece en la pestaña Presupuestos activos.

Ver un presupuesto

Después de crear un presupuesto, puede verlo en la página del administrador de presupuestos. Desde allí, puedes ver el importe total del presupuesto y el coste total asignado al presupuesto específico.

Para ver un presupuesto, utilice el siguiente procedimiento.

1. Si aún no lo has hecho, inicia sesión en la consola de Deadline Cloud AWS Management Console, abre la consola de Deadline Cloud, elige una granja y, a continuación, selecciona Administrar trabajos.
2. Selecciona Presupuestos en el panel de navegación de la izquierda. Aparece la página Gestor de presupuestos.
3. Para ver un presupuesto activo, seleccione la pestaña Presupuestos activos y elija el nombre del presupuesto que desea ver. Aparece la página de detalles del presupuesto.
4. Para ver los detalles del presupuesto de un presupuesto vencido, seleccione la pestaña Presupuestos inactivos. A continuación, elija el nombre del presupuesto que desee ver. Aparece la página de detalles del presupuesto.

Editar un presupuesto

Puede editar cualquier presupuesto activo. Para editar un presupuesto activo, utilice el siguiente procedimiento.

1. Si aún no lo ha hecho, inicie sesión en la consola de Deadline Cloud AWS Management Console, abra la consola de Deadline Cloud, elija una granja y, a continuación, elija Administrar trabajos.
2. En la página del gestor de presupuestos, en la pestaña Presupuestos activos, selecciona el botón situado junto al presupuesto que quieres editar.
3. En el menú desplegable Acciones de la esquina superior derecha, selecciona Editar presupuesto.

4. Realiza los cambios que desees y, a continuación, selecciona Actualizar presupuesto.

Desactiva un presupuesto

Puede desactivar cualquier presupuesto activo. Al desactivar un presupuesto, su estado cambia de Activo a Inactivo. Cuando se desactiva un presupuesto, deja de realizar un seguimiento de un recurso hasta el importe de ese presupuesto.

Para desactivar un presupuesto, utilice el siguiente procedimiento.

1. Si aún no lo has hecho, inicia sesión en la consola de Deadline Cloud AWS Management Console, abre la consola de Deadline Cloud, elige una granja y, a continuación, selecciona Administrar trabajos.
2. En la página del administrador de presupuestos, en la pestaña Presupuestos activos, selecciona el botón situado junto al presupuesto que quieres desactivar.
3. En el menú desplegable Acciones de la esquina superior derecha, selecciona Desactivar el presupuesto. En unos instantes, el presupuesto seleccionado pasará de activo a inactivo y pasará de la pestaña Presupuestos activos a la pestaña Presupuestos inactivos.

Uso del explorador de uso de Deadline Cloud

Con el explorador de uso de Deadline Cloud, puedes ver las métricas en tiempo real de la actividad que se lleva a cabo en cada granja. Puedes analizar los costos de la granja por diferentes variables, como la cola, el trabajo, la licencia, el producto o el tipo de instancia. Selecciona varios periodos de tiempo para ver el uso durante un período de tiempo específico y observa las tendencias de uso a lo largo del tiempo. También puedes ver un desglose detallado de los puntos de datos seleccionados, lo que te permitirá analizar más de cerca las métricas. El uso se puede mostrar por tiempo (minutos y horas) o por costo (USD).

En las siguientes secciones, se muestran los pasos para acceder y utilizar el explorador de uso de Deadline Cloud.

Temas

- Requisito previo
- Abre el explorador de uso
- Usa el explorador de uso

Requisito previo

Para usar el explorador de uso de Deadline Cloud, debes tener uno `MANAGER` o varios permisos de `OWNER` granja. Para obtener más información, consulte Administre los usuarios y grupos de granjas, colas y flotas.

Abre el explorador de uso

Para abrir el explorador de uso de Deadline Cloud, utilice el siguiente procedimiento.

1. Inicie sesión en la consola de Deadline Cloud AWS Management Console y ábrala.
2. Para ver todas las granjas disponibles, selecciona Ver granjas.
3. Localice la granja sobre la que desee obtener información y, a continuación, seleccione Administrar trabajos. El monitor de Deadline Cloud se abre en una pestaña nueva.
4. En el monitor de Deadline Cloud, en el menú de la izquierda, selecciona el explorador de usos.

Usa el explorador de uso

En la página del explorador de uso, puede seleccionar parámetros específicos en los que se pueden mostrar los datos. De forma predeterminada, se muestra el uso total en tiempo (horas y minutos) de los últimos 7 días. Puede cambiar estos parámetros y la información que se muestra cambia de forma dinámica en función de la configuración de los parámetros.

Puede agrupar los resultados en función de la cola, el trabajo, el uso informático, el tipo de instancia o el producto de licencia. Si elige un producto de licencia, los costos se calculan para licencias específicas. Para todos los demás grupos, el tiempo se calcula sumando el tiempo que tarda cada tarea en ejecutarse.

El explorador de uso devuelve solo 100 resultados en función de los criterios de filtro que establezca. Los resultados se muestran en orden descendente según la fecha y hora de creación. Si hay más de 100 resultados, aparecerá un mensaje de error. Puede refinar la consulta para reducir el número de resultados:

- Seleccione un intervalo de tiempo más pequeño
- Selecciona menos colas
- Seleccione un grupo diferente, como agrupar por cola en lugar de por trabajo

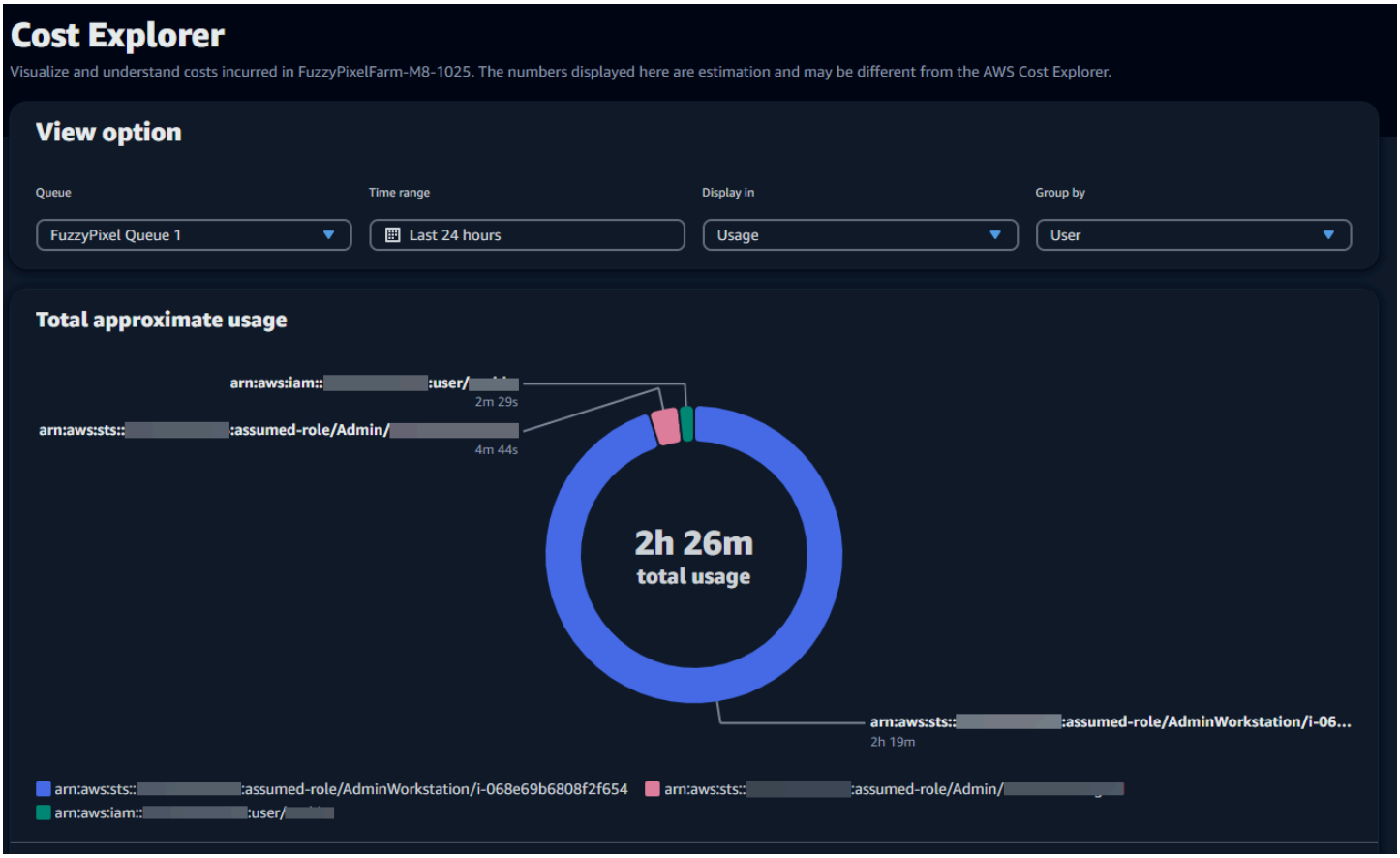
Temas

- Utilice gráficos visuales para revisar los datos
- Vea un desglose de las métricas
- Vea el tiempo de ejecución aproximado de las colas

Utilice gráficos visuales para revisar los datos

Puede revisar los datos en un formato visual para identificar tendencias y posibles áreas que podrían necesitar más análisis o atención. El explorador de uso ofrece un gráfico circular que muestra el uso y el costo generales con la opción de agrupar los totales en subtotales más pequeños.

> **Note**
>
> El gráfico solo muestra los cinco resultados principales, junto con los demás resultados combinados en una sección denominada «otros». Puedes ver todos los resultados en la sección de desglose situada debajo del gráfico.



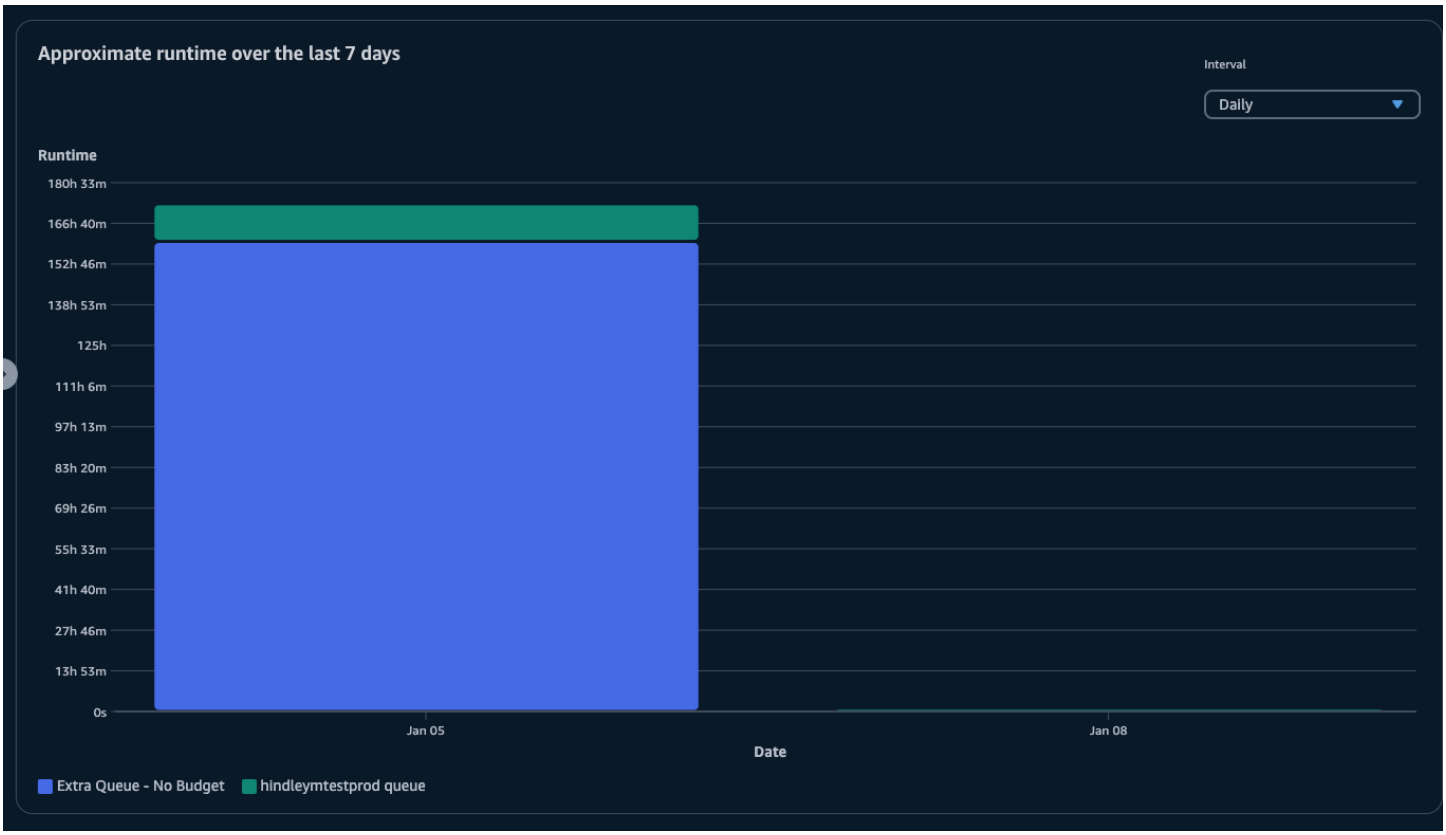
Vea un desglose de las métricas

Debajo del gráfico circular, el explorador de uso ofrece un desglose más detallado de métricas específicas, que cambiarán a medida que cambien los parámetros. De forma predeterminada, se muestran cinco resultados en el explorador de uso. Puedes desplazarte por los resultados con las flechas de paginación de la sección de desglose.

El desglose se minimiza de forma predeterminada. Para expandir y mostrar los resultados, seleccione la flecha Ver todo el desglose. Para descargar el desglose, selecciona Descargar datos.

Vea el tiempo de ejecución aproximado de las colas

También puede ver el tiempo de ejecución aproximado de las colas en función de los distintos intervalos que especifique. Las opciones de intervalo son por hora, por día, por semana y por mes. Tras seleccionar un intervalo, el gráfico muestra el tiempo de ejecución aproximado de las colas.



Administración de costos

AWS Deadline Cloud proporciona presupuestos y un explorador de uso para ayudarte a controlar y visualizar los costes de tus trabajos. Sin embargo, Deadline Cloud utiliza otros AWS servicios, como

Amazon S3. Los costos de esos servicios no se reflejan en los presupuestos de Deadline Cloud ni en el explorador de uso y se cobran por separado en función del uso. Según cómo configure Deadline Cloud, puede utilizar los siguientes AWS servicios, entre otros:

Servicio	Página de precios
Amazon CloudWatch Logs	Precios de Amazon CloudWatch Logs
Amazon Elastic Compute Cloud	Precios de Amazon Elastic Compute Cloud
AWS Key Management Service	Precios de AWS Key Management Service
AWS PrivateLink	Precios de AWS PrivateLink
Amazon Simple Storage Service	Precios de Amazon Simple Storage Service
Amazon Virtual Private Cloud	Precios de Amazon Virtual Private Cloud

Mejores prácticas de administración de costos

El uso de las siguientes prácticas recomendadas puede ayudarle a comprender y controlar sus costos al usar Deadline Cloud y las compensaciones que puede hacer entre costo y eficiencia.

> **Note**
>
> El costo final de usar Deadline Cloud depende de la interacción entre varios AWS servicios, de la cantidad de trabajo que procese y del Región de AWS lugar en el que ejecute sus trabajos. Las siguientes prácticas recomendadas son directrices y es posible que no reduzcan los costes de forma significativa.

Prácticas recomendadas para los CloudWatch registros

Deadline Cloud envía los registros de los trabajadores y las tareas a CloudWatch Logs. Se le cobrará por recopilar, almacenar y analizar estos registros. Puede reducir los costes registrando solo la cantidad mínima de datos necesaria para supervisar sus tareas.

Al crear una cola o una flota, Deadline Cloud crea un grupo de CloudWatch registros con los siguientes nombres:

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

De forma predeterminada, estos registros nunca caducan. Puede ajustar la política de retención de los grupos de registros para eliminar los registros antiguos y ayudar a reducir los costes de almacenamiento. También puede exportar registros a Amazon S3. Los costes de almacenamiento de Amazon S3 son más bajos que los de CloudWatch. Para obtener más información, consulte Exportación de datos de registro a Amazon S3.

Prácticas recomendadas de Amazon EC2

Puede utilizar instancias de Amazon EC2 tanto para flotas gestionadas por el servicio como para las gestionadas por el cliente. Hay tres consideraciones:

- En el caso de las flotas gestionadas por el servicio, puede optar por tener una o más instancias disponibles en todo momento estableciendo el número mínimo de trabajadores de la flota. Si estableces el número mínimo de trabajadores por encima de 0, la flota siempre tendrá esa cantidad de trabajadores en activo. Esto puede reducir el tiempo que tarda Deadline Cloud en empezar a procesar los trabajos; sin embargo, se te cobrará por el tiempo de inactividad de la instancia.
- Para las flotas gestionadas por el servicio, establece un tamaño máximo para la flota. Esto limita la cantidad de instancias a las que una flota puede escalar automáticamente. Las flotas no superarán este tamaño aunque haya más trabajos pendientes de ser procesados.
- Tanto para las flotas gestionadas por el servicio como para las gestionadas por el cliente, puede especificar los tipos de instancias de Amazon EC2 en sus flotas. El uso de instancias más pequeñas cuesta menos por minuto, pero completar un trabajo puede llevar más tiempo. Por el contrario, una instancia más grande cuesta más por minuto, pero puede reducir el tiempo necesario para completar un trabajo. Entender las exigencias que sus trabajos imponen a una instancia puede ayudarle a reducir los costes.
- Cuando sea posible, elija instancias Amazon EC2 Spot para su flota. Las instancias puntuales están disponibles a un precio reducido, pero las solicitudes a pedido pueden interrumpirlas. Las instancias bajo demanda se cobran por segundo y no se interrumpen.

Prácticas recomendadas para AWS KMS

De forma predeterminada, Deadline Cloud cifra tus datos con una clave AWS propia. No se le cobrará por esta clave.

Puede optar por utilizar una clave gestionada por el cliente para cifrar sus datos. Cuando utilizas tu propia clave, se te cobrará en función de cómo se utilice la clave. Si utilizas una clave existente, se cobrará un coste adicional por el uso adicional.

Mejores prácticas para AWS PrivateLink

Puede usarlo AWS PrivateLink para crear una conexión entre su VPC y Deadline Cloud mediante un punto final de interfaz. Al crear una conexión, puede llamar a todas las acciones de la API de Deadline Cloud. Se le cobrará por hora por cada punto de conexión que cree. Si lo usa PrivateLink, debe crear al menos tres puntos de conexión y, según la configuración, es posible que necesite hasta cinco.

Prácticas recomendadas para Amazon S3

Deadline Cloud usa Amazon S3 para almacenar activos para su procesamiento, adjuntos de trabajos, resultados y registros. Para reducir los costes asociados a Amazon S3, reduzca la cantidad de datos que almacena. Algunas sugerencias:

- Almacene únicamente los activos que estén en uso actualmente o que se vayan a utilizar en breve.
- Utilice una configuración de ciclo de vida de S3 para eliminar automáticamente los archivos no utilizados de un bucket de S3.

Prácticas recomendadas para Amazon VPC

Cuando utilizas licencias basadas en el uso para tu flota gestionada por el cliente, creas un punto de enlace de licencia de Deadline Cloud, que es un punto de enlace de Amazon VPC creado en tu cuenta. A este punto de conexión se le cobra una tarifa por hora. Para reducir los costes, elimine los puntos finales cuando no utilice licencias basadas en el uso.

Seguridad en Deadline Cloud

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que se ejecuta Servicios de AWS en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de cumplimiento aplicables AWS Deadline Cloud, consulte Servicios de AWS Alcance by Compliance Servicios de AWS .
- Seguridad en la nube: su responsabilidad viene determinada por lo Servicio de AWS que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Deadline Cloud. Los siguientes temas muestran cómo configurarlo Deadline Cloud para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros Servicios de AWS que le ayuden a supervisar y proteger sus Deadline Cloud recursos.

Temas

- Protección de datos en Deadline Cloud
- Identity and Access Management en Deadline Cloud
- Validación de conformidad para Deadline Cloud
- Resiliencia en Deadline Cloud
- Seguridad de la infraestructura en Deadline Cloud
- Análisis de configuración y vulnerabilidad en Deadline Cloud
- Prevención de la sustitución confusa entre servicios
- Acceda AWS Deadline Cloud mediante un punto final de interfaz (AWS PrivateLink)
- Prácticas recomendadas de seguridad para Deadline Cloud

Protección de datos en Deadline Cloud

El modelo de responsabilidad AWS compartida modelo se aplica a la protección de datos en AWS Deadline Cloud. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja Deadline Cloud o Servicios de AWS utiliza la consola, la API o los SDK. AWS CLI AWS Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o

diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya la información de las credenciales en la URL para validar la solicitud para ese servidor.

Temas

- Cifrado en reposo
- Cifrado en tránsito
- Administración de claves
- Privacidad del tráfico entre redes
- Optar por no participar

Cifrado en reposo

AWS Deadline Cloud protege los datos confidenciales cifrándolos en reposo mediante claves de cifrado almacenadas en AWS Key Management Service ()AWS KMS. El cifrado en reposo está disponible en todos los Regiones de AWS lugares donde Deadline Cloud esté disponible.

El cifrado de datos significa que un usuario o una aplicación no pueden leer los datos confidenciales guardados en los discos sin una clave válida. Solo una parte con una clave gestionada válida puede descifrar los datos.

Para obtener información sobre cómo se Deadline Cloud utiliza AWS KMS el cifrado de datos en reposo, consulte. Administración de claves

Cifrado en tránsito

Para los datos en tránsito, AWS Deadline Cloud utiliza Transport Layer Security (TLS) 1.2 o 1.3 para cifrar los datos enviados entre el servicio y los trabajadores. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3. Además, si utiliza una nube privada virtual (VPC), puede utilizarla AWS PrivateLink para establecer una conexión privada entre su VPC y. Deadline Cloud

Administración de claves

Al crear una granja nueva, puede elegir una de las siguientes claves para cifrar los datos de la granja:

- AWS clave KMS propia: tipo de cifrado predeterminado si no especificas una clave al crear la granja. La clave KMS es propiedad de AWS Deadline Cloud. No puede ver, administrar ni usar las claves AWS propias. Sin embargo, no es necesario que realices ninguna acción para proteger las

claves que cifran tus datos. Para obtener más información, consulta las claves AWS propias en la guía para AWS Key Management Service desarrolladores.

- Clave de KMS gestionada por el cliente: al crear una granja, se especifica una clave gestionada por el cliente. Todo el contenido de la granja se cifra con la clave KMS. La clave se almacena en su cuenta y es usted quien la crea, es de su propiedad y la administra, por lo que se aplican AWS KMS cargos. Usted controla plenamente la clave KMS. Puede realizar tareas como las siguientes:
  - Establecer y mantener políticas clave
  - Establecer y mantener concesiones y políticas de IAM
  - Habilitar y deshabilitar políticas de claves
  - Agregar etiquetas.
  - Crear alias de clave

  No se puede rotar manualmente una clave propiedad del cliente que se utiliza en una Deadline Cloud granja. Se admite la rotación automática de la llave.

  Para obtener más información, consulte las claves propiedad del cliente en la Guía para AWS Key Management Service desarrolladores.

  Para crear una clave gestionada por el cliente, sigue los pasos para crear claves simétricas gestionadas por el cliente que se indican en la Guía para AWS Key Management Service desarrolladores.

¿Cómo Deadline Cloud usar AWS KMS las subvenciones?

Deadline Cloud requiere una concesión para utilizar la clave gestionada por el cliente. Cuando crea una granja cifrada con una clave gestionada por el cliente, Deadline Cloud crea una concesión en su nombre enviando una `CreateGrant` solicitud AWS KMS para obtener acceso a la clave KMS que especificó.

Deadline Cloud utiliza varias concesiones. Cada subvención es utilizada por una parte diferente Deadline Cloud que necesita cifrar o descifrar sus datos. Deadline Cloud también utiliza subvenciones para permitir el acceso a otros AWS servicios utilizados para almacenar datos en su nombre, como Amazon Simple Storage Service, Amazon Elastic Block Store o OpenSearch.

Las subvenciones que permiten Deadline Cloud gestionar las máquinas de una flota gestionada por un servicio incluyen un número de Deadline Cloud cuenta y una función en el centro del servicio, en `GranteePrincipal` lugar de un director de servicio. Si bien no es habitual, esto es necesario para

cifrar los volúmenes de Amazon EBS para los trabajadores de las flotas gestionadas por el servicio mediante la clave de KMS gestionada por el cliente especificada para la granja.

Política de claves administradas por el cliente

Las políticas de clave controlan el acceso a la clave administrada por el cliente. Cada clave debe tener exactamente una política de claves que contenga instrucciones que determinen quién puede usar la clave y cómo puede usarla. Al crear la clave gestionada por el cliente, puede especificar una política clave. Para obtener más información, consulte Administración del acceso a las claves en la Guía para desarrolladores de AWS Key Management Service .

Política de IAM mínima para CreateFarm

Para usar la clave administrada por el cliente para crear granjas mediante la consola o la operación de `CreateFarm` API, deben estar permitidas las siguientes operaciones de AWS KMS API:

- `kms:CreateGrant`: añade una concesión a una clave administrada por el cliente. Concede acceso a la consola a una AWS KMS clave específica. Para obtener más información, consulta Cómo usar las subvenciones en la guía para AWS Key Management Service desarrolladores.
- `kms:Decrypt`— Permite Deadline Cloud descifrar los datos de la granja.
- `kms:DescribeKey`— Proporciona los detalles clave gestionados por el cliente Deadline Cloud para permitir su validación.
- `kms:GenerateDataKey`— Permite cifrar Deadline Cloud los datos mediante una clave de datos única.

La siguiente declaración de política otorga los permisos necesarios para la `CreateFarm` operación.

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

Política de IAM mínima para operaciones de solo lectura

Utilizar la clave gestionada por el cliente para Deadline Cloud operaciones de solo lectura, como obtener información sobre granjas, colas y flotas. Deben permitirse las siguientes operaciones AWS KMS de API:

- `kms:Decrypt`— Permite Deadline Cloud descifrar los datos de la granja.
- `kms:DescribeKey`— Proporciona los detalles clave gestionados por el cliente Deadline Cloud para permitir su validación.

La siguiente declaración de política otorga los permisos necesarios para las operaciones de solo lectura.

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

```
}
```

Política de IAM mínima para las operaciones de lectura-escritura

Utilizar la clave gestionada por el cliente para Deadline Cloud operaciones de lectura-escritura, como la creación y actualización de granjas, colas y flotas. Deben permitirse las siguientes operaciones AWS KMS de API:

- `kms:Decrypt`— Permite Deadline Cloud descifrar los datos de la granja.
- `kms:DescribeKey`— Proporciona los detalles clave gestionados por el cliente Deadline Cloud para permitir su validación.
- `kms:GenerateDataKey`— Permite cifrar Deadline Cloud los datos mediante una clave de datos única.

La siguiente declaración de política otorga los permisos necesarios para la `CreateFarm` operación.

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

Supervisión de sus claves de cifrado

Cuando utilizas una clave gestionada por el AWS KMS cliente en tus Deadline Cloud granjas, puedes utilizar AWS CloudTrailAmazon CloudWatch Logs para realizar un seguimiento de las solicitudes que se Deadline Cloud envían a AWS KMS.

CloudTrail evento de concesión de subvenciones

El siguiente CloudTrail evento de ejemplo se produce cuando se crean las concesiones, normalmente cuando se llama a la `CreateFleet` operación `CreateFarmCreateMonitor`, o.


```
{
    "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-abcdef12345678900987654321fedcba",
                "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 evento de descifrado

El siguiente CloudTrail evento de ejemplo se produce al descifrar valores mediante la clave KMS administrada por el cliente.

```
{
    "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-abcdef1234567890098765432 1fedcba",
            "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 evento de cifrado

El siguiente CloudTrail evento de ejemplo se produce al cifrar valores mediante la clave KMS administrada por el cliente.


```
{
    "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"
}
```


Eliminar una clave KMS administrada por el cliente

Eliminar una clave de KMS gestionada por el cliente en AWS Key Management Service (AWS KMS) es destructivo y potencialmente peligroso. Elimina el material de claves y todos los metadatos asociados con la clave. Esta acción es irreversible. Una vez que se elimina una clave KMS

administrada por el cliente, ya no puede descifrar los datos que se habían cifrado con ella. Esto significa que los datos se vuelven irrecuperables.

Por eso, los AWS KMS clientes tienen un período de espera de hasta 30 días antes de eliminar la clave KMS. El periodo de espera predeterminado es de 30 días.

Acerca del período de espera

Dado que eliminar una clave de KMS gestionada por el cliente es destructivo y potencialmente peligroso, te pedimos que establezcas un período de espera de 7 a 30 días. El periodo de espera predeterminado es de 30 días.

Sin embargo, el período de espera real puede ser hasta 24 horas más largo que el período que programaste. Para obtener la fecha y la hora reales en las que se eliminará la clave, utilice la DescribeKeyoperación. O en la consola AWS KMS, en la página de detalles para la clave, en la sección Configuración general, consulte la eliminación programada. Fíjese en la zona horaria.

Durante el periodo de espera, el estado de la clave administrada por el cliente y el estado de la clave es Eliminación pendiente.

- Una clave KMS administrada por el cliente que está pendiente de eliminación no puede utilizarse en ninguna operación criptográfica.
- AWS KMS no rota las claves de respaldo de las claves de KMS administradas por el cliente que están pendientes de ser eliminadas.

Para obtener más información sobre cómo eliminar una clave KMS administrada por el cliente, consulte Eliminar las claves maestras del cliente en la Guía para AWS Key Management Service desarrolladores.

Privacidad del tráfico entre redes

AWS Deadline Cloud es compatible con Amazon Virtual Private Cloud (Amazon VPC) para proteger las conexiones. Amazon VPC ofrece características que puede utilizar para aumentar y monitorear la seguridad de su nube privada virtual (VPC):

Puede configurar una flota gestionada por el cliente (CMF) con instancias de Amazon Elastic Compute Cloud (Amazon EC2) que se ejecuten dentro de una VPC. Al implementar los puntos de enlace de Amazon VPC para su uso AWS PrivateLink, el tráfico entre los trabajadores de su CMF y el Deadline Cloud punto final permanece dentro de su VPC. Además, puede configurar su VPC para restringir el acceso a Internet a sus instancias.

En las flotas gestionadas por servicios, no se puede acceder a los trabajadores desde Internet, pero sí tienen acceso a Internet y se conectan al servicio a través de Deadline Cloud Internet.

Optar por no participar

AWS Deadline Cloud recopila cierta información operativa para ayudarnos a desarrollarnos y mejorar Deadline Cloud. Los datos recopilados incluyen datos como su ID de AWS cuenta y su ID de usuario, para que podamos identificarlo correctamente si tiene algún problema con ellos Deadline Cloud. También recopilamos información Deadline Cloud específica, como los identificadores de recursos (un FarmID o un QueueID, cuando proceda), el nombre del producto (por ejemplo,, JobAttachments WorkerAgent, etc.) y la versión del producto.

Puede optar por excluirse de esta recopilación de datos mediante la configuración de la aplicación. Cada ordenador con el que interactúe Deadline Cloud, tanto las estaciones de trabajo del cliente como los trabajadores de la flota, debe excluirse por separado.

Deadline Cloud monitor - sobremesa

Deadline Cloud monitor: desktop recopila información operativa, como cuándo se producen bloqueos y cuándo se abre la aplicación, para ayudarnos a saber cuándo tiene problemas con la aplicación. Para excluirse de la recopilación de esta información operativa, vaya a la página de configuración y desactive la opción Activar la recopilación de datos para medir el rendimiento de Deadline Cloud Monitor.

Tras excluirse, el monitor de escritorio ya no envía los datos operativos. Todos los datos recopilados anteriormente se conservan y pueden seguir utilizándose para mejorar el servicio. Para obtener más información, consulte Preguntas frecuentes sobre la privacidad de datos de .

AWS Deadline Cloud CLI y herramientas

La AWS Deadline Cloud CLI, los remitentes y el agente laboral recopilan información operativa, como cuándo se producen accidentes y cuándo se envían los trabajos, para ayudarnos a saber cuándo tiene problemas con estas solicitudes. Para excluirse de la recopilación de esta información operativa, utilice cualquiera de los siguientes métodos:

- En la terminal, ingresa**`deadline config set telemetry.opt_out true`**.

  Esto excluirá la CLI, los remitentes y el agente de trabajo cuando se ejecute como el usuario actual.

- Al instalar el agente de Deadline Cloud trabajo, añada el argumento de la línea de **`--telemetry-opt-out`** comandos. Por ejemplo, **`./install.sh --farm-id $FARM_ID --fleet-id $FLEET_ID --telemetry-opt-out`**.
- Antes de ejecutar el agente de trabajo, la CLI o el remitente, establezca una variable de entorno: **`DEADLINE_CLOUD_TELEMETRY_OPT_OUT=true`**

Tras excluirse, las Deadline Cloud herramientas dejarán de enviar los datos operativos. Todos los datos recopilados anteriormente se conservan y pueden seguir utilizándose para mejorar el servicio. Para obtener más información, consulte Preguntas frecuentes sobre la privacidad de datos de .

Identity and Access Management en Deadline Cloud

AWS Identity and Access Management (IAM) es una herramienta Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos de Deadline Cloud. La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Temas

- Público
- Autenticación con identidades
- Administración de acceso mediante políticas
- Cómo funciona Deadline Cloud con IAM
- Ejemplos de políticas basadas en la identidad para Deadline Cloud
- AWS políticas gestionadas para Deadline Cloud
- Solución de problemas de identidad y acceso a AWS Deadline Cloud

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realices en Deadline Cloud.

Usuario del servicio: si utilizas el servicio Deadline Cloud para realizar tu trabajo, el administrador te proporcionará las credenciales y los permisos que necesitas. A medida que utilices más funciones

de Deadline Cloud para realizar tu trabajo, es posible que necesites permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una función de Deadline Cloud, consulteSolución de problemas de identidad y acceso a AWS Deadline Cloud.

Administrador de servicios: si estás a cargo de los recursos de Deadline Cloud en tu empresa, probablemente tengas acceso completo a Deadline Cloud. Es tu trabajo determinar a qué funciones y recursos de Deadline Cloud deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar la IAM con Deadline Cloud, consulteCómo funciona Deadline Cloud con IAM.

Administrador de IAM: si eres administrador de IAM, quizá te interese obtener más información sobre cómo puedes redactar políticas para gestionar el acceso a Deadline Cloud. Para ver ejemplos de políticas basadas en la identidad de Deadline Cloud que puedes usar en IAM, consulta. Ejemplos de políticas basadas en la identidad para Deadline Cloud

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener

más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWSen la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos, incluidos los que requieren acceso de administrador, que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué

pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .

- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso entre cuentas, consulte el tema sobre el acceso a los recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos utilizan funciones en otros. Servicios de AWS Servicios de AWS Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations .
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo AWS determinar si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo funciona Deadline Cloud con IAM

Antes de utilizar IAM para gestionar el acceso a Deadline Cloud, infórmese sobre las funciones de IAM disponibles para su uso con Deadline Cloud.

Funciones de IAM que puedes usar con Deadline Cloud AWS

Característica de IAM	Soporte de Deadline Cloud
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACL	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Sesiones de acceso directo (FAS)	Sí
Roles de servicio	Sí
Roles vinculados al servicio	No

Para obtener una visión general de cómo Servicios de AWS funcionan Deadline Cloud y otros dispositivos con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas de Deadline Cloud basadas en la identidad

Compatibilidad con las políticas basadas en identidad	Sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en la identidad para Deadline Cloud

Para ver ejemplos de políticas basadas en la identidad de Deadline Cloud, consulte. Ejemplos de políticas basadas en la identidad para Deadline Cloud

Políticas basadas en recursos dentro de Deadline Cloud

Compatibilidad con las políticas basadas en recursos	No

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los directores pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte el tema Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones políticas para Deadline Cloud

Admite acciones de política	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de Deadline Cloud, consulte las acciones definidas por AWS Deadline Cloud en la Referencia de autorización de servicios.

Las acciones políticas en Deadline Cloud usan el siguiente prefijo antes de la acción:

```
deadline
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
```

```
      "deadline:action1",
      "deadline:action2"
         ]
```

Para ver ejemplos de políticas basadas en la identidad de Deadline Cloud, consulte. Ejemplos de políticas basadas en la identidad para Deadline Cloud

Recursos de políticas para Deadline Cloud

Admite recursos de políticas	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de los tipos de recursos de Deadline Cloud y sus ARN, consulte los recursos definidos por AWS Deadline Cloud en la referencia de autorización de servicios. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS Deadline Cloud.

Para ver ejemplos de políticas basadas en la identidad de Deadline Cloud, consulte. Ejemplos de políticas basadas en la identidad para Deadline Cloud

Claves de condición de la política de Deadline Cloud

Admite claves de condición de políticas específicas del servicio	Sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de Deadline Cloud, consulte las claves de condición de AWS Deadline Cloud en la Referencia de autorización de servicio. Para saber con qué acciones y recursos puede utilizar una clave de condición, consulte Acciones definidas por AWS Deadline Cloud.

Para ver ejemplos de políticas basadas en la identidad de Deadline Cloud, consulte. Ejemplos de políticas basadas en la identidad para Deadline Cloud

ACL en Deadline Cloud

Admite las ACL	No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con Deadline Cloud

Admite ABAC (etiquetas en las políticas)	Sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con Deadline Cloud

Compatible con el uso de credenciales temporales	Sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Sesiones de acceso directo para Deadline Cloud

Admite Forward access sessions (FAS)	Sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en AWSél, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Funciones de servicio para Deadline Cloud

Compatible con roles de servicio	Sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de Deadline Cloud. Edita las funciones de servicio solo cuando Deadline Cloud te dé instrucciones para hacerlo.

Funciones vinculadas al servicio para Deadline Cloud

Compatible con roles vinculados al servicio	No

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en la identidad para Deadline Cloud

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de Deadline Cloud. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la AWS API. Un administrador de IAM puede

crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Deadline Cloud, incluido el formato de los ARN de cada uno de los tipos de recursos, consulte las acciones, los recursos y las claves de condición de AWS Deadline Cloud en la Referencia de autorización de servicios.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola de Deadline Cloud
- Política para enviar los trabajos a una cola
- Política que permite la creación de un punto final de licencia
- Política que permite monitorear una cola de granja específica

Prácticas recomendadas sobre las políticas

Las políticas basadas en la identidad determinan si alguien puede crear, acceder o eliminar los recursos de Deadline Cloud de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se

pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Política de validación de Analizador de acceso de IAM en la Guía de usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Configuración del acceso a una API protegido por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de la consola de Deadline Cloud

Para acceder a la consola de AWS Deadline Cloud, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de Deadline Cloud que tiene en su cuenta Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la consola de Deadline Cloud, adjunta también la nube de Deadline *ConsoleAccess* o la política *ReadOnly* AWS gestionada a las entidades. Para más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Política para enviar los trabajos a una cola

En este ejemplo, se crea una política exhaustiva que concede permiso para enviar trabajos a una cola específica de una granja específica.

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

Política que permite la creación de un punto final de licencia

En este ejemplo, se crea una política exhaustiva que concede los permisos necesarios para crear y gestionar los puntos de enlace de licencia. Utilice esta política para crear el punto de enlace de licencia para la VPC asociada a su granja.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "SID": "CreateLicenseEndpoint",
        "Effect": "Allow",
        "Action": [
            "deadline:CreateLicenseEndpoint",
            "deadline:DeleteLicenseEndpoint",
            "deadline:GetLicenseEndpoint",
            "deadline:UpdateLicenseEndpoint",
            "deadline:ListLicenseEndpoints",
            "deadline:PutMeteredProduct",
```

```
            "deadline:DeleteMeteredProduct",
            "deadline:ListMeteredProducts",
            "deadline:ListAvailableMeteredProducts",
            "ec2:CreateVpcEndpoint",
            "ec2:DescribeVpcEndpoints",
            "ec2:DeleteVpcEndpoints"
        ],
        "Resource": "*"
    }]
}
```

Política que permite monitorear una cola de granja específica

En este ejemplo, se crea una política exhaustiva que concede permiso para supervisar los trabajos de una cola específica para una granja específica.

```
{
    "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 políticas gestionadas para Deadline Cloud

Una política AWS gestionada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

AWS política gestionada: AWSDeadlineCloud-FleetWorker

Puede adjuntar la `AWSDeadlineCloud-FleetWorker` política a sus identidades AWS Identity and Access Management (de IAM).

Esta política otorga a los trabajadores de esta flota los permisos necesarios para conectarse al servicio y recibir tareas del mismo.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `deadline`— Permite a los directores gestionar a los trabajadores de una flota.

Para obtener una lista en JSON de los detalles de la política, consulte AWSDeadlineCloud-FleetWorker en la guía de referencia de políticas administradas de AWS.

AWS política gestionada: AWSDeadlineCloud-WorkerHost

Puede adjuntar la política `AWSDeadlineCloud-WorkerHost` a las identidades de IAM.

Esta política concede los permisos necesarios para conectarse inicialmente al servicio. Se puede utilizar como perfil de instancia de Amazon Elastic Compute Cloud (Amazon EC2).

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `deadline`— Permite a los directores crear trabajadores.

Para obtener una lista en JSON de los detalles de la política, consulte AWSDeadlineCloud-WorkerHost en la guía de referencia de políticas administradas de AWS.

AWS política gestionada: AWSDeadlineCloud-UserAccessFarms

Puede adjuntar la política `AWSDeadlineCloud-UserAccessFarms` a las identidades de IAM.

Esta política permite a los usuarios acceder a los datos de las granjas en función de las granjas de las que son miembros y de su nivel de membresía.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `deadline`— Permite al usuario acceder a los datos de la granja.
- `ec2`— Permite a los usuarios ver detalles sobre los tipos de instancias de Amazon EC2.
- `identitystore`— Permite a los usuarios ver los nombres de usuarios y grupos.

Para ver una lista en JSON de los detalles de la política, consulte AWSDeadlineCloudUserAccessFarms en la guía de referencia de políticas administradas por AWS.

AWS política gestionada: AWSDeadlineCloud-UserAccessFleets

Puede adjuntar la política `AWSDeadlineCloud-UserAccessFleets` a las identidades de IAM.

Esta política permite a los usuarios acceder a los datos de la flota en función de las granjas de las que son miembros y de su nivel de membresía.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `deadline`— Permite al usuario acceder a los datos de la granja.
- `ec2`— Permite a los usuarios ver detalles sobre los tipos de instancias de Amazon EC2.
- `identitystore`— Permite a los usuarios ver los nombres de usuarios y grupos.

Para ver una lista en JSON de los detalles de la política, consulte AWSDeadlineCloudUserAccessFlotas en la guía de referencia sobre políticas administradas por AWS.

AWS política gestionada: AWSDeadlineCloud-UserAccessJobs

Puede adjuntar la política `AWSDeadlineCloud-UserAccessJobs` a las identidades de IAM.

Esta política permite a los usuarios acceder a los datos de trabajo en función de las granjas de las que son miembros y de su nivel de membresía.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `deadline`— Permite al usuario acceder a los datos de la granja.
- `ec2`— Permite a los usuarios ver detalles sobre los tipos de instancias de Amazon EC2.
- `identitystore`— Permite a los usuarios ver los nombres de usuarios y grupos.

Para ver una lista en JSON de los detalles de la política, consulte AWSDeadlineCloud la guía de referencia de UserAccessJobs in the AWS Managed Policy.

AWS política gestionada: AWSDeadlineCloud-UserAccessQueues

Puede adjuntar la política `AWSDeadlineCloud-UserAccessQueues` a las identidades de IAM.

Esta política permite a los usuarios acceder a los datos de las colas en función de las granjas de las que son miembros y de su nivel de membresía.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `deadline`— Permite al usuario acceder a los datos de la granja.
- `ec2`— Permite a los usuarios ver detalles sobre los tipos de instancias de Amazon EC2.
- `identitystore`— Permite a los usuarios ver los nombres de usuarios y grupos.

Para ver una lista en JSON de los detalles de la política, consulte AWSDeadlineCloud-UserAccessQueues en la guía de referencia de políticas administradas de AWS.

Deadline Cloud actualiza las políticas AWS gestionadas

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas de Deadline Cloud desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial de documentos de Deadline Cloud.

Cambio	Descripción	Fecha
Deadline Cloud comenzó a rastrear los cambios	Deadline Cloud comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	2 de abril de 2024

Solución de problemas de identidad y acceso a AWS Deadline Cloud

Usa la siguiente información para ayudarte a diagnosticar y solucionar los problemas más comunes que pueden surgir al trabajar con Deadline Cloud e IAM.

Temas

- No estoy autorizado a realizar ninguna acción en Deadline Cloud
- No estoy autorizado a realizar tareas como: PassRole

- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Deadline Cloud

No estoy autorizado a realizar ninguna acción en Deadline Cloud

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `deadline:`*`GetWidget`*.

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

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `deadline:`*`GetWidget`*.

Si necesitas ayuda, ponte en contacto con tu AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibes un mensaje de error que indica que no estás autorizado a realizar la `iam:PassRole` acción, debes actualizar tus políticas para que puedas transferir una función a Deadline Cloud.

Algunas te Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

El siguiente ejemplo de error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Deadline Cloud. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

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

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Deadline Cloud

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para saber si Deadline Cloud admite estas funciones, consulteCómo funciona Deadline Cloud con IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer la diferencia entre usar roles y políticas basadas en recursos para el acceso entre cuentas, consulte el tema Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Validación de conformidad para Deadline Cloud

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

> **Note**
>
> No Servicios de AWS todas cumplen los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.

- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en Deadline Cloud

La infraestructura AWS global se basa en zonas Regiones de AWS de disponibilidad. Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

AWS Deadline Cloud no hace copias de seguridad de los datos almacenados en el depósito de S3 de sus adjuntos de trabajo. Puede activar las copias de seguridad de los datos adjuntos de su trabajo mediante cualquier mecanismo de copia de seguridad estándar de Amazon S3, como S3 Versioning o AWS Backup.

Seguridad de la infraestructura en Deadline Cloud

Como servicio gestionado, AWS Deadline Cloud está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a Deadline Cloud a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM principal. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Deadline Cloud no admite el uso de políticas de puntos finales de nube privada AWS PrivateLink virtual (VPC). Utiliza la política AWS PrivateLink predeterminada, que otorga acceso total al punto final. Para obtener más información, consulte la política de puntos finales predeterminada en la guía del AWS PrivateLink usuario.

Análisis de configuración y vulnerabilidad en Deadline Cloud

AWS se encarga de tareas de seguridad básicas, como la aplicación de parches al sistema operativo (SO) huésped y a las bases de datos, la configuración del firewall y la recuperación ante desastres. Estos procedimientos han sido revisados y certificados por los terceros pertinentes. Para obtener más detalles, consulte los siguientes recursos de :

- Modelo de responsabilidad compartida
- Amazon Web Services: información general de procesos de seguridad (documento técnico)

AWS Deadline Cloud gestiona las tareas en flotas gestionadas por el servicio o por el cliente:

- En el caso de las flotas gestionadas por servicios, Deadline Cloud gestiona el sistema operativo huésped.
- En el caso de las flotas gestionadas por el cliente, usted es responsable de gestionar el sistema operativo.

Para obtener información adicional sobre la configuración y el análisis de vulnerabilidades de AWS Deadline Cloud, consulte

- Prácticas recomendadas de seguridad para Deadline Cloud

Prevención de la sustitución confusa entre servicios

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación de identidad entre servicios puede provocar el confuso problema

de un diputado. La suplantación entre servicios puede producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puede manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que lo ayudan a proteger sus datos para todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta.

Se recomienda utilizar las claves de contexto de condición aws:SourceAccountglobal aws:SourceArny las claves de contexto en las políticas de recursos para limitar los permisos que se AWS Deadline Cloud otorgan a otro servicio al recurso. Utilice `aws:SourceArn` si desea que solo se asocie un recurso al acceso entre servicios. Utilice `aws:SourceAccount` si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.

La forma más eficaz de protegerse contra el problema de la sustitución confusa es utilizar la clave de contexto de condición global de `aws:SourceArn` con el nombre de recurso de Amazon (ARN) completo del recurso. Si no conoce el ARN completo del recurso o si está especificando varios recursos, utilice la clave de condición de contexto global `aws:SourceArn` con caracteres comodines (*) para las partes desconocidas del ARN. Por ejemplo, `arn:aws:deadline:*:`*`123456789012`*`:*`.

Si el valor de `aws:SourceArn` no contiene el ID de cuenta, como un ARN de bucket de Amazon S3, debe utilizar ambas claves de contexto de condición global para limitar los permisos.

En el siguiente ejemplo, se muestra cómo utilizar las claves de contexto de condición `aws:SourceAccount` global `aws:SourceArn` y las claves contextuales Deadline Cloud para evitar el confuso problema de los diputados.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "deadline.amazonaws.com"
    },
    "Action": "deadline:ActionName",
    "Resource": [
      "*"
    ],
    "Condition": {
      "ArnLike": {
```

```
        "aws:SourceArn": "arn:aws:deadline:*:123456789012:*"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

Acceda AWS Deadline Cloud mediante un punto final de interfaz (AWS PrivateLink)

Puede usarlo AWS PrivateLink para crear una conexión privada entre su VPC y. AWS Deadline Cloud Puede acceder Deadline Cloud como si estuviera en su VPC, sin el uso de una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o AWS Direct Connect una conexión. Las instancias de la VPC no necesitan direcciones IP públicas para acceder a Deadline Cloud.

Esta conexión privada se establece mediante la creación de un punto de conexión de interfaz alimentado por AWS PrivateLink. Creamos una interfaz de red de punto de conexión en cada subred habilitada para el punto de conexión de interfaz. Se trata de interfaces de red administradas por el solicitante que sirven como punto de entrada para el tráfico destinado a Deadline Cloud.

Para obtener más información, consulte Acceso a los Servicios de AWS a través de AWS PrivateLink en la Guía de AWS PrivateLink .

Consideraciones sobre Deadline Cloud

Antes de configurar un punto de enlace de interfaz para Deadline Cloud, consulte Acceder a un servicio de AWS mediante un punto de enlace de VPC de interfaz en la AWS PrivateLink Guía.

Deadline Cloud permite realizar llamadas a todas sus acciones de API a través del punto final de la interfaz.

De forma predeterminada, Deadline Cloud se permite el acceso total a través del punto final de la interfaz. Como alternativa, puede asociar un grupo de seguridad a las interfaces de red del punto final para controlar el tráfico que Deadline Cloud pasa por el punto final de la interfaz.

Deadline Cloud no admite políticas de puntos finales de VPC. Para obtener más información, consulte Uso de políticas de punto de conexión para controlar el acceso a puntos de conexión de VPC en la Guía de AWS PrivateLink .

Deadline Cloud puntos finales

Deadline Cloud utiliza dos puntos finales para acceder al servicio mediante. AWS PrivateLink

Los trabajadores utilizan el `com.amazonaws.region.deadline.scheduling` terminal para obtener las tareas de la cola, informar sobre su Deadline Cloud progreso y enviar los resultados de las tareas. Si utiliza una flota gestionada por el cliente, el punto final de programación es el único punto final que debe crear, a menos que utilice operaciones de gestión. Por ejemplo, si un trabajo crea más puestos de trabajo, debe habilitar el punto final de administración para que llame a la `CreateJob` operación.

El Deadline Cloud monitor lo utiliza `com.amazonaws.region.deadline.management` para administrar los recursos de la granja, por ejemplo, para crear y modificar colas y flotas o para obtener listas de trabajos, pasos y tareas.

Deadline Cloud también requiere puntos de conexión para los siguientes puntos de conexión de servicio: AWS

- Deadline Cloud AWS STS se utiliza para autenticar a los trabajadores para que puedan acceder a los activos laborales. Para obtener más información AWS STS, consulte las credenciales de seguridad temporales en IAM en la Guía del AWS Identity and Access Management usuario.
- Si configuras tu flota gestionada por el cliente en una subred sin conexión a Internet, debes crear un punto de enlace de VPC para CloudWatch Amazon Logs para que los trabajadores puedan escribir registros. Para obtener más información, consulte Monitorear con. CloudWatch
- Si usa adjuntos de trabajo, debe crear un punto de enlace de VPC para Amazon Simple Storage Service (Amazon S3) para que los trabajadores puedan acceder a los archivos adjuntos. Para obtener más información, consulte Adjuntos de trabajos en Deadline Cloud.

Cree puntos finales para Deadline Cloud

Puede crear puntos de enlace de interfaz para Deadline Cloud utilizar la consola de Amazon VPC o AWS Command Line Interface ().AWS CLI Para obtener más información, consulte Creación de un punto de conexión de interfaz en la Guía de AWS PrivateLink .

Cree puntos de enlace de administración y programación para Deadline Cloud utilizar los siguientes nombres de servicio. Sustituya *la región* por la ubicación Región de AWS en la que realizó el despliegue Deadline Cloud.

```
com.amazonaws.region.deadline.management
```

```
com.amazonaws.region.deadline.scheduling
```

Si habilitas el DNS privado para los puntos finales de la interfaz, puedes realizar solicitudes a la API Deadline Cloud utilizando su nombre de DNS regional predeterminado. Por ejemplo, `worker.deadline.us-east-1.amazonaws.com` para las operaciones de los trabajadores o `management.deadline.us-east-1.amazonaws.com` para todas las demás operaciones.

También debe crear un punto final para AWS STS usar el siguiente nombre de servicio:

```
com.amazonaws.region.sts
```

Si su flota gestionada por el cliente se encuentra en una subred sin conexión a Internet, debe crear un punto final de CloudWatch Logs con el siguiente nombre de servicio:

```
com.amazonaws.region.logs
```

Si utiliza adjuntos de trabajo para transferir archivos, debe crear un punto de conexión de Amazon S3 con el siguiente nombre de servicio:

```
com.amazonaws.region.s3
```

Prácticas recomendadas de seguridad para Deadline Cloud

AWS Deadline Cloud (Deadline Cloud) ofrece una serie de características de seguridad que debes tener en cuenta a la hora de desarrollar e implementar tus propias políticas de seguridad. Las siguientes prácticas recomendadas son directrices generales y no constituyen una solución de seguridad completa. Puesto que es posible que estas prácticas recomendadas no sean adecuadas o suficientes para el entorno, considérelas como consideraciones útiles en lugar de como normas.

> **Note**
>
> Para obtener más información sobre la importancia de muchos temas de seguridad, consulte el Modelo de responsabilidad compartida.

Protección de datos

Para proteger los datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure cuentas individuales con AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice avanzados servicios de seguridad administrados, como Amazon Macie, que lo ayuden a detectar y proteger los datos personales almacenados en Amazon Simple Storage Service (Amazon S3).
- Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de conexión de FIPS. Para obtener más información acerca de los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Le recomendamos encarecidamente que nunca introduzca información de identificación confidencial, como, por ejemplo, números de cuenta de sus clientes, en los campos de formato libre, como el campo Nombre. Esto incluye cuando trabajas con AWS Deadline Cloud u otro Servicios de AWS dispositivo mediante la consola, la API o AWS los SDK. AWS CLI Todos los datos que introduzcas en Deadline Cloud u otros servicios podrían recopilarse para incluirlos en los registros de diagnóstico. Cuando le proporcione una URL a un servidor externo, no incluya información sobre las credenciales en la URL para validar la solicitud en ese servidor.

AWS Identity and Access Management permisos

Gestione el acceso a los AWS recursos mediante los usuarios, las funciones AWS Identity and Access Management (IAM) y concediendo el mínimo de privilegios a los usuarios. Establezca políticas y procedimientos de administración de credenciales para crear, distribuir, rotar y revocar AWS las credenciales de acceso. Para obtener más información, consulte Prácticas recomendadas de IAM en la Guía del usuario de IAM.

Ejecute trabajos como usuarios y grupos

Al utilizar la funcionalidad de colas en Deadline Cloud, se recomienda especificar un usuario del sistema operativo (SO) y su grupo principal para que el usuario del sistema operativo tenga los permisos con menos privilegios para los trabajos de la cola.

Si especificas «Ejecutar como usuario» (y grupo), todos los procesos de los trabajos enviados a la cola se ejecutarán con ese usuario del sistema operativo y heredarán los permisos del sistema operativo asociados a ese usuario.

Las configuraciones de flota y cola se combinan para establecer una postura de seguridad. Por el lado de la cola, se pueden especificar el rol «Job run as user» y el rol de IAM para usar el sistema operativo y AWS los permisos para los trabajos de la cola. La flota define la infraestructura (servidores de los trabajadores, redes, almacenamiento compartido montado) que, cuando se asocia a una cola determinada, ejecuta los trabajos dentro de la cola. Los trabajos de una o más colas asociadas deben acceder a los datos disponibles en los hosts de los trabajadores. La especificación de un usuario o un grupo ayuda a proteger los datos de los trabajos frente a otras colas, otro software instalado u otros usuarios con acceso a los hosts de los trabajadores. Cuando una cola no tiene un usuario, se ejecuta como el usuario agente, que puede hacerse pasar por (`sudo`) cualquier usuario de la cola. De esta forma, una cola sin un usuario puede escalar los privilegios a otra cola.

Red

Para evitar que el tráfico sea interceptado o redirigido, es fundamental proteger cómo y hacia dónde se enruta el tráfico de la red.

Le recomendamos que proteja su entorno de red de las siguientes maneras:

- Proteja las tablas de enrutamiento de subred de Amazon Virtual Private Cloud (Amazon VPC) para controlar cómo se enruta el tráfico de la capa IP.
- Si utiliza Amazon Route 53 (Route 53) como proveedor de DNS en la configuración de su granja o estación de trabajo, asegure el acceso a la API de Route 53.
- Si se conecta a Deadline Cloud desde fuera, por AWS ejemplo, mediante estaciones de trabajo locales u otros centros de datos, proteja cualquier infraestructura de red local. Esto incluye los servidores DNS y las tablas de enrutamiento en enrutadores, conmutadores y otros dispositivos de red.

Trabajos y datos de trabajos

Los trabajos de Deadline Cloud se ejecutan dentro de las sesiones en los anfitriones de los trabajadores. Cada sesión ejecuta uno o más procesos en el host del trabajador, que por lo general requieren la introducción de datos para generar resultados.

Para proteger estos datos, puede configurar los usuarios del sistema operativo con colas. El agente de trabajo utiliza el usuario del sistema operativo de colas para ejecutar los subprocesos de la sesión. Estos subprocesos heredan los permisos del usuario del sistema operativo de colas.

Le recomendamos que siga las mejores prácticas para proteger el acceso a los datos a los que acceden estos subprocesos. Para obtener más información, consulte el Modelo de responsabilidad compartida.

Estructura de la granja

Puedes organizar las flotas y colas de Deadline Cloud de muchas maneras. Sin embargo, algunos acuerdos tienen implicaciones de seguridad.

Una granja tiene uno de los límites más seguros porque no puede compartir los recursos de Deadline Cloud con otras granjas, incluidas las flotas, las colas y los perfiles de almacenamiento. Sin embargo, puedes compartir AWS recursos externos dentro de una granja, lo que pone en peligro el límite de seguridad.

También puede establecer límites de seguridad entre las colas de la misma granja mediante la configuración adecuada.

Siga estas prácticas recomendadas para crear colas seguras en la misma granja:

- Asocie una flota únicamente a las colas que se encuentren dentro del mismo límite de seguridad. Tenga en cuenta lo siguiente:
  - Una vez que el trabajo se ejecuta en el host de trabajo, es posible que los datos permanezcan ocultos, por ejemplo, en un directorio temporal o en el directorio principal del usuario de la cola.
  - El mismo usuario del sistema operativo ejecuta todos los trabajos en un host de trabajadores de flota propiedad del servicio, independientemente de la cola a la que envíe el trabajo.
  - Un trabajo puede dejar los procesos en ejecución en un host de trabajo, lo que permite que los trabajos de otras colas observen otros procesos en ejecución.
- Asegúrese de que solo las colas que se encuentren dentro del mismo límite de seguridad compartan un bucket de Amazon S3 para adjuntar trabajos.

- Asegúrese de que solo las colas que se encuentren dentro del mismo límite de seguridad compartan un usuario del sistema operativo.
- Proteja cualquier otro AWS recurso que esté integrado en la granja hasta el límite.

Colas de adjuntos de trabajos

Los adjuntos de trabajos se asocian a una cola, que utiliza tu bucket de Amazon S3.

- Los adjuntos de trabajo se escriben y leen desde un prefijo raíz del bucket de Amazon S3. Este prefijo raíz se especifica en la llamada a la `CreateQueue` API.
- El bucket tiene una correspondiente`Queue Role`, que especifica la función que concede a los usuarios de la cola acceso al bucket y al prefijo raíz. Al crear una cola, debe especificar el nombre del recurso de `Queue Role` Amazon (ARN) junto con el depósito de adjuntos de trabajos y el prefijo raíz.
- Las llamadas autorizadas a las operaciones de `AssumeQueueRoleForReadAssumeQueueRoleForUser`, y `AssumeQueueRoleForWorker` API devuelven un conjunto de credenciales de seguridad temporales para. `Queue Role`

Si crea una cola y reutiliza un bucket y un prefijo raíz de Amazon S3, existe el riesgo de que la información se divulgue a terceros no autorizados. Por ejemplo, QueueA y QueueB comparten el mismo bucket y el mismo prefijo raíz. En un flujo de trabajo seguro, Artista tiene acceso a QueueA pero no a QueueB. Sin embargo, cuando varias colas comparten un depósito, Artista puede acceder a los datos de los datos de QueueB porque utiliza el mismo depósito y el mismo prefijo raíz que QueuEa.

La consola configura colas que son seguras de forma predeterminada. Asegúrese de que las colas tengan una combinación distinta de bucket de Amazon S3 y prefijo raíz, a menos que formen parte de un límite de seguridad común.

Para aislar las colas, debe configurarlas de manera que solo se permita el `Queue Role` acceso de las colas al bucket y al prefijo raíz. En el siguiente ejemplo, sustituya cada *`marcador`* de posición por la información específica del recurso.

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

También debe establecer una política de confianza para el rol. En el siguiente ejemplo, sustituya el texto del *marcador* de posición por la información específica del recurso.

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

Buckets Amazon S3 de software personalizados

Puede añadir la siguiente declaración para acceder `Queue Role` al software personalizado de su bucket de Amazon S3. En el siguiente ejemplo, sustituya *`SOFTWARE_BUCKET_NAME por el nombre de su`* bucket de S3.

```
"Statement": [
    {
        "Action": [
            "s3:GetObject",
            "s3:ListBucket"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::SOFTWARE_BUCKET_NAME",
            "arn:aws:s3:::SOFTWARE_BUCKET_NAME/*"
        ]
    }
]
```

Para obtener más información sobre las prácticas recomendadas de seguridad de Amazon S3, consulte las prácticas recomendadas de seguridad para Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Los trabajadores son anfitriones

Proteja los hosts de los trabajadores para garantizar que cada usuario solo pueda realizar operaciones para el rol que se le ha asignado.

Recomendamos las siguientes prácticas recomendadas para proteger los anfitriones de los trabajadores:

- No utilices el mismo `jobRunAsUser` valor con varias colas, a menos que los trabajos enviados a esas colas estén dentro del mismo límite de seguridad.
- No `jobRunAsUser` defina la cola con el nombre del usuario del sistema operativo en el que se ejecuta el agente de trabajo.
- Otorgue a los usuarios de la cola los permisos de sistema operativo con menos privilegios necesarios para las cargas de trabajo de cola previstas. Asegúrese de que no tengan permisos de escritura en el sistema de archivos para trabajar, agentes, archivos de programas u otro software compartido.
- Asegúrese de que solo el usuario root Linux y el `Administrator` propietario de la cuenta posean los Windows archivos del programa del agente de trabajo y puedan modificarlos.
- En los Linux hosts de trabajo, considere la posibilidad `umask` de configurar una alternativa `/etc/sudoers` que permita al usuario del agente de trabajo iniciar procesos como usuarios en cola. Esta configuración ayuda a garantizar que otros usuarios no puedan acceder a los archivos escritos en la cola.
- Otorgue a las personas de confianza con menos privilegios el acceso a los anfitriones de los trabajadores.
- Restrinja los permisos al DNS local, a los archivos de configuración (`/etc/hosts`activos y activos) Linux y a las tablas de enrutamiento `C:\Windows\system32\etc\hosts` en Windows las estaciones de trabajo y los sistemas operativos de los hosts de los trabajadores.
- Restrinja los permisos a la configuración de DNS en las estaciones de trabajo y los sistemas operativos de los hosts de los trabajadores.
- Aplica parches periódicos al sistema operativo y a todo el software instalado. Este enfoque incluye el software que se utiliza específicamente con Deadline Cloud, como los remitentes, los adaptadores, los agentes de trabajo, OpenJD los paquetes y otros.
- Usa contraseñas seguras para la Windows cola. `jobRunAsUser`
- Cambia las contraseñas de la cola `jobRunAsUser` con regularidad.
- Asegúrese de que el acceso con menos privilegios a las Windows contraseñas secretas y elimine las que no se utilicen.
- No dé `jobRunAsUser` permiso a la cola para que los comandos de programación se ejecuten en el futuro:
  - SíLinux, deniega a estas cuentas el acceso a `cron` `yat`.
  - ActivadoWindows, deniega el acceso de estas cuentas al programador de Windows tareas.

> **Note**
>
> Para obtener más información sobre la importancia de actualizar periódicamente el sistema operativo y el software instalado, consulte el Modelo de responsabilidad compartida.

Estaciones de trabajo

Es importante proteger las estaciones de trabajo con acceso a Deadline Cloud. Este enfoque ayuda a garantizar que los trabajos que envíes a Deadline Cloud no puedan ejecutar cargas de trabajo arbitrarias que se te facturen. Cuenta de AWS

Recomendamos las siguientes prácticas recomendadas para proteger las estaciones de trabajo de los artistas. Para obtener más información, consulte Modelo de responsabilidad compartida de .

- Proteja todas las credenciales persistentes a las que pueda acceder AWS, incluida Deadline Cloud. Para obtener más información, consulte Administración de claves de acceso para usuarios de IAM en la Guía del usuario de IAM.
- Instale únicamente software seguro y confiable.
- Exija a los usuarios que se federen con un proveedor de identidad para acceder AWS con credenciales temporales.
- Utilice permisos seguros en los archivos del programa de envío de Deadline Cloud para evitar su manipulación.
- Conceda a las personas de confianza con menos privilegios el acceso a las estaciones de trabajo de los artistas.
- Utilice únicamente los remitentes y adaptadores que obtenga a través del Deadline Cloud Monitor.
- Restrinja los permisos `/etc/hosts` y las tablas de enrutamiento en las estaciones de trabajo y los sistemas operativos anfitriones de los trabajadores.
- Restrinja los permisos a `/etc/resolv.conf` las estaciones de trabajo y a los sistemas operativos anfitriones de los trabajadores.
- Aplica parches periódicos al sistema operativo y a todo el software instalado. Este enfoque incluye el software que se utiliza específicamente con Deadline Cloud, como los remitentes, los adaptadores, los agentes de trabajo, OpenJD los paquetes y otros.

Supervisión de AWS Deadline Cloud

El monitoreo es una parte importante para mantener la confiabilidad, la disponibilidad y el rendimiento de AWS Deadline Cloud (Deadline Cloud) y sus AWS soluciones. Recopile datos de supervisión de todas las partes de su AWS solución para poder depurar con mayor facilidad una falla multipunto en caso de que se produzca. Antes de comenzar a monitorear Deadline Cloud, debe crear un plan de monitoreo que incluya respuestas a las siguientes preguntas:

- ¿Cuáles son los objetivos de la monitorización?
- ¿Qué recursos va a monitorizar?
- ¿Con qué frecuencia va a monitorizar estos recursos?
- ¿Qué herramientas de monitorización va a utilizar?
- ¿Quién se encargará de realizar las tareas de monitoreo?
- ¿Quién debería recibir una notificación cuando surjan problemas?

AWS y Deadline Cloud proporcionan herramientas que puede utilizar para supervisar sus recursos y responder a posibles incidentes. Algunas de estas herramientas se encargan de la supervisión por usted, mientras que otras requieren una intervención manual. Debe automatizar las tareas de supervisión en la medida de lo posible.

- Amazon CloudWatch monitorea tus AWS recursos y las aplicaciones en las que AWS ejecutas en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique. Por ejemplo, puede CloudWatch hacer un seguimiento del uso de la CPU u otras métricas de sus instancias de Amazon EC2 y lanzar automáticamente nuevas instancias cuando sea necesario. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.

  Deadline Cloud tiene tres CloudWatch métricas.
- Amazon CloudWatch Logs le permite supervisar, almacenar y acceder a sus archivos de registro desde instancias de Amazon EC2 y otras fuentes. CloudTrail CloudWatch Los registros pueden monitorear la información de los archivos de registro y notificarle cuando se alcancen ciertos umbrales. También se pueden archivar los datos del registro en un almacenamiento de larga duración. Para obtener más información, consulta la Guía del usuario CloudWatch de Amazon Logs.

- Amazon se EventBridge puede utilizar para automatizar sus AWS servicios y responder automáticamente a los eventos del sistema, como los problemas de disponibilidad de las aplicaciones o los cambios de recursos. Los eventos de AWS los servicios se envían casi EventBridge en tiempo real. Puede crear reglas sencillas para indicar qué eventos le resultan de interés, así como qué acciones automatizadas se van a realizar cuando un evento cumple una de las reglas. Para obtener más información, consulta la Guía EventBridge del usuario de Amazon.
- AWS CloudTrailcaptura las llamadas a la API y los eventos relacionados realizados por su AWS cuenta o en su nombre y entrega los archivos de registro a un bucket de Amazon S3 que especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron las llamadas. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Temas

- Registrar llamadas con CloudTrail
- Monitorear con CloudWatch
- Actuar en función de EventBridge los acontecimientos

Registrar llamadas con CloudTrail

AWS Deadline Cloud está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o una persona Servicio de AWS en Deadline Cloud. CloudTrail captura todas las llamadas a la API de Deadline Cloud como eventos. Las llamadas capturadas incluyen llamadas desde la consola de Deadline Cloud y llamadas en código a las operaciones de la API de Deadline Cloud.

Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos de Deadline Cloud. Si no configuras una ruta, podrás ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puedes determinar la solicitud que se realizó a Deadline Cloud, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulta la Guía AWS CloudTrail del usuario.

Información sobre Deadline Cloud en CloudTrail

CloudTrail está activado en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en Deadline Cloud, esa actividad se registra en un CloudTrail evento junto con otros

Servicio de AWS eventos del historial de eventos. Puedes ver, buscar y descargar eventos recientes en tu Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

CloudTrail también registra los eventos cuando los usuarios inician sesión en el monitor de Deadline Cloud y reciben AWS credenciales. Cuando un usuario inicia sesión, se produce un CloudTrail evento con la fuente `signin.amazonaws.com` y el nombre`UserAuthentication`. Hay un segundo evento en el que el usuario que ha iniciado sesión recibe AWS las credenciales de la fuente `sts.amazonaws.com` y el nombre. `AssumeRole` El ID del usuario se registra en el segundo evento dentro del nombre de la sesión del rol.

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los eventos de Deadline Cloud, crea un registro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las Regiones de AWS. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros Servicios de AWS para que analicen más a fondo los datos de eventos recopilados en los CloudTrail registros y actúen en función de ellos.

Para más información, consulte los siguientes temas:

Introducción a la creación de registros de seguimiento

CloudTrail servicios e integraciones compatibles

Configuración de las notificaciones de Amazon SNS para CloudTrail

Recibir archivos de CloudTrail registro de varias regiones

Recibir archivos de CloudTrail registro de varias cuentas

Deadline Cloud permite registrar las siguientes acciones como eventos en los archivos de CloudTrail registro:

- associate-member-to-farm
- associate-member-to-fleet
- associate-member-to-job
- associate-member-to-queue
- assume-fleet-role-for-leer

- assume-fleet-role-for-trabajador
- assume-queue-role-for-leer
- assume-queue-role-for-usuario
- assume-queue-role-for-trabajador
- crear presupuesto
- crear granja
- create-fleet
- create-license-endpoint
- crear monitor
- crear cola
- create-queue-environment
- create-queue-fleet-association
- create-storage-profile
- create-worker
- eliminar-presupuesto
- delete-farm
- delete-fleet
- delete-license-endpoint
- delete-metered-product
- eliminar-monitor
- eliminar cola
- delete-queue-environment
- delete-queue-fleet-association
- delete-storage-profile
- delete-worker
- disassociate-member-from-farm
- disassociate-member-from-fleet
- disassociate-member-from-job
- disassociate-member-from-queue

- get-application-version
- obtener presupuesto
- get-farm
- get-feature-map
- get-fleet
- get-license-endpoint
- get-monitor
- get-queue
- get-queue-environment
- get-queue-fleet-association
- get-sessions-statistics-aggregation
- get-storage-profile
- get-storage-profile-for-cola
- list-available-metered-products
- listas de presupuestos
- list-farm-members
- listas de granjas
- list-fleet-members
- listas de flotas
- list-job-members
- list-license-endpoints
- list-metered-products
- monitores de listas
- list-queue-environments
- list-queue-fleet-associations
- list-queue-members
- listas de colas
- list-storage-profiles
- list-storage-profiles-for-cola

- list-tags-for-resource
- put-metered-product
- start-sessions-statistics-aggregation
- tag-resource
- untag-resource
- actualizar el presupuesto
- update-farm
- actualizar flota
- actualizar el monitor
- cola de actualizaciones
- update-queue-environment
- update-queue-fleet-association
- update-storage-profile
- update-worker

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de .

Para obtener más información, consulte el elemento de identidad CloudTrail del usuario.

Descripción de las entradas del archivo de registro de Deadline Cloud

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud,

etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

En este ejemplo de JSON se muestra el registro generado por una llamada a la **`CreateFarm`** API:

```
{
    "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",
}
```

El ejemplo muestra la AWS región, la dirección IP y otros «`requestParameters`», como «» y `displayName` «`kmsKeyArn`», que pueden ayudarte a identificar el evento.

Monitorear con CloudWatch

Amazon CloudWatch (CloudWatch) recopila datos sin procesar y los procesa para convertirlos en métricas legibles y casi en tiempo real. Puedes abrir la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/ para ver y filtrar las métricas de Deadline Cloud.

- En una flota gestionada por el cliente de Deadline Cloud, te CloudWatch envía dos métricas `UnhealthyWorkerCount` y: `RecommendedFleetSize`
- El espacio de nombres de estas métricas es `AWS/DeadlineCloud.`
- Puede usar las dimensiones `farmID` y filtrar `fleetID` las métricas.
- Ambas métricas utilizan la unidad`count`.

Estas estadísticas se guardan durante 15 meses para que pueda acceder a la información histórica y obtener una mejor perspectiva del rendimiento de su aplicación o servicio web. También puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se cumplan dichos umbrales. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.

Deadline Cloud tiene dos tipos de registros: registros de tareas y registros de trabajadores. Un registro de tareas es cuando se ejecutan registros de ejecución como un script o mientras se ejecuta un DCC. Un registro de tareas puede mostrar eventos como la carga de activos, la representación de teselas o la falta de localización de texturas.

Un registro de trabajo muestra los procesos de los agentes de trabajo. Estos pueden incluir datos como el momento en que el agente de trabajo se pone en marcha, se registra, informa del progreso, carga las configuraciones o completa las tareas.

En el caso de Deadline Cloud, los trabajadores suben estos CloudWatch registros a Logs. De forma predeterminada, los registros nunca caducan. Si un trabajo genera un gran volumen de datos, puede incurrir en costes adicionales. Para obtener más información, consulta los CloudWatch precios de Amazon.

Puede ajustar la política de retención para cada grupo de registros. Una retención más corta elimina los registros antiguos y puede ayudar a reducir los costos de almacenamiento. Para conservar los registros, puede archivarlos en Amazon Simple Storage Service antes de eliminarlos. Para obtener más información, consulte Exportación de datos de registro a Amazon S3 mediante la consola en la guía del CloudWatch usuario de Amazon.

> **Note**
>
> CloudWatch las lecturas de registro están limitadas por AWS. Si tienes pensado incorporar a muchos artistas, te sugerimos que contactes con el servicio de AWS atención al cliente y solicites un aumento de la `GetLogEvents` cuota CloudWatch. Además, te recomendamos cerrar el portal de registro cuando no estés depurando.

Para obtener más información, consulta las cuotas de CloudWatch registros en la guía del CloudWatch usuario de Amazon.

Actuar en función de EventBridge los acontecimientos

Deadline Cloud envía eventos EventBridge a Amazon para notificarte los cambios en el estado del servicio. Puedes usar EventBridge estos eventos para escribir reglas que tomen medidas, como notificarte, cuando se produzca un cambio en tu flota. Para obtener más información, consulta ¿Qué es Amazon? EventBridge

Cambio recomendado de tamaño de flota

Cuando configuras tu flota para usar el escalado automático basado en eventos, Deadline Cloud envía eventos que puedes usar para administrar tus flotas. Cada uno de estos eventos contiene información sobre el tamaño actual y el tamaño solicitado de una flota. Para ver un ejemplo del

uso de un EventBridge evento y un ejemplo de función Lambda para gestionar el evento, consulte. Amplíe automáticamente su flota de Amazon EC2 con la función de recomendación de escalado de Deadline Cloud

El evento de cambio de recomendación de tamaño de la flota se envía cuando ocurre lo siguiente:

- Cuando el tamaño de flota recomendado cambia y `oldFleetSize` es diferente de`newFleetSize`.
- Cuando el servicio detecta que el tamaño real de la flota no coincide con el tamaño de flota recomendado. Puede obtener el tamaño real de la flota a partir de `workerCount` la respuesta de la GetFleetoperación. Esto puede ocurrir cuando una instancia activa de Amazon EC2 no se registra como trabajadora de Deadline Cloud.

El evento tiene el siguiente formato:

```
{
    "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,
    }
}
```

Los siguientes campos definen el patrón del evento:

`"source": "aws.deadline"`

Identifica que el origen de este evento es Deadline Cloud.

`"detail-type": "Fleet Size Recommendation Change"`

Identifica el tipo de evento.

```
"detail": { }
```

Proporciona información sobre los cambios recomendados en el tamaño de la flota.

`"farmId": "farm-12345678900000000000000000000000"`

El identificador de la granja que contiene la flota.

`"fleetId": "fleet-12345678900000000000000000000000"`

El identificador de la flota que necesita un cambio de tamaño.

`"oldFleetSize": 1`

El tamaño actual de la flota.

`"newFleetSize": 5`

El nuevo tamaño recomendado de la flota.

Cuotas para Deadline Cloud

AWS Deadline Cloud proporciona recursos, como granjas, flotas y colas, que puede utilizar para procesar trabajos. Al crear los suyos Cuenta de AWS, establecemos las cuotas predeterminadas de estos recursos para cada uno de ellos. Región de AWS

Service Quotas es una ubicación central donde puede ver y administrar sus cuotas Servicios de AWS. También puede solicitar un aumento de cuota para muchos de los recursos que utilice.

Para ver las cuotas Deadline Cloud, abra la consola Service Quotas. En el panel de navegación, seleccione los Servicios de AWS y elija Deadline Cloud.

Para solicitar un aumento de cuota, consulte Solicitud de un aumento de cuota en la Guía de usuario de Service Quotas. Si la cuota aún no está disponible en Service Quotas, utilice el formulario de aumento de cuota de servicio.

Creación de recursos de AWS Deadline Cloud con AWS CloudFormation

AWS Deadline Cloud está integrado con AWS CloudFormation un servicio que te ayuda a modelar y configurar tus AWS recursos para que puedas dedicar menos tiempo a crear y gestionar tus recursos e infraestructura. Crea una plantilla que describe todos los AWS recursos que desea (como granjas, colas y flotas) y AWS CloudFormation aprovisiona y configura esos recursos por usted.

Cuando la utilices AWS CloudFormation, podrás reutilizar la plantilla para configurar tus recursos de Deadline Cloud de forma coherente y repetida. Describa sus recursos una vez y, a continuación, aprovisione los mismos recursos una y otra vez en varias Cuentas de AWS regiones.

Deadline Cloud y AWS CloudFormation plantillas

Para aprovisionar y configurar los recursos para Deadline Cloud y los servicios relacionados, debe conocer AWS CloudFormation las plantillas. Las plantillas son archivos de texto con formato JSON o YAML. Estas plantillas describen los recursos que deseas aprovisionar en tus AWS CloudFormation pilas. Si no estás familiarizado con JSON o YAML, puedes usar AWS CloudFormation Designer para ayudarte a empezar con AWS CloudFormation las plantillas. Para obtener más información, consulte ¿Qué es Designer de AWS CloudFormation ? en la Guía del usuario de AWS CloudFormation .

Deadline Cloud permite crear granjas, colas y flotas en. AWS CloudFormationPara obtener más información, incluidos ejemplos de plantillas JSON y YAML para granjas, colas y flotas, consulta AWS Deadline Cloud en la guía del usuario.AWS CloudFormation

Más información sobre AWS CloudFormation

Para obtener más información AWS CloudFormation, consulte los siguientes recursos:

- AWS CloudFormation
- AWS CloudFormation Guía del usuario
- AWS CloudFormation Referencia de la API
- AWS CloudFormation Guía del usuario de la interfaz de línea de comandos

Historial de documentos de la guía del usuario de Deadline Cloud

La siguiente tabla describe los cambios importantes en cada versión de la guía del usuario de AWS Deadline Cloud.

Cambio	Descripción	Fecha
Versión inicial	Esta es la versión inicial de la guía del usuario de Deadline Cloud.	2 de abril de 2024

AWS Glosario

Para obtener la AWS terminología más reciente, consulte el AWS glosario de la Glosario de AWS Referencia.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.