



Manual do usuário

# AWS Nuvem de prazos



Versão latest

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# AWS Nuvem de prazos: Manual do usuário

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

---

# Table of Contents

O que é Deadline Cloud? .....	1
Características do Deadline Cloud .....	1
Conceitos e terminologia .....	2
Introdução ao Deadline Cloud .....	4
Acessando o Deadline Cloud .....	5
Serviços relacionados .....	5
Como funciona o Deadline Cloud .....	6
.....	7
Permissões no Deadline Cloud .....	7
Suporte de software com Deadline Cloud .....	8
Conceitos básicos .....	9
Configurar a Conta da AWS .....	9
Configure seu monitor .....	10
Etapa 1: configurar seu monitor .....	10
Etapa 2: definir os detalhes da fazenda .....	13
Etapa 3: definir detalhes da fila .....	14
Etapa 4: Definir detalhes da frota .....	15
Etapa 5: Configurar os requisitos do trabalhador .....	16
Etapa 6: Definir níveis de acesso .....	16
Etapa 7: revisar e criar .....	17
Configurar uma estação de trabalho para desenvolvedores .....	17
Etapa 1: criar fazenda .....	18
Etapa 2: Executar o agente de trabalho .....	22
Etapa 3: enviar e executar trabalhos .....	24
Etapa 4: Executar trabalhos com anexos .....	32
Etapa 5: adicionar uma frota gerenciada por serviços .....	41
Etapa 6: limpar os recursos agrícolas .....	44
Configurar o remetente .....	47
Etapa 1: instalar o remetente do Deadline Cloud .....	47
Etapa 2: instalar e configurar o monitor Deadline Cloud .....	55
Etapa 3: Inicie o remetente do Deadline Cloud .....	58
Use a fazenda .....	62
Usando o monitor .....	63
Compartilhe o URL do monitor do Deadline Cloud .....	63

Abra o monitor Deadline Cloud .....	64
Exibir detalhes da fila e da frota .....	66
Visualize e gerencie trabalhos, etapas e tarefas .....	67
Exibir detalhes do trabalho .....	68
Exibir uma etapa .....	69
Exibir uma tarefa .....	69
Visualizar logs do .....	70
Baixe a saída finalizada .....	71
Fazendas .....	73
Crie uma fazenda .....	73
Excluir uma fazenda .....	73
Editar uma fazenda .....	74
Filas .....	75
Criar uma fila .....	75
Crie um ambiente de fila .....	77
Ambiente de Conda fila padrão .....	78
Excluir uma fila .....	79
Editar uma fila .....	79
Associe uma fila e uma frota .....	80
Gerenciando frotas .....	81
Frotas gerenciadas por serviços .....	81
Plataforma VFX .....	83
Frotas gerenciadas pelo cliente .....	84
Crie um CMF .....	84
Configuração do host do trabalhador .....	89
Gerenciar acesso .....	94
Instale software para trabalhos .....	97
Configurar credenciais do .....	98
Criar uma AMI .....	99
Crie uma infraestrutura de frota .....	102
Conecte-se a um endpoint de licença .....	112
Gerenciamento de usuários .....	117
Gerencie usuários e grupos para o monitor .....	117
Gerencie usuários e grupos para fazendas, filas e frotas .....	119
Tarefas .....	121
Envio de trabalhos .....	122

Mais opções para enviar trabalhos .....	124
Agendamento de trabalhos .....	126
Determine a compatibilidade da frota .....	126
Dimensionamento da frota .....	128
Sessões .....	128
Dependências de etapas .....	130
Estados do trabalho .....	131
Modificando trabalhos .....	134
Trabalhos de processamento .....	139
Solução de problemas de trabalhos .....	140
Por que a criação do meu emprego falhou? .....	140
Por que meu trabalho não é compatível? .....	140
Por que meu trabalho está pronto? .....	141
Por que meu trabalho falhou? .....	141
Por que minha etapa está pendente? .....	141
Armazenamento .....	142
Anexos de trabalho .....	142
Criptografia para buckets S3 de anexo de tarefas .....	143
Gerenciando anexos de tarefas em buckets do S3 .....	144
Sistema de arquivos virtual .....	144
Armazenamento compartilhado .....	147
Perfis de armazenamento no Deadline Cloud .....	147
Gerenciando orçamentos e uso .....	150
Suposições de custo .....	150
Usando o gerenciador de orçamento .....	151
Pré-requisito .....	152
Gerenciador de orçamento de acesso .....	152
Criar um orçamento .....	152
Exibir um orçamento .....	154
Editar um orçamento .....	154
Desativar um orçamento .....	154
Usando o explorador de uso .....	155
Pré-requisito .....	155
Abra o explorador de uso .....	155
Use o explorador de uso .....	155
Gerenciamento de custos .....	158

Melhores práticas de gerenciamento de custos .....	159
Segurança .....	162
Proteção de dados .....	163
Criptografia em repouso .....	164
Criptografia em trânsito .....	164
Gerenciamento de chaves .....	164
Privacidade do tráfego entre redes .....	174
Optar por não participar .....	175
Identity and Access Management .....	176
Público .....	177
Autenticando com identidades .....	177
Gerenciando acesso usando políticas .....	181
Como o Deadline Cloud funciona com o IAM .....	184
Exemplos de políticas baseadas em identidade .....	191
AWS políticas gerenciadas .....	196
Solução de problemas .....	199
Validação de conformidade .....	201
Resiliência .....	203
Segurança da infraestrutura .....	203
Análise de configuração e vulnerabilidade .....	204
Prevenção contra o ataque do “substituto confuso” em todos os serviços .....	204
AWS PrivateLink .....	206
Considerações .....	206
Deadline Cloud endpoints .....	207
Crie endpoints .....	207
Melhores práticas de segurança .....	208
Proteção de dados .....	209
Permissões do IAM .....	209
Execute trabalhos como usuários e grupos .....	210
Redes .....	210
Dados do trabalho .....	211
Estrutura da fazenda .....	211
Filas de anexação de trabalhos .....	212
Caixas de software personalizadas .....	214
Trabalhadores anfitriões .....	214
Estações de trabalho .....	216

---

Monitoramento .....	217
Fazendo login com CloudTrail .....	218
Informações do Deadline Cloud em CloudTrail .....	218
Compreendendo as entradas do arquivo de log do Deadline Cloud .....	222
Monitoramento com CloudWatch .....	224
Atuando em EventBridge eventos .....	225
Alteração na recomendação do tamanho da frota .....	225
Cotas .....	228
AWS CloudFormation recursos .....	229
Deadline Cloud e AWS CloudFormation modelos .....	229
Saiba mais sobre AWS CloudFormation .....	229
Histórico do documento .....	230
AWS Glossário .....	231
.....	ccxxxii

# O que é AWS Deadline Cloud?

O Deadline Cloud é um AWS service (Serviço da AWS) que você pode usar para criar e gerenciar projetos e trabalhos de renderização em instâncias do Amazon Elastic Compute Cloud (Amazon EC2) diretamente de estações de trabalho e pipelines de criação de conteúdo digital.

O Deadline Cloud fornece interfaces de console, aplicativos locais, ferramentas de linha de comando e uma API. Com o Deadline Cloud, você pode criar, gerenciar e monitorar fazendas, frotas, trabalhos, grupos de usuários e armazenamento. Você também pode especificar requisitos de hardware, criar ambientes para cargas de trabalho específicas e integrar as ferramentas de criação de conteúdo que sua produção exige em seu pipeline do Deadline Cloud.

O Deadline Cloud fornece uma interface unificada para gerenciar todos os seus projetos de renderização em um só lugar. Você pode gerenciar usuários, atribuir projetos a eles e conceder permissões para cargos.

## Tópicos

- [Características do Deadline Cloud](#)
- [Conceitos e terminologia do Deadline Cloud](#)
- [Introdução ao Deadline Cloud](#)
- [Acessando o Deadline Cloud](#)
- [Serviços relacionados](#)
- [Como funciona o Deadline Cloud](#)

## Características do Deadline Cloud

Aqui estão algumas das principais maneiras pelas quais o Deadline Cloud pode ajudar você a executar e gerenciar cargas de trabalho de computação visual:

- Crie rapidamente suas fazendas, filas e frotas. Monitore seu status e obtenha informações sobre a operação de sua fazenda e seus empregos.
- Gerencie centralmente usuários e grupos do Deadline Cloud e atribua permissões.
- Gerencie a segurança de login para usuários do projeto e provedores de identidade externos com AWS IAM Identity Center



- Gerencie com segurança o acesso aos recursos do projeto com políticas e funções AWS Identity and Access Management (IAM).
- Use tags para organizar e encontrar rapidamente os recursos do projeto.
- Gerencie o uso dos recursos do projeto e os custos estimados do seu projeto.
- Forneça uma ampla variedade de opções de gerenciamento de computação para oferecer suporte à renderização na nuvem ou pessoalmente.

## Conceitos e terminologia do Deadline Cloud

Para ajudar você a começar a usar AWS o Deadline Cloud, este tópico explica alguns de seus principais conceitos e terminologia.

### Gerente de orçamento

O gerente de orçamento faz parte do monitor Deadline Cloud. Use o gerenciador de orçamento para criar e gerenciar orçamentos. Você também pode usá-lo para limitar as atividades para ficar dentro do orçamento.

### Biblioteca de cliente Deadline Cloud

A biblioteca de cliente inclui uma interface de linha de comando e uma biblioteca para gerenciar o Deadline Cloud. A funcionalidade inclui enviar pacotes de tarefas com base na especificação Open Job Description para o Deadline Cloud, baixar saídas de anexos de tarefas e monitorar sua fazenda usando a interface de linha de comando.

### Aplicativo de criação de conteúdo digital (DCC)

Os aplicativos de criação de conteúdo digital (DCCs) são produtos de terceiros nos quais você cria conteúdo digital. Exemplos de DCCs são MayaNuke, e. Houdini O Deadline Cloud fornece plug-ins integrados ao remetente de trabalhos para DCCs específicos.

### Farm

Uma fazenda é o local onde os recursos do seu projeto estão localizados. Consiste em filas e frotas.

### Frota

Uma frota é um grupo de nós de trabalho que fazem a renderização. Os nós de trabalho processam trabalhos. Uma frota pode ser associada a várias filas e uma fila pode ser associada a várias frotas.

## Trabalho

Um trabalho é uma solicitação de renderização. Os usuários enviam trabalhos. Os trabalhos contêm propriedades de trabalho específicas que são descritas como etapas e tarefas.

### Anexos de trabalho

Um anexo de trabalho é um recurso do Deadline Cloud que você pode usar para gerenciar entradas e saídas de trabalhos. Os arquivos de trabalho são enviados como anexos do trabalho durante o processo de renderização. Esses arquivos podem ser texturas, modelos 3D, equipamentos de iluminação e outros itens similares.

### Propriedades do trabalho

As propriedades do trabalho são configurações que você define ao enviar um trabalho de renderização. Alguns exemplos incluem faixa de quadros, caminho de saída, anexos de tarefas, câmera renderizável e muito mais. As propriedades variam com base no DCC do qual a renderização é enviada.

### Modelo de trabalho

Um modelo de trabalho define o ambiente de execução e todos os processos que são executados como parte de um trabalho do Deadline Cloud.

### Fila

Uma fila é onde os trabalhos enviados estão localizados e programados para serem renderizados. Uma fila deve estar associada a uma frota para criar uma renderização bem-sucedida. Uma fila pode ser associada a várias frotas.

### Associação de filas e frotas

Quando uma fila é associada a uma frota, há uma associação fila-frota. Use uma associação para programar trabalhadores de uma frota para trabalhos nessa fila. Você pode iniciar e interromper associações para controlar o agendamento do trabalho.

### Etapas

Uma etapa é um processo específico a ser executado na tarefa.

### Remetente do Deadline Cloud

Um remetente do Deadline Cloud é um plug-in de criação de conteúdo digital (DCC). Os artistas o usam para enviar trabalhos a partir de uma interface de DCC de terceiros com a qual estão familiarizados.

## Tags

Uma tag é um rótulo que você pode atribuir a um AWS recurso. Cada tag consiste de uma chave e um valor opcional definido por você.

Com as tags, você pode categorizar seus AWS recursos de maneiras diferentes. Por exemplo, é possível definir um conjunto de tags para as instâncias do Amazon EC2 da sua conta que vão ajudar a rastrear o proprietário e o nível da pilha de cada instância.

Você também pode categorizar seus AWS recursos por finalidade, proprietário ou ambiente. Essa abordagem é útil quando você tem muitos recursos do mesmo tipo. Você pode identificar rapidamente um recurso específico com base nas tags que você atribuiu a ele.

## Tarefa

Uma tarefa é um componente único de uma etapa de renderização.

## Licenciamento baseado no uso (UBL)

O licenciamento baseado no uso (UBL) é um modelo de licenciamento sob demanda que está disponível para produtos selecionados de terceiros. Esse modelo é pago conforme o uso e você é cobrado pelo número de horas e minutos que usa.

## Explorador de uso

O explorador de uso é um recurso do monitor Deadline Cloud. Ele fornece uma estimativa aproximada de seus custos e uso.

## Operador

Os trabalhadores pertencem a frotas e executam tarefas atribuídas ao Deadline Cloud para concluir etapas e trabalhos. Os trabalhadores armazenam os registros das operações de tarefas no Amazon CloudWatch Logs. Os trabalhadores também podem usar o recurso de anexos de trabalho para sincronizar entradas e saídas em um bucket do Amazon Simple Storage Service (Amazon S3).

# Introdução ao Deadline Cloud

Use o Deadline Cloud para criar rapidamente um render farm com configurações e recursos padrão, como a configuração da instância do Amazon EC2 e os buckets do Amazon Simple Storage Service (Amazon S3).

Você também pode definir as configurações e os recursos ao criar uma fazenda de renderização. Esse método leva mais tempo do que usar as configurações e os recursos padrão, mas oferece mais controle.

Depois de se familiarizar com [os conceitos e a terminologia](#) do Deadline Cloud, consulte [Introdução](#) para obter step-by-step instruções sobre como criar sua fazenda, adicionar usuários e links para informações úteis.

## Acessando o Deadline Cloud

Você pode acessar o Deadline Cloud de qualquer uma das seguintes formas:

- Console Deadline Cloud — Acesse o console em um navegador para criar uma fazenda e seus recursos e gerenciar o acesso dos usuários. Para obter mais informações, consulte [Conceitos básicos](#).
- Deadline Cloud Monitor — gerencie seus trabalhos de renderização, incluindo a atualização de prioridades e status dos trabalhos. Monitore sua fazenda e visualize os registros e o status do trabalho. Para usuários com permissões de proprietário, o monitor Deadline Cloud também fornece acesso para explorar o uso e criar orçamentos. O monitor Deadline Cloud está disponível como navegador da web e aplicativo de desktop.
- AWS SDK e AWS CLI — Use o AWS Command Line Interface (AWS CLI) para chamar as operações da Deadline Cloud API a partir da linha de comando em seu sistema local. Para obter mais informações, consulte [Configurar uma estação de trabalho para desenvolvedores](#).

## Serviços relacionados

O Deadline Cloud funciona com o seguinte Serviços da AWS:

- Amazon CloudWatch — Com CloudWatch, você pode monitorar seus projetos e AWS recursos associados. Para obter mais informações, consulte o [Guia CloudWatch do usuário da Amazon](#).
- Amazon EC2 — Isso AWS service (Serviço da AWS) fornece servidores virtuais que executam seus aplicativos na nuvem. Você pode configurar seus projetos para usar instâncias do Amazon EC2 para suas cargas de trabalho. Para obter mais informações, consulte [Instâncias do Amazon EC2](#).
- Amazon EC2 Auto Scaling — Com o Auto Scaling, você pode aumentar ou diminuir automaticamente o número de instâncias à medida que a demanda por suas instâncias muda. O Auto Scaling ajuda a garantir que você esteja executando o número desejado de instâncias,

mesmo se uma instância falhar. Se você habilitar o Auto Scaling com o Deadline Cloud, as instâncias iniciadas pelo Auto Scaling serão automaticamente registradas com a carga de trabalho. Da mesma forma, as instâncias encerradas pelo Auto Scaling são automaticamente canceladas do registro da carga de trabalho. Para obter mais informações, consulte o Guia do usuário do [Amazon EC2 Auto Scaling](#).

- **AWS PrivateLink**— AWS PrivateLink fornece conectividade privada entre nuvens privadas virtuais (VPCs) e suas redes locais, sem expor seu tráfego à Internet pública. Serviços da AWS AWS PrivateLink facilita a conexão de serviços em diferentes contas e VPCs. Para ter mais informações, consulte [AWS PrivateLink](#).
- **Amazon S3** — O Amazon S3 é um serviço de armazenamento de objetos. O Deadline Cloud usa buckets do Amazon S3 para armazenar anexos de trabalhos.
- **IAM Identity Center** — O IAM Identity Center é um AWS service (Serviço da AWS) local onde você pode fornecer aos usuários acesso de login único a todas as contas e aplicativos atribuídos em um só lugar. Você também pode ter um gerenciamento centralizado do acesso a várias contas e permissões de usuário para todas as suas contas no AWS Organizations. Para obter mais informações, consulte [Perguntas frequentes sobre o AWS IAM Identity Center](#).

## Como funciona o Deadline Cloud

Com o Deadline Cloud, você pode criar e gerenciar projetos e trabalhos de renderização diretamente dos pipelines e estações de trabalho de criação de conteúdo digital (DCC).

Você envia trabalhos para o Deadline Cloud usando o AWS SDK, AWS Command Line Interface (AWS CLI) ou os remetentes de trabalhos do Deadline Cloud. O Deadline Cloud suporta a Open Job Description (OpenJD) para a especificação do modelo de trabalho. Para obter mais informações, consulte [Open Job Description](#) no GitHub site.

O Deadline Cloud fornece candidatos a vagas. Um remetente de trabalhos é um plug-in DCC para enviar trabalhos de renderização a partir de uma interface DCC de terceiros, como ou. Maya Nuke Com um remetente, os artistas podem enviar trabalhos de renderização de uma interface de terceiros para o Deadline Cloud, onde os recursos do projeto são gerenciados e os trabalhos são monitorados, tudo em um único local.

Com um farm do Deadline Cloud, você pode criar filas e frotas, gerenciar usuários e gerenciar o uso e os custos dos recursos do projeto. Uma fazenda consiste em filas e frotas. Uma fila é onde os trabalhos enviados estão localizados e programados para serem renderizados. Uma frota é um grupo de nós de trabalho que executam tarefas para concluir trabalhos. Uma fila deve estar

associada a uma frota para que os trabalhos possam ser renderizados. Uma única frota pode suportar várias filas e uma fila pode ser suportada por várias frotas.

Os trabalhos consistem em etapas, e cada etapa consiste em tarefas específicas. Com o monitor Deadline Cloud, você pode acessar status, registros e outras métricas de solução de problemas para trabalhos, etapas e tarefas.

## Permissões no Deadline Cloud

O Deadline Cloud oferece suporte ao seguinte:

- Gerenciando o acesso às suas operações de API usando AWS Identity and Access Management (IAM)
- Gerenciando o acesso dos usuários da força de trabalho usando uma integração com AWS IAM Identity Center

Antes que qualquer pessoa possa trabalhar em um projeto, ela deve ter acesso a esse projeto e à fazenda associada. O Deadline Cloud é integrado ao IAM Identity Center para gerenciar a autenticação e autorização da força de trabalho. Os usuários podem ser adicionados diretamente ao IAM Identity Center ou podem ser conectados ao seu provedor de identidade (IdP) existente, como Okta ou Active Directory. Os administradores de TI podem conceder permissões de acesso a usuários e grupos em diferentes níveis. Cada nível subsequente inclui as permissões dos níveis anteriores. A lista a seguir descreve os quatro níveis de acesso, do nível mais baixo ao mais alto:

- Visualizador — Permissão para ver recursos nas fazendas, filas, frotas e trabalhos aos quais eles têm acesso. Um espectador não pode enviar nem fazer alterações nas vagas.
- Colaborador — O mesmo que um espectador, mas com permissão para enviar trabalhos para uma fila ou fazenda.
- Gerente — O mesmo que colaborador, mas com permissão para editar trabalhos nas filas às quais eles têm acesso e conceder permissões sobre os recursos aos quais eles têm acesso.
- Proprietário — O mesmo que gerente, mas pode visualizar e criar orçamentos e ver o uso.

### Note

Essas permissões não dão aos usuários acesso AWS Management Console ou permissão para modificar a infraestrutura do Deadline Cloud.

Os usuários devem ter acesso a uma fazenda antes de poderem acessar as filas e frotas associadas. O acesso do usuário é atribuído a filas e frotas separadamente dentro de uma fazenda.

Você pode adicionar usuários como indivíduos ou como parte de um grupo. Adicionar grupos a uma fazenda, frota ou fila pode facilitar o gerenciamento das permissões de acesso para grandes grupos de pessoas. Por exemplo, se você tem uma equipe que está trabalhando em um projeto específico, você pode adicionar cada um dos membros da equipe a um grupo. Em seguida, você pode conceder permissões de acesso a todo o grupo para a fazenda, frota ou fila correspondente.

## Suporte de software com Deadline Cloud

O Deadline Cloud funciona com qualquer aplicativo de software que pode ser executado a partir de uma interface de linha de comando e controlado usando valores de parâmetros. O Deadline Cloud suporta a OpenJD especificação para descrever o trabalho como trabalhos com etapas de script de software que são parametrizadas (como em um intervalo de quadros) em tarefas. OpenJD reúne instruções de trabalho em pacotes de tarefas com as ferramentas e os recursos do Deadline Cloud para criar, executar e licenciar as etapas de um aplicativo de software de terceiros.

Os trabalhos precisam de licenciamento para serem renderizados. O Deadline Cloud oferece licenciamento baseado no uso (UBL) para uma seleção de licenças de aplicativos de software que são cobradas por incrementos de hora em minuto com base no uso. Com o Deadline Cloud, você também pode usar suas próprias licenças de software, se quiser. Se um trabalho não puder acessar uma licença, ele não será renderizado e produzirá um erro exibido no registro de tarefas no monitor do Deadline Cloud.

# Começando com o Deadline Cloud

Para criar uma fazenda no AWS Deadline Cloud, você pode usar o [console do Deadline Cloud](#) ou o AWS Command Line Interface (AWS CLI). Use o console para uma experiência guiada na criação da fazenda, incluindo filas e frotas. Use o AWS CLI para trabalhar diretamente com o serviço ou para desenvolver suas próprias ferramentas que funcionem com o Deadline Cloud.

Para criar uma fazenda e usar o monitor do Deadline Cloud, configure sua conta no Deadline Cloud. Você só precisa configurar a infraestrutura de monitoramento do Deadline Cloud uma vez por conta. Na sua fazenda, você pode gerenciar seu projeto, incluindo o acesso do usuário à sua fazenda e seus recursos.

Para criar uma fazenda sem configurar a infraestrutura de monitoramento do Deadline Cloud, configure uma estação de trabalho de desenvolvedor para o Deadline Cloud.

Para criar uma fazenda com recursos mínimos para aceitar trabalhos, selecione Início rápido na página inicial do console. [Configurar o monitor Deadline Cloud](#) orienta você por essas etapas. Essas fazendas começam com uma fila e uma frota que são associadas automaticamente. Essa abordagem é uma maneira conveniente de criar fazendas no estilo sandbox para fazer experiências.

## Tópicos

- [Configurar a Conta da AWS](#)
- [Configurar o monitor Deadline Cloud](#)
- [Configurando uma estação de trabalho de desenvolvedor para o Deadline Cloud](#)
- [Configurar remetentes do Deadline Cloud](#)
- [Use a fazenda](#)

## Configurar a Conta da AWS

Configure seu Conta da AWS para usar o AWS Deadline Cloud.

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar um.

Para se inscrever em um Conta da AWS

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



## 2. Siga as instruções online.

Parte do procedimento de inscrição envolve receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.

Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWS é criado. O usuário raiz tem acesso a todos os Serviços da AWS e atributos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar [tarefas que exigem acesso de usuário-raiz](#).

Ao criar um pela primeira vez Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta.

### Important

É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte [Tarefas que exigem credenciais de usuário raiz](#) no Guia do Usuário do IAM.

## Configurar o monitor Deadline Cloud


Para começar, você precisará criar sua infraestrutura de monitoramento do Deadline Cloud e definir sua fazenda. Você também pode realizar etapas adicionais opcionais, incluindo adicionar grupos e usuários, escolher uma função de serviço e adicionar tags aos seus recursos.

### Etapa 1: configurar seu monitor

O monitor Deadline Cloud usa AWS IAM Identity Center para autorizar usuários. A instância do IAM Identity Center que você usa para o Deadline Cloud deve estar na Região da AWS mesma do monitor. Se o console estiver usando uma região diferente ao criar o monitor, você receberá um lembrete para mudar para a região do Centro de Identidades do IAM.


A infraestrutura do seu monitor consiste nos seguintes componentes:

- Nome de exibição do monitor: O nome de exibição do monitor é como você pode identificar seu monitor — por exemplo, AnyCompany monitor. O nome do seu monitor também determina a URL do seu monitor.

 Important


Você não pode alterar o nome de exibição do monitor depois de concluir a configuração.

- URL do monitor: você pode acessar seu monitor usando o URL do monitor. O URL é baseado no nome de exibição do Monitor — por exemplo, <https://anycompanymonitor.awsapps.com>.

 Important

Você não pode alterar o URL do Monitor depois de concluir a configuração.

- Região da AWS: Região da AWS é o local físico de uma coleção de AWS data centers. Quando você configura seu monitor, o padrão da Região é o local mais próximo de você. Recomendamos alterar a região para que ela fique mais próxima de seus usuários. Isso reduz o atraso e melhora as velocidades de transferência de dados. AWS IAM Identity Center deve ser habilitado da mesma forma que Região da AWS o Deadline Cloud.

 Important

Você não pode alterar sua região depois de concluir a configuração do Deadline Cloud.

Conclua as tarefas nesta seção para configurar a infraestrutura do seu monitor.

Para configurar a infraestrutura do seu monitor

1. Faça login no para iniciar AWS Management Console configuração do Welcome to Deadline Cloud e escolha Avançar.
2. Insira o nome de exibição do monitor — por exemplo **AnyCompany Monitor**.
3. (Opcional) Para alterar o nome do monitor, escolha Editar URL.
4. (Opcional) Para alterar o para que Região da AWS fique mais próximo de seus usuários, escolha Alterar região.
  - a. Escolha a região mais próxima para a maioria dos seus usuários.

- b. Escolha Aplicar região.
  - (Opcional) Para adicionar grupos e usuários, selecione [\(Opcional\) Adicionar grupos e usuários](#).
  - (Opcional) Para personalizar ainda mais a configuração do monitor, selecione [Configurações adicionais](#).
5. Se você estiver pronto [Etapa 2: definir os detalhes da fazenda](#), escolha Avançar.

## (Opcional) Adicionar grupos e usuários

Antes de concluir a configuração do monitor do Deadline Cloud, você pode adicionar usuários do monitor e adicioná-los a um grupo.

Depois que a configuração estiver concluída, você poderá criar novos usuários e grupos e gerenciar usuários, atribuindo-lhes grupos, permissões e aplicativos ou excluindo usuários do seu monitor.

## Configurações adicionais

A configuração do Deadline Cloud inclui configurações adicionais. Com essas configurações, você pode ver todas as alterações que a configuração do Deadline Cloud faz em sua Conta da AWS, configurar sua função de usuário de monitor e alterar o tipo de chave de criptografia.

### AWS IAM Identity Center

AWS IAM Identity Center é um serviço de login único baseado em nuvem para gerenciar usuários e grupos. O IAM Identity Center também pode ser integrado ao seu provedor corporativo de autenticação única (SSO) para que os usuários possam fazer login com a conta da empresa.

O Deadline Cloud habilita o IAM Identity Center por padrão, e é necessário configurar e usar o Deadline Cloud. A instância do IAM Identity Center que você usa para o Deadline Cloud deve estar na Região da AWS mesma do monitor. Para obter mais informações, consulte [O que é AWS IAM Identity Center](#).

### Configurar a função de acesso ao serviço

Um AWS serviço pode assumir uma função de serviço para realizar ações em seu nome. O Deadline Cloud exige uma função de usuário de monitor para dar aos usuários acesso aos recursos em seu monitor.

Você pode anexar políticas gerenciadas AWS Identity and Access Management (IAM) à função de usuário do monitor. As políticas permitem que os usuários realizem determinadas ações, como criar empregos em um aplicativo específico do Deadline Cloud. Como as aplicações dependem de condições específicas na política gerenciada, se você não usar as políticas gerenciadas, a aplicação pode não funcionar conforme o esperado.

Você pode alterar a função do usuário do monitor depois de concluir a configuração, a qualquer momento. Para obter mais informações sobre perfis de usuário, consulte [Perfis do IAM](#).

As guias a seguir contêm instruções para dois casos de uso diferentes. Para criar e usar um novo perfil de serviço, escolha a guia Novo perfil de serviço. Para usar um perfil de serviço existente, escolha a guia Perfil de serviço existente.

### New service role

Para criar e usar um novo perfil de serviço

1. Selecione Criar e usar um novo perfil de serviço.
2. (Opcional) Insira um nome de perfil de usuário do serviço.
3. Escolha Exibir detalhes da permissão para obter mais informações sobre a função.

### Existing service role

Para usar um perfil de serviço existente

1. Selecione Usar um perfil de serviço existente.
2. Abra a lista suspensa para escolher um perfil de serviço existente.
3. (Opcional) Escolha Exibir no console do IAM para obter mais informações sobre o perfil.

## Etapa 2: definir os detalhes da fazenda

De volta ao console do Deadline Cloud, conclua as etapas a seguir para definir os detalhes da fazenda.

1. Em Detalhes da fazenda, adicione um nome para a fazenda.
2. Em Descrição, insira a descrição da fazenda. Uma descrição clara pode ajudá-lo a identificar rapidamente o propósito da sua fazenda.

3. (Opcional) Por padrão, seus dados são criptografados com uma chave que AWS possui e gerencia para sua segurança. Você pode escolher Personalizar configurações de criptografia (avançadas) para usar uma chave existente ou criar uma nova que você gerencie.

Se você optar por personalizar as configurações de criptografia usando a caixa de seleção, insira um AWS KMS ARN ou crie um AWS KMS novo escolhendo Criar nova chave KMS.

4. (Opcional) Escolha Adicionar nova tag para adicionar uma ou mais tags à sua fazenda.
5. Escolha uma das seguintes opções:
  - Selecione Ir para revisar e Criar para [revisar e criar sua fazenda](#).
  - Selecione Avançar para prosseguir com as etapas adicionais opcionais.

## (Opcional) Etapa 3: definir detalhes da fila

A fila é responsável por acompanhar o progresso e programar o trabalho para seus trabalhos.

1. Começando nos detalhes da fila, forneça um nome para a fila.
2. Em Descrição, insira a descrição da fila. Uma descrição clara pode ajudar você a identificar rapidamente a finalidade da sua fila.
3. Para anexos de trabalho, você pode criar um novo bucket do Amazon S3 ou escolher um bucket do Amazon S3 existente. Se você não tiver um bucket Amazon S3 existente, precisará criar um.
  - a. Para criar um novo bucket do Amazon S3, selecione Create new job bucket. Você pode definir o nome do bucket de tarefas no campo Prefixo raiz. Recomendamos ligar para o bucket **deadlinecloud-job-attachments-[MONITORNAME]**.

Você só pode usar letras minúsculas e traços. Sem espaços ou caracteres especiais.
  - b. Para pesquisar e selecionar um bucket existente do Amazon S3, selecione Escolher do bucket do Amazon S3 existente. Em seguida, pesquise um bucket existente escolhendo Browse S3. Quando a lista de seus buckets do Amazon S3 disponíveis for exibida, selecione o bucket do Amazon S3 que você deseja usar para sua fila.
4. Se você estiver usando frotas gerenciadas pelo cliente, selecione Habilitar associação com frotas gerenciadas pelo cliente.
  - Para frotas gerenciadas pelo cliente, adicione um usuário configurado em fila e, em seguida, defina as credenciais POSIX e/ou Windows. Como alternativa, você pode ignorar a funcionalidade de execução como marcando a caixa de seleção.

5. Sua fila requer permissão para acessar o Amazon S3 em seu nome. Recomendamos que você crie uma nova função de serviço para cada fila.
  - a. Para uma nova função, conclua as etapas a seguir.
    - i. Selecione Criar e usar um novo perfil de serviço.
    - ii. Insira um nome de função para sua função na fila ou use o nome de função fornecido.
    - iii. (Opcional) Adicione uma descrição da função de fila.
    - iv. Você pode ver as permissões do IAM para a função de fila escolhendo Exibir detalhes da permissão.
  - b. Como alternativa, você pode escolher uma função de serviço existente.
6. (Opcional) Adicione variáveis de ambiente para o ambiente de fila usando pares de nome e valor.
7. (Opcional) Adicione tags à fila usando pares de chaves e valores.

Depois de inserir todos os detalhes da fila, selecione Avançar.

## (Opcional) Etapa 4: Definir detalhes da frota

Uma frota aloca trabalhadores para executar suas tarefas de renderização. Se você precisar de uma frota para suas tarefas de renderização, marque a caixa Criar frota.

1. Detalhes da frota
  - a. Forneça um nome e uma descrição opcional para sua frota.
  - b. Selecione a forma como seus recursos computacionais devem ser escalados. A opção de gerenciamento de serviços permite que o Deadline Cloud escale automaticamente seus recursos de computação. A opção Gerenciado pelo cliente deixa você no controle de sua própria escalabilidade computacional.
2. Na seção Opções de instância, escolha Spot ou On-demand. As instâncias sob demanda do Amazon EC2 oferecem disponibilidade mais rápida e as instâncias spot do Amazon EC2 são melhores para esforços de redução de custos.
3. Para escalonar automaticamente o número de instâncias em sua frota, escolha um número mínimo de instâncias e um número máximo de instâncias.

É altamente recomendável sempre definir o número mínimo de instâncias **0** para evitar custos extras.

4. Sua frota precisa de permissão para escrever CloudWatch em seu nome. Recomendamos que você crie uma nova função de serviço para cada frota.
  - a. Para uma nova função, conclua as etapas a seguir.
    - i. Selecione Criar e usar um novo perfil de serviço.
    - ii. Insira um nome de função para sua função de frota ou use o nome de função fornecido.
    - iii. (Opcional) Adicione uma descrição da função da frota.
    - iv. Você pode ver as permissões do IAM para a função de frota escolhendo Exibir detalhes da permissão.
  - b. Como alternativa, você pode usar uma função de serviço existente.
5. (Opcional) Adicione etiquetas para a frota usando pares de chaves e valores.

Depois de inserir todos os detalhes da frota, selecione Avançar.

## (Opcional) Etapa 5: Configurar os requisitos do trabalhador

Defina os requisitos para suas instâncias de trabalho.

1. Revise as configurações do sistema operacional (SO) e da arquitetura da CPU para verificar.
2. Atualize o número mínimo e máximo de vCPUs de acordo com seus requisitos de hardware.
3. Atualize o número mínimo e máximo de memória (GiB) de acordo com seus requisitos de hardware.
4. Você pode filtrar os tipos de instância permitindo ou excluindo tipos de instâncias de trabalho. Nas duas opções de filtragem, você pode filtrar até 10 tipos de instância do Amazon EC2.
5. Em Requisitos adicionais (opcional), você pode definir o volume raiz do EBS por tamanho (GiB), IOPS e taxa de transferência (MiB/s).
6. Depois que todos os requisitos de trabalhadores estiverem definidos, escolha Avançar para definir o nível de acesso dos seus grupos.

## (Opcional) Etapa 6: definir níveis de acesso

Se você tiver grupos conectados ao seu monitor, poderá definir o nível de acesso deles. A permissão para usar os recursos do Deadline Cloud é gerenciada por níveis de acesso. Você pode atribuir diferentes níveis de acesso a grupos de usuários.

1. Use o menu de nível de acesso à fazenda do Deadline Cloud para selecionar o nível de permissão para o grupo.
2. Escolha Avançar para continuar e revisar todos os detalhes da fazenda inseridos.

## Etapa 7: revisar e criar

Revise todas as informações inseridas para criar sua fazenda. Quando estiver pronto, escolha Criar fazenda.

O progresso da criação da sua fazenda é exibido na página Fazendas. Uma mensagem de sucesso é exibida quando sua fazenda está pronta para uso.

## Configurando uma estação de trabalho de desenvolvedor para o Deadline Cloud

Neste tutorial, você usará AWS CloudShell para criar um farm de desenvolvedores simples e executar o agente de trabalho. Em seguida, você pode enviar e executar um trabalho simples com parâmetros e anexos, adicionar uma frota gerenciada por serviços e limpar os recursos da fazenda quando terminar.

As seções a seguir apresentam os diferentes recursos do Deadline Cloud e como eles funcionam e funcionam juntos. Seguir essas etapas é útil para desenvolver e testar novas cargas de trabalho e personalizações.

### Tópicos

- [Etapa 1: criar um Deadline Cloud Farm](#)
- [Etapa 2: executar o agente de trabalho no modo de desenvolvedor no Deadline Cloud](#)
- [Etapa 3: enviar e executar trabalhos com o Deadline Cloud](#)
- [Etapa 4: Executar trabalhos com anexos de trabalhos no Deadline Cloud](#)
- [Etapa 5: adicione uma frota gerenciada por serviços à sua fazenda de desenvolvedores no Deadline Cloud](#)
- [Etapa 6: limpe os recursos da sua fazenda no Deadline Cloud](#)



## Etapa 1: criar um Deadline Cloud Farm

Para criar sua fazenda de desenvolvedores e enfileirar recursos no AWS Deadline Cloud, use o AWS Command Line Interface (AWS CLI), conforme mostrado no procedimento a seguir. Você também criará uma função AWS Identity and Access Management (IAM) e uma frota gerenciada pelo cliente (CMF) e associará a frota à sua fila. Em seguida, você pode configurar AWS CLI e confirmar se sua fazenda está configurada e funcionando conforme especificado.

Você pode usar essa fazenda para explorar os recursos do Deadline Cloud e, em seguida, desenvolver e testar novas cargas de trabalho, personalizações e integrações de pipeline.

Para criar uma fazenda

1. Instale e configure o AWS Command Line Interface (AWS CLI), caso ainda não tenha feito isso. Para obter informações, consulte [Instalar ou atualizar para a versão mais recente do AWS CLI](#).
2. Crie um nome para sua fazenda e adicione esse nome à `~/ .bashrc`. Isso o disponibilizará para outras sessões do terminal.

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

3. Crie o recurso da fazenda e adicione seu ID da fazenda `~/ .bashrc` a.

```
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. Crie o recurso de fila e adicione seu ID de fila ao `~/ .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. Crie uma função do IAM para a frota. Essa função fornece aos anfitriões de trabalhadores em sua frota as credenciais de segurança necessárias para executar trabalhos em sua fila.

```
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. Crie a frota gerenciada pelo cliente (CMF) e adicione sua ID de frota 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. Certifique-se de que você possa acessar o Deadline Cloud.

```
pip install deadline
```

8. Associe o CMF à sua fila.

```

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

```

9. Para definir a fazenda padrão como a ID da fazenda e a fila como a ID da fila que você criou anteriormente, use o comando a seguir.

```

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

```

10. (Opcional) Para confirmar se sua fazenda está configurada de acordo com suas especificações, use os seguintes comandos:

- Listar todas as fazendas — **deadline farm list**
- Listar todas as filas na fazenda padrão — **deadline queue list**
- Listar todas as frotas na fazenda padrão — **deadline fleet list**
- Obtenha a fazenda padrão — **deadline farm get**
- Obtenha a fila padrão — **deadline queue get**
- Obtenha todas as frotas associadas à fila padrão — **deadline fleet get**

## Etapa 2: executar o agente de trabalho no modo de desenvolvedor no Deadline Cloud

Antes de executar os trabalhos enviados para a fila em seu farm de desenvolvedores, você deve executar o agente de trabalho do AWS Deadline Cloud no modo desenvolvedor em um host de trabalho.

Durante o restante deste tutorial, você executará AWS CLI operações em seu farm de desenvolvedores usando duas AWS CloudShell guias. Na primeira guia, você pode enviar trabalhos. Na segunda guia, você pode executar o agente de trabalho.

### Note

Se você deixar sua CloudShell sessão ociosa por mais de 20 minutos, o tempo limite será atingido e o agente de trabalho será interrompido. Para reiniciar o agente de trabalho, siga as instruções no procedimento a seguir.

Para executar o agente de trabalho no modo de desenvolvedor

1. Instale e configure o AWS Command Line Interface (AWS CLI), caso ainda não tenha feito isso. Para obter informações, consulte [Instalar ou atualizar para a versão mais recente do AWS CLI](#).
2. Com sua fazenda ainda aberta na primeira CloudShell guia, abra uma segunda CloudShell guia `demoenv-logs` e crie os `demoenv-persist` diretórios e.

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

3. Baixe e instale os pacotes do agente Deadline Cloud Worker do PyPI:

### Note

`AtivadoWindows`, é necessário que os arquivos do agente sejam instalados no diretório global de pacotes de sites do Python. Atualmente, não há suporte para ambientes virtuais Python.

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

- Para permitir que o agente de trabalho crie os diretórios temporários para execução de trabalhos, crie um diretório:

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

- Execute o agente Deadline Cloud Worker no modo de desenvolvedor com as variáveis DEV\_FARM\_ID e DEV\_CMF\_ID que você adicionou ao ~/.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
```

Conforme o agente de trabalho inicializa e, em seguida, pesquisa a operação da UpdateWorkerSchedule API, a seguinte saída é exibida:

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

- Selecione sua primeira CloudShell guia e, em seguida, liste os trabalhadores da frota.

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

Uma saída como a seguinte é exibida:

```
Displaying 1 of 1 workers starting at 0  
  
- workerId: worker-8c9af877c8734e89914047111f  
  status: STARTED  
  createdAt: 2023-12-13 20:43:06+00:00
```

Em uma configuração de produção, o agente do Deadline Cloud Worker exige a configuração de vários usuários e diretórios de configuração como usuário administrativo na máquina host. Você pode substituir essas configurações porque está executando trabalhos em sua própria fazenda de desenvolvimento, que somente você pode acessar.

## Etapa 3: enviar e executar trabalhos com o Deadline Cloud

Para usar o AWS Deadline Cloud para executar trabalhos, use os procedimentos a seguir. Use a primeira AWS CloudShell guia para enviar trabalhos para sua fazenda de desenvolvedores. Use a segunda CloudShell guia para visualizar a saída do agente de trabalho.

### Tópicos

- [Envie a simple\\_job amostra](#)
- [Envie um simple\\_job com um parâmetro](#)
- [Crie um pacote de tarefas simple\\_file\\_job com E/S de arquivo](#)

### Envie a simple\_job amostra

Depois de criar uma fazenda e executar o agente de trabalho, você pode enviar a simple\_job amostra para o Deadline Cloud.

Para enviar a simple\_job amostra para o Deadline Cloud

1. Instale e configure o AWS Command Line Interface (AWS CLI), caso ainda não tenha feito isso. Para obter informações, consulte [Instalar ou atualizar para a versão mais recente do AWS CLI](#).
2. Faça o download da amostra em GitHub.

```
cd ~
```

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

- Escolha sua primeira CloudShell guia e, em seguida, navegue até o diretório de exemplos do pacote de tarefas.

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

- Envie a `simple_job` amostra.


```
deadline bundle submit simple_job
```

- Escolha sua segunda CloudShell guia para ver a saída de registro sobre chamadas `BatchGetJobEntities`, obtenção de uma sessão e execução de uma ação de sessão.

```
...
[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

Somente a saída de registro do agente de trabalho é mostrada. Há um registro separado para a sessão que executa o trabalho.

6. Escolha sua primeira guia e, em seguida, inspecione os arquivos de log que o agente de trabalho grava.
  - a. Navegue até o diretório de registros do agente de trabalho e visualize seu conteúdo.

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

- b. Imprima o primeiro arquivo de log criado pelo agente de trabalho.

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

Esse arquivo contém a saída do agente de trabalho sobre como ele chamou a API Deadline Cloud para criar um recurso de trabalhador em sua frota e, em seguida, assumiu a função de frota.

- c. Imprima a saída do arquivo de log quando o agente de trabalho se junta à frota.

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

Esse registro contém saídas sobre todas as ações que o agente de trabalho realiza, mas não contém saídas sobre as filas a partir das quais ele executa trabalhos, exceto as IDs desses recursos.

- d. Imprima os arquivos de log de cada sessão em um diretório com o mesmo nome do ID do recurso da fila.

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

Se o trabalho for bem-sucedido, a saída do arquivo de log será semelhante à seguinte:

```
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_files_gj55_/tmp2u9yqtsz
2024-03-27 16:00:22,406 INFO Wrote: runScript -> /sessions/
session-053d77cef82648fea9c698271812a/embedded_files_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 informações sobre o trabalho.

```
deadline job get
```

Quando você envia o trabalho, o sistema o salva como padrão para que você não precise inserir o ID do trabalho.

## Envie um `simple_job` com um parâmetro

Você pode enviar trabalhos com parâmetros. No procedimento a seguir, você edita o `simple_job` modelo para incluir uma mensagem personalizada, envia e imprime o arquivo de log da sessão para visualizar a mensagem. `simple_job`

Para enviar a `simple_job` amostra com um parâmetro

1. Selecione sua primeira CloudShell guia e, em seguida, navegue até o diretório de amostras do pacote de tarefas.

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

2. Imprima o conteúdo do `simple_job` modelo.

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

A `parameterDefinitions` seção com o Message parâmetro deve ter a seguinte aparência:

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

3. Envie a `simple_job` amostra com um valor de parâmetro e aguarde a conclusão da execução do trabalho.

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

4. Para ver a mensagem personalizada, veja o arquivo de registro da sessão mais recente.

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

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

## Crie um pacote de tarefas `simple_file_job` com E/S de arquivo

Um trabalho de renderização precisa ler a definição da cena, renderizar uma imagem a partir dela e depois salvar essa imagem em um arquivo de saída. Você pode simular essa ação fazendo com que o trabalho calcule o hash da entrada em vez de renderizar uma imagem.

Para criar um pacote de tarefas `simple_file_job` com E/S de arquivo

1. Selecione sua primeira CloudShell guia e, em seguida, navegue até o diretório de amostras do pacote de tarefas.

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

2. Faça uma cópia do `simple_job` com o novo nome `simple_file_job`.

```
cp -r simple_job simple_file_job
```

3. Edite o modelo de trabalho da seguinte forma:

### Note

Recomendamos que você use nano nessas etapas. Se você preferir usar Vim, defina o modo de colagem usando `:set paste`.

- a. Abra o modelo em um editor de texto.

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

- b. Adicione o seguinte `type` `objectType`, `dataFlow` `parameterDefinitions` e.

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

**dataFlow: OUT**

- c. Adicione o seguinte comando de bash script ao final do arquivo que lê o arquivo de entrada e grava no arquivo de saída.

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

A atualização `template.yaml` deve corresponder exatamente ao seguinte:

```
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**

Se você quiser ajustar o espaçamento no `template.yaml`, certifique-se de usar espaços em vez de recuos.

- d. Salve o arquivo e saia do editor de texto.
4. Forneça valores de parâmetros para os arquivos de entrada e saída para enviar o `simple_file_job`.

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

5. Imprima informações sobre o trabalho.

```
deadline job get
```

- Você verá resultados como os seguintes:

```
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
```

- Embora você tenha fornecido somente caminhos relativos, os parâmetros têm o caminho completo definido. O AWS CLI une o diretório de trabalho atual a todos os caminhos fornecidos como parâmetros quando os caminhos têm o tipo `PATH`.
- O agente de trabalho em execução na outra janela do terminal pega e executa o trabalho. Essa ação cria o `hash.txt` arquivo, que você pode visualizar com o comando a seguir.

```
cat hash.txt
```

Esse comando imprimirá uma saída semelhante à seguinte.

```
eea2df5d34b54be5ac34c56a24a8c237b8487231a607eaf530a04d76b89c9cd3 /local/home/  
cloudshell-user/BundleFiles/JobBundle-Examples/simple_job/template.yaml
```

## Etapa 4: Executar trabalhos com anexos de trabalhos no Deadline Cloud

Muitas fazendas usam sistemas de arquivos compartilhados para compartilhar arquivos entre os hosts que enviam trabalhos e aqueles que executam trabalhos. Por exemplo, no `simple_file_job` exemplo anterior, o sistema de arquivos local é compartilhado entre as janelas do AWS CloudShell terminal, que são executadas na guia um, na qual você envia o trabalho, e na guia dois, na qual você executa o agente de trabalho.

Um sistema de arquivos compartilhado é vantajoso quando a estação de trabalho remetente e os hosts do trabalhador estão na mesma rede local. Se você armazena seus dados no local próximo às estações de trabalho que os acessam, usar um farm baseado em nuvem significa que você precisa compartilhar seus sistemas de arquivos por meio de uma VPN de alta latência ou sincronizar seus sistemas de arquivos na nuvem. Nenhuma dessas opções é fácil de configurar ou operar.

AWS O Deadline Cloud oferece uma solução simples com anexos de trabalho, que são semelhantes aos anexos de e-mail. Com os anexos do trabalho, você anexa dados ao seu trabalho. Em seguida, o Deadline Cloud trata dos detalhes da transferência e armazenamento dos dados do seu trabalho nos buckets do Amazon Simple Storage Service (Amazon S3).

Os fluxos de trabalho de criação de conteúdo geralmente são iterativos, o que significa que um usuário envia trabalhos com um pequeno subconjunto de arquivos modificados. Como os buckets do Amazon S3 armazenam anexos de trabalho em um armazenamento endereçável por conteúdo, o nome de cada objeto é baseado no hash dos dados do objeto e o conteúdo de uma árvore de diretórios é armazenado em um formato de arquivo manifesto anexado a um trabalho.

Para executar trabalhos com anexos de trabalhos, conclua as etapas a seguir.

### Tópicos

- [Adicione uma configuração de anexos de tarefas à sua fila](#)
- [Envie `simple\_file\_job` com anexos de emprego](#)
- [Entendendo como os anexos de trabalho são armazenados no Amazon S3](#)

## Adicione uma configuração de anexos de tarefas à sua fila

Para habilitar anexos de trabalhos em sua fila, adicione uma configuração de anexos de trabalhos ao recurso de fila em sua conta.

Para adicionar uma configuração de anexos de tarefas à sua fila

1. Instale e configure o AWS Command Line Interface (AWS CLI), caso ainda não tenha feito isso. Para obter informações, consulte [Instalar ou atualizar para a versão mais recente do AWS CLI](#).
2. Escolha sua primeira CloudShell guia e, em seguida, insira um dos seguintes comandos para usar um bucket do Amazon S3 para anexos de trabalhos.
  - Se você não tiver um bucket Amazon S3 privado existente, você pode criar e usar um novo bucket S3.

```
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}
```

- Se você já tem um bucket privado do Amazon S3, você pode usá-lo *MY\_BUCKET\_NAME* substituindo-o pelo nome do seu bucket.

```
DEV_FARM_BUCKET=MY_BUCKET_NAME
```

3. Depois de criar ou escolher seu bucket do Amazon S3, adicione o nome do bucket `~/ .bashrc` para disponibilizá-lo para outras sessões do terminal.

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

4. Crie uma função AWS Identity and Access Management (IAM) para a fila.

```
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"
        }
      ]
    }'

```

- Atualize sua fila para incluir as configurações de anexos do trabalho e a função do 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 se você atualizou sua fila.

```
deadline queue get
```

Uma saída como a seguinte é mostrada:

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

## Envie `simple_file_job` com anexos de emprego

Quando você usa anexos de tarefas, os pacotes de tarefas devem fornecer ao Deadline Cloud informações suficientes para determinar o fluxo de dados da tarefa, como o uso de parâmetros. `PATH` No caso do `simple_file_job`, você editou o `template.yaml` arquivo para informar ao Deadline Cloud que o fluxo de dados está no arquivo de entrada e no arquivo de saída.

Depois de adicionar a configuração dos anexos do trabalho à sua fila, você pode enviar a amostra `simple_file_job` com os anexos do trabalho. Depois de fazer isso, você pode visualizar o registro e a saída do trabalho para confirmar se o `simple_file_job` com anexos do trabalho está funcionando.

Para enviar o pacote de tarefas `simple_file_job` com anexos de tarefas

1. Escolha sua primeira CloudShell guia e, em seguida, abra o `JobBundle-Samples` diretório.

2. 

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

3. Envie `simple_file_job` para a fila. Quando solicitado a confirmar o upload, insira `y`.

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

4. Para visualizar a saída do log da sessão de transferência de dados dos anexos do trabalho, escolha sua segunda CloudShell guia.

```
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. Liste as ações da sessão que foram executadas na sessão.

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

Uma saída como a seguinte é mostrada:

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

A primeira ação da sessão baixou os anexos do trabalho de entrada, enquanto a segunda ação executa a tarefa como antes e depois carregou os anexos do trabalho de saída.

6. Liste o diretório de saída.

```
ls *.txt
```

Saída como `hash.txt` a mostrada, mas `hash-jobattachments.txt` não existe.

7. Baixe a saída do trabalho mais recente.

```
deadline job download-output
```

8. Visualize a saída do arquivo baixado.

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

Uma saída como a seguinte é mostrada:

```
eea2df5d34b54be5ac34c56a24a8c237b8487231a607eaf530a04d76b89c9cd3 /tmp/openjd/
session-123/assetroot-abc/simple_job/template.yaml
```

## Entendendo como os anexos de trabalho são armazenados no Amazon S3

Você pode usar o AWS Command Line Interface (AWS CLI) para carregar ou baixar dados para anexos de tarefas, que são armazenados em buckets do Amazon S3. Entender como o Deadline

Cloud armazena anexos de trabalhos no Amazon S3 ajudará você a desenvolver cargas de trabalho e integrações de pipeline.

Para inspecionar como os anexos de trabalho do Deadline Cloud são armazenados no Amazon S3

1. Escolha sua primeira CloudShell guia e, em seguida, abra o diretório de amostras do pacote de tarefas.

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

2. Inspecione as propriedades do trabalho.

```
deadline job get
```

Uma saída como a seguinte é mostrada:

```
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
```

O campo de anexos contém uma lista de estruturas de manifesto que descrevem os caminhos de dados de entrada e saída que a tarefa usa quando é executada. Veja `rootPath` o caminho do diretório local na máquina que enviou o trabalho. Para ver o sufixo do objeto Amazon S3

que contém um arquivo de manifesto, consulte. `inputManifestFile` O arquivo de manifesto contém metadados para um instantâneo da árvore de diretórios dos dados de entrada do trabalho.

3. Imprima bem o objeto de manifesto do Amazon S3 para ver a estrutura do diretório de entrada para o trabalho.

```
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 .
```

Uma saída como a seguinte é mostrada:

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

4. Crie o prefixo do Amazon S3 que contém manifestos para os anexos do trabalho de saída e liste o objeto abaixo dele.

```
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
```

Os anexos do trabalho de saída não são referenciados diretamente do recurso de trabalho, mas são colocados em um bucket do Amazon S3 com base em IDs de recursos agrícolas.

- Obtenha a chave de objeto de manifesto mais recente para o ID de ação de sessão específico e, em seguida, imprima bem os objetos do manifesto.

```
SESSION_ACTION_ID=$(echo $SESSION_ACTION | jq -r .sessionId)
MANIFEST_KEY=$(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 .
```

Você verá propriedades do arquivo `hash-jobattachments.txt` na saída, como as seguintes:

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

Seu trabalho terá apenas um único objeto manifesto por tarefa executada, mas, em geral, é possível ter mais objetos por tarefa executada.

- Visualize a saída de armazenamento do Amazon S3 endereçável ao conteúdo sob o prefixo.

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 -
```

Uma saída como a seguinte é mostrada:

```
eea2df5d34b54be5ac34c56a24a8c237b8487231a607eaf530a04d76b89c9cd3 /tmp/openjd/
session-123/assetroot-abc/simple_job/template.yaml
```

## Etapa 5: adicione uma frota gerenciada por serviços à sua fazenda de desenvolvedores no Deadline Cloud

AWS CloudShell não fornece capacidade computacional suficiente para testar cargas de trabalho maiores. Também não está configurado para funcionar com trabalhos que distribuem tarefas em vários hosts de trabalho.

Em vez de usar CloudShell, você pode adicionar uma frota gerenciada de serviços (SMF) do Auto Scaling à sua fazenda de desenvolvedores. Um SMF fornece capacidade computacional suficiente para cargas de trabalho maiores e pode lidar com trabalhos que precisam distribuir tarefas de trabalho em vários hosts de trabalho. O agendador usará os trabalhadores SMF e CMF para executar trabalhos, a menos que você desligue o trabalhador CMF.

Para adicionar uma frota gerenciada por serviços à sua fazenda de desenvolvedores

1. Instale e configure o AWS Command Line Interface (AWS CLI), caso ainda não tenha feito isso. Para obter informações, consulte [Instalar ou atualizar para a versão mais recente do AWS CLI](#).
2. Escolha sua primeira AWS CloudShell guia e, em seguida, crie a frota gerenciada por serviços e adicione sua ID de frota `.bashrc` a. Essa ação o torna disponível para outras sessões do 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. Associe o SMF à sua fila.

```

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

```

- 4.

 Note

O agendador usará os trabalhadores SMF e CMF para executar trabalhos, a menos que você desligue o trabalhador CMF.

Envie `simple_file_job` para a fila. Quando solicitado a confirmar o upload, insira `y`.

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

5. Confirme se o SMF está funcionando corretamente.

```
deadline fleet get
```

- O trabalhador pode levar alguns minutos para começar.
- `queueFleetAssociationsStatus` para sua frota gerenciada pelo cliente e a frota gerenciada por serviços, serão `ACTIVE`.
- O SMF `autoScalingStatus` mudará de `GROWING` para `STEADY`.

Seu status será semelhante ao seguinte:

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

6. Visualize o registro do trabalho que você enviou. Esse log é armazenado em um log no Amazon CloudWatch Logs, não no sistema de CloudShell arquivos.

```
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
```

## Etapa 6: limpe os recursos da sua fazenda no Deadline Cloud

Para desenvolver e testar novas cargas de trabalho e integrações de pipeline, você pode continuar usando o farm de desenvolvedores do Deadline Cloud que você criou para este tutorial. Se você não precisar mais da sua fazenda de desenvolvedores, poderá excluir seus recursos, incluindo fazenda, frota, fila, funções AWS Identity and Access Management (IAM) e registros no Amazon CloudWatch Logs. Depois de excluir esses recursos, você precisará começar o tutorial novamente para usar os recursos. Para ter mais informações, consulte [Configurando uma estação de trabalho de desenvolvedor para o Deadline Cloud](#).

Para limpar os recursos da fazenda de desenvolvedores

1. Instale e configure o AWS Command Line Interface (AWS CLI), caso ainda não tenha feito isso. Para obter informações, consulte [Instalar ou atualizar para a versão mais recente do AWS CLI](#).
2. Escolha sua primeira CloudShell guia e, em seguida, interrompa todas as associações de filas e frotas da sua fila.

```
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. Liste as associações de frotas de filas.

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

Talvez seja necessário executar novamente o comando até que a saída seja reportada e, em seguida "status": "STOPPED", você pode prosseguir para a próxima etapa. O processo pode demorar vários minutos para ser concluído.

```
{
  "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. Exclua todas as associações de filas e frota da sua fila.

```
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. Exclua todas as frota associadas à sua fila.

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

```
done
```

6. Exclua a fila.

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

7. Exclua a fazenda.

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

8. Exclua outros AWS recursos da sua fazenda.

- a. Exclua a função de frota 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. Exclua a função IAM da fila.

```
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. Exclua os grupos de CloudWatch log do Amazon Logs. Cada fila e frota tem seu próprio 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"
```

# Configurar remetentes do Deadline Cloud

Esse processo é para administradores e artistas que desejam instalar, configurar e lançar o remetente do AWS Deadline Cloud. Um remetente do Deadline Cloud é um plug-in de criação de conteúdo digital (DCC). Os artistas o usam para enviar trabalhos a partir de uma interface de DCC de terceiros com a qual estão familiarizados.

## Note

Esse processo deve ser concluído em todas as estações de trabalho que os artistas usarão para enviar renderizações.

## Tópicos

- [Etapa 1: instalar o remetente do Deadline Cloud](#)
- [Etapa 2: instalar e configurar o monitor Deadline Cloud](#)
- [Etapa 3: Inicie o remetente do Deadline Cloud](#)

## Etapa 1: instalar o remetente do Deadline Cloud

As seções a seguir orientam você pelas etapas para instalar o remetente do Deadline Cloud.

### Baixe o instalador do remetente

Antes de instalar o remetente do Deadline Cloud, você deve baixar o instalador do remetente. Atualmente, o instalador de envio do Deadline Cloud suporta apenas e. Windows Linux

1. Faça login AWS Management Console e abra o [console](#) do Deadline Cloud.
2. No painel de navegação lateral, escolha Downloads.
3. Localize a seção de instalação para remetentes do Deadline Cloud.
4. Selecione o instalador para o sistema operacional do seu computador e escolha Baixar.

### (Opcional) Verifique a autenticidade do software baixado

Para verificar se o software que você baixou é autêntico, use o procedimento a seguir para Windows ouLinux.

**Note**

Você pode usar essas instruções para primeiro verificar o instalador e, em seguida, verificar o monitor do Deadline Cloud depois de baixá-lo na próxima seção (Etapa 2).

## Windows

Para verificar a autenticidade dos arquivos baixados, conclua as etapas a seguir.

1. No comando a seguir, *file* substitua pelo arquivo que você deseja verificar. Por exemplo, **`C:\PATH\TO\MY\DeadlineCloudSubmitter-windows-x64-installer.exe`** . Além disso, *signtool-sdk-version* substitua pela versão do SignTool SDK instalada. Por exemplo, **`10.0.22000.0`**.

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

2. Por exemplo, você pode verificar o arquivo de instalação do remetente do Deadline Cloud executando o seguinte 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 verificar a autenticidade dos arquivos baixados, use a ferramenta de linha de gpg comando.

1. Importe a OpenPGP chave para o instalador de envio do Deadline Cloud executando o seguinte comando:

```
gpg --import --armor <<EOF  
-----BEGIN PGP PUBLIC KEY BLOCK-----  
  
mQINBGX6GQsBEADduUtJgqSXI+q7606fsFwEYKmbnlyL0xKv1q32EZuyv0otZo5L  
le4m5Gg52AzrvPvDiUTLooAlvYeozaYyirIGsK08Ydz0Ftdjroiuh/mw9JSJDJRI  
rnRn5yKet1JFzckjopA3pjsTBP6lW/mb1bDBDEwwwtH0x91V7A03FJ9T7Uzu/qSh  
q0/UYdkafro3cPASvkqgDt2tCvURfBcUCAjZVFcLZcVD5iwXacxvKsxxS/e7kuVV  
I1+VGT8Hj8XzWYhjCZx0LZk/fvpYPMYEEujN0fYUp6RtMIXve0C9awwMCy5nBG2J  
eE2015DsCpTaBd4Fdr3LWcSs8JFA/YfP9auL3Ncz0ozPoVJt+fw8CB1VIX00J715
```

```

hvHDjcC+5v0wxqA1MG6+f/SX7CT8FXK+L3i0J5gBYUNXqHSxUdv8kt76/KVmQa1B
Ak1+MPKpMq+1hw++S3G/1XqwWaDNQbRRw7dSZHymQVXvPp1nscq3hV7K10M+6s6g
1g4mvFY41f6DhptwZLWYQXU8rBQpojvQfiSmDFrFPWF5BexesuVnkGIo1Qok1Kx
AVUSdJPVEJCTeyy7td4FPhBaSqT5vW3+ANbr9b/uoRYWJvn17dN0cc9HuRh/Ai+I
nkfECo2WUDLZ0fEKGjGyFX+todWvJXjvc5kmE9Ty5vJp+M9Vvb8jd6t+mwARAQAB
tCxBV1MgRGVhZGxpbnUgQ2xvdWQgPGF3cy1kZWFKbGluZUBhbWF6b24uY29tPokC
VwQTAQgAQRyhBLhAwIwpqQeWoHH6pfbNP0a3bzzvBQJ1+hkLAXsvBAUJA8JnAAUL
CQgHAgIiAgYVCgkICwIDFgIBAh4HAheAAAoJEPbNP0a3bzzvKswQAjXzKSAY8sY8
F6Eas2oYwIDDdDurs8FiEnFghjUE06MTt9AykF/jw+CQg2UzFtEy0bHBymhgmhXE
3buVeom96tgM3ZDfZu+sxi5pGX6oAQnZ6riztN+VpkpQmLgwtMGpSML13KLwnv2k
WK8mrR/fPMkfdawB7A6RIUYiW33GAL4KfMI8/vIwIjw99NxHpZQVoU6dFpuDtE
10uxGcCqGJ7mAmo6H/YawSNp2Ns80gyqIKYo7o3LJ+WRroIRlQyctq8gnR9JvYXX
42ASqLq5+0XKo4qh81b1XKYqtc176BbbSNFjWnzIQgKDgNiHFZCdc0VgqDhw015r
NICbqqwNLj/Fr2kecYx180Ktp10j00w5I0yh3bf3MVGWnYRdjvA1v+/CO+55N4g
z0kf50Lcdu5RtqV10XBCifn28pecqPaSdYcssYSR15DLiFktGbNzTGcZZwITTKQc
af8PPdTGtnnb6P+cdbW3bt9MvtN5/dgSHLThnS8MPEuNCtkTnpXshuVuBGgwBMdb
qUC+HjqvhZzbwns8dr5WI+6HWNBFgGANN6ageY158vVp0UkuNP8wcWjRARciHXZx
ku6W2jPTHDWGNrBQ02Fx7fd2QYJheIPPAShHcfJ0+XgWcof45D0vAxAJ8gGg9Eq+
gFwhsx4NSHn2gh1gDZ410u/4exJ11wPM
=uVaX
-----END PGP PUBLIC KEY BLOCK-----
EOF

```

2. Determine se você deve confiar na OpenPGP chave. Alguns fatores a serem considerados ao decidir se deve confiar na chave acima incluem o seguinte:
  - A conexão com a internet que você usou para obter a chave GPG deste site é segura.
  - O dispositivo em que você está acessando este site é seguro.
  - AWS tomou medidas para garantir a hospedagem da chave OpenPGP pública neste site.
3. Se você decidir confiar na OpenPGP chave, edite a chave para confiar de gpg forma semelhante ao exemplo a seguir:

```
$ 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. Verifique o instalador

Para verificar o instalador, conclua as seguintes etapas:

- a. Volte para a página de downloads do [console do](#) Deadline Cloud e baixe o arquivo de assinatura para o instalador remetente do Deadline Cloud.
- b. Verifique a assinatura do instalador remetente do Deadline Cloud executando:

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

## 5. Verifique o monitor Deadline Cloud

### Note

Você pode verificar o download do monitor Deadline Cloud usando arquivos de assinatura ou métodos específicos da plataforma. Para métodos específicos da plataforma, consulte a Linux (DEB) guia ou a Linux (AppImage) guia com base no tipo de arquivo baixado.

Para verificar o aplicativo de desktop Deadline Cloud Monitor com arquivos de assinatura, conclua as seguintes etapas:

- a. Volte para a página de downloads [do console](#) Deadline Cloud, baixe o arquivo.sig correspondente e execute

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 se a saída é semelhante à seguinte:

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

```
gpg: using RSA key B840C08C29A90796A071FAA5F6CD3CE6B7
```

Se a saída contiver a frase `Good signature from "AWS Deadline Cloud"`, significa que a assinatura foi verificada com sucesso e você pode executar o script de instalação do monitor Deadline Cloud.

## Linux (DEB)

Para verificar os pacotes que usam um Linux binário.deb, primeiro conclua as etapas 1 a 3 na guia. Linux

O dpkg é a principal ferramenta de gerenciamento de pacotes na maioria das distribuições debian baseadasLinux. Você pode verificar o arquivo.deb com a ferramenta.

1. Na página de downloads do [console do](#) Deadline Cloud, baixe o arquivo.deb do monitor do Deadline Cloud.
2. **<APP\_VERSION>**Substitua pela versão do arquivo.deb que você deseja verificar.

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

3. A saída será semelhante a:

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

4. Para verificar o arquivo.deb, confirme se ele GOODSIG está presente na saída.

## Linux (AppImage)

Para verificar pacotes que usam umLinux. AppImage binário, primeiro conclua as etapas 1 a 3 na Linux guia.

1. Na página de downloads do [console](#) Deadline Cloud, baixe o monitor do Deadline Cloud. AppImage arquivo.
2. Para <APP\_VERSION>substituir pela versão do. AppImage arquivo que você deseja verificar, conclua as seguintes etapas:
  - a. Escreva a assinatura do. AppImage arquivo em um arquivo.sig.

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

- b. Use o arquivo.sig gerado para verificar usando o comando a seguir.

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

- c. (Opcional) Se um erro de permissão negada for exibido, use o comando a seguir para adicionar a permissão de execução.

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

- d. Confirme se a saída é semelhante à seguinte:

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

```
gpg: using RSA key B840C08C29A90796A071FAA5F6CD3CE6B7
```

Se a saída contiver a frase `Good signature from "AWS Deadline Cloud"`, significa que a assinatura foi verificada com sucesso e você pode executar o script de instalação do monitor Deadline Cloud.

## Instale o remetente do Deadline Cloud

Você pode instalar um remetente do Deadline Cloud com Windows ou Linux. Com o instalador, você pode instalar os seguintes remetentes:

- Maia 2024
- Nuke 14.0 - 15.0
- Houdini 19,5
- Captura de tecla 12
- Liquidificador 3.6
- Unreal Engine 5

### Windows

1. Em um navegador de arquivos, navegue até a pasta em que o instalador foi baixado e selecione `DeadlineCloudSubmitter-windows-x64-installer.exe`.
  - a. Se um pop-up do Windows protegeu seu PC for exibido, escolha Mais informações.
  - b. Escolha Executar de qualquer maneira.
2. Depois que o Assistente de configuração do AWS Deadline Cloud Submitter for aberto, escolha Avançar.
3. Escolha o escopo da instalação concluindo uma das seguintes etapas:

- Para instalar somente para o usuário atual, escolha Usuário.
- Para instalar para todos os usuários, escolha Sistema.

Se você escolher Sistema, deverá sair do instalador e executá-lo novamente como administrador, concluindo as seguintes etapas:

- a. Clique com o botão direito do mouse em **DeadlineCloudSubmitter-windows-x64-installer.exe** e escolha Executar como administrador.
  - b. Insira suas credenciais de administrador e escolha Sim.
  - c. Escolha Sistema para o escopo da instalação.
4. Depois de selecionar o escopo da instalação, escolha Avançar.
  5. Escolha Avançar novamente para aceitar o diretório de instalação.
  6. Selecione Enviador integrado para Nuke, ou qualquer remetente que você deseja instalar.
  7. Escolha Próximo.
  8. Revise a instalação e escolha Avançar.
  9. Escolha Avançar novamente e, em seguida, escolha Concluir.

## Linux

### Note

O Nuke instalador integrado do Deadline Cloud Linux e o monitor do Deadline Cloud só podem ser instalados em Linux distribuições com pelo menos o GLIBC 2.31.

1. Abra uma janela do terminal.
2. Para fazer uma instalação do instalador no sistema, digite o comando **sudo -i** e pressione Enter para se tornar root.
3. Navegue até o local em que você baixou o instalador.

Por exemplo, **cd /home/*USER*/Downloads**.

4. Para tornar o instalador executável, digite **chmod +x DeadlineCloudSubmitter-linux-x64-installer.run**.
5. Para executar o instalador de envio do Deadline Cloud, insira. **./DeadlineCloudSubmitter-linux-x64-installer.run**

6. Quando o instalador for aberto, siga as instruções na tela para concluir o Assistente de Configuração.

Você pode instalar outros remetentes não listados aqui. Usamos as bibliotecas do Deadline Cloud para criar remetentes. Você pode encontrar o código-fonte dessas bibliotecas e remetentes na organização [GitHubaws-deadline](#).

## Etapa 2: instalar e configurar o monitor Deadline Cloud

Você pode instalar o aplicativo de desktop de monitor Deadline Cloud com Windows ou Linux.

### Windows

1. Se ainda não o fez, faça login AWS Management Console e abra o [console](#) do Deadline Cloud.
2. No painel de navegação esquerdo, escolha Downloads.
3. Na seção Monitor do Deadline Cloud, selecione o arquivo do sistema operacional do seu computador.
4. Para baixar o monitor Deadline Cloud, escolha Baixar.

### Linux

Para instalar o monitor Deadline Cloud AppImage em distribuições RPM

1. Baixe o monitor Deadline Cloud mais recente AppImage.
2. Para tornar o AppImage executável, insira `chmod a+x deadline-cloud-monitor_<APP_VERSION>_amd64.AppImage`.
3. Para configurar o caminho correto do certificado SSL, digite. `sudo ln -sf /etc/ssl/certs/ca-bundle.crt /etc/ssl/certs/ca-certificates.crt`

Para instalar o monitor Deadline Cloud AppImage nas distribuições do Debian

1. Baixe o monitor Deadline Cloud mais recente AppImage.

2.

**Note**

Esta etapa é para o Ubuntu 22 e versões posteriores. Para outras versões do Ubuntu, pule esta etapa.

Para instalar libfuse2, digite **sudo apt update**

**sudo apt install libfuse2.**

3. Para tornar o AppImage executável, insira **chmod a+x deadline-cloud-monitor\_<APP\_VERSION>\_amd64.AppImage.**

Para instalar o pacote Debian Deadline Cloud monitor Debian nas distribuições Debian

1. Baixe o pacote Debian mais recente do Deadline Cloud Monitor.

2.

**Note**

Esta etapa é para o Ubuntu 22 e versões posteriores. Para outras versões do Ubuntu, pule esta etapa.

Para instalar libssl1.1, digite **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 o pacote Debian Deadline Cloud monitor, digite **sudo apt update**

**sudo apt install ./deadline-cloud-monitor\_<APP\_VERSION>\_amd64.deb.**

4. Se a instalação falhar em pacotes com dependências não atendidas, corrija os pacotes corrompidos e execute os comandos a seguir.

**sudo apt --fix-missing update**

**sudo apt update**

**sudo apt install -f**

Depois de concluir o download, você pode verificar a autenticidade do software baixado. Consulte [Verificar a autenticidade do software baixado na Etapa 1](#).

Depois de baixar o monitor do Deadline Cloud e verificar a autenticidade, use o procedimento a seguir para configurar o monitor do Deadline Cloud.

Para configurar o monitor Deadline Cloud

1. Monitor Open Deadline Cloud.
2. Quando solicitado a criar um novo perfil, conclua as etapas a seguir.
  - a. Insira o URL do seu monitor na entrada do URL, que se parece com **https://MY-MONITOR.deadlinecloud.amazonaws.com/**
  - b. Insira um nome de perfil.
  - c. Escolha Criar perfil.

Seu perfil foi criado e suas credenciais agora são compartilhadas com qualquer software que use o nome do perfil que você criou.

3. Depois de criar o perfil de monitor do Deadline Cloud, você não pode alterar o nome do perfil ou a URL do estúdio. Se você precisar fazer alterações, faça o seguinte:
  - a. Exclua o perfil. No painel de navegação esquerdo, escolha Deadline Cloud Monitor, Configurações, Excluir.
  - b. Crie um novo perfil com as alterações que você deseja.
4. No painel de navegação esquerdo, use a opção de monitor >Deadline Cloud para fazer o seguinte:
  - Altere o perfil do monitor do Deadline Cloud para fazer login em um monitor diferente.
  - Ative o login automático para que você não precise inserir a URL do seu monitor nas aberturas subsequentes do monitor Deadline Cloud.
5. Feche a janela do monitor do Deadline Cloud. Ele continua sendo executado em segundo plano e sincroniza suas credenciais a cada 15 minutos.
6. Para cada aplicativo de criação de conteúdo digital (DCC) que você planeja usar em seus projetos de renderização, conclua as seguintes etapas:
  - a. Do remetente do Deadline Cloud, abra a configuração da estação de trabalho Deadline Cloud.



- b. Na configuração da estação de trabalho, selecione o perfil que você criou no monitor do Deadline Cloud. Suas credenciais do Deadline Cloud agora são compartilhadas com este DCC e suas ferramentas devem funcionar conforme o esperado.

## Etapa 3: Inicie o remetente do Deadline Cloud

As seções a seguir orientam você pelas etapas para iniciar o plug-in de envio do Deadline Cloud em Blender, NukeMaya, e. Houdini

Para lançar o remetente do Deadline Cloud em Blender

### Note

Support for Blender é fornecido usando o Conda ambiente para frotas gerenciadas por serviços. Para ter mais informações, consulte [Ambiente de Conda fila padrão](#).

1. Abra o Blender.
2. Abra uma Blender cena com dependências que existem no diretório raiz do ativo.
3. No menu Renderizar, selecione a caixa de diálogo Deadline Cloud.
  - a. Se você ainda não estiver autenticado no remetente do Deadline Cloud, o status das credenciais exibirá NEEDS\_LOGIN.
  - b. Escolha Fazer login.
  - c. Uma janela do navegador de login é exibida. Faça login com suas credenciais de usuário.
  - d. Selecione Permitir. Agora você está logado e o status das credenciais será exibido como AUTENTICADO.
4. Selecione Enviar.


Para lançar o remetente do Deadline Cloud em Foundry Nuke

### Note

Support for Nuke é fornecido usando o Conda ambiente para frotas gerenciadas por serviços. Para ter mais informações, consulte [Ambiente de Conda fila padrão](#).

1. Abra o Nuke.
2. Abra um Nuke script com dependências que existem no diretório raiz do ativo.
3. Escolha Thinkbox e, em seguida, escolha Enviar para o Deadline Cloud para iniciar o remetente.
  - a. Se você ainda não estiver autenticado no remetente do Deadline Cloud, o status das credenciais será exibido como NEEDS\_LOGIN.
  - b. Escolha Fazer login.
  - c. Na janela do navegador de login, faça login com suas credenciais de usuário.
  - d. Selecione Permitir. Agora você está logado e o status das credenciais será exibido como AUTENTICADO.
4. Selecione Enviar.

Para lançar o remetente do Deadline Cloud em Maya


 Note

Support Maya e Arnold for Maya(MtoA) é fornecido usando o Conda ambiente para frotas gerenciadas por serviços. Para ter mais informações, consulte [Ambiente de Conda fila padrão](#).

1. Abra o Maya.
2. Defina seu projeto e abra um arquivo que existe no diretório raiz do ativo.
3. Escolha Windows → Configurações/Preferências → Gerenciador de plug-ins.
4. Pesquise o DeadlineCloudremetente.
5. Para carregar o plug-in de envio do Deadline Cloud, selecione Loaded.
  - a. Se você ainda não estiver autenticado no remetente do Deadline Cloud, o status das credenciais será exibido como NEEDS\_LOGIN.
  - b. Escolha Fazer login.
  - c. Uma janela do navegador de login é exibida. Faça login com suas credenciais de usuário.
  - d. Selecione Permitir. Agora você está logado e o status das credenciais é exibido como AUTENTICADO.
6. (Opcional) Para carregar o plug-in de envio do Deadline Cloud toda vez que você abrir Maya, escolha Carregar automaticamente.

7. Selecione a prateleira Deadline Cloud e, em seguida, selecione o botão verde para iniciar o remetente.

Para lançar o remetente do Deadline Cloud em Houdini

 Note

Support for Houdini é fornecido usando o Conda ambiente para frotas gerenciadas por serviços. Para ter mais informações, consulte [Ambiente de Conda fila padrão](#).

1. Abra o Houdini.
2. No Editor de rede, selecione a rede /out.
3. Pressione tab e entre **deadline**.
4. Selecione a opção Deadline Cloud e conecte-a à sua rede existente.
5. Clique duas vezes no nó Deadline Cloud.

Para lançar o remetente do Deadline Cloud em KeyShot

Isso pressupõe que você já tenha baixado o Deadline Cloud e PySide 2.

1. Copie ou vincule o arquivo `Deadline-cloud-for-keyshot/keyshot_script/submit to AWS Deadline Cloud.py` à pasta de scripts. KeyShot

Por exemplo, ativadoWindows, a localização da pasta de scripts seria **C:/Users/USER/Documents/KeyShot 12/Scripts**.

2. Defina as seguintes variáveis de ambiente.
  - a. Defina a variável de ambiente **DEADLINE\_PYTHON** como o caminho para a instalação do Python, onde `deadline-cloud` e `2` estão localizados. PySide

Por exemplo, ativadoWindows, se estiver usando o Python 3.10, o comando pode ser.  
**set DEADLINE\_PYTHON=C:/Users/USER/AppData/Local/Programs/Python/Python310/python**

- b. Defina a variável de ambiente **DEADLINE\_KEYSHOT** como o caminho para a pasta `keyshot_submitter`.

Por exemplo, ativadoWindows, se a fonte estiver em sua área de trabalho, o comando pode estar **set DEADLINE\_KEYSHOT=C:/Users/*USER*/Desktop/deadline-cloud-for-keyshot/src/deadline/keyshot\_submitter**.

3. Com as variáveis de ambiente definidas, inicie KeyShot.
4. Para iniciar o remetente a partir de KeyShot, escolha Scripting console Windows, Enviar para o AWS Deadline Cloud e Executar.

Para lançar o remetente do Deadline Cloud em Unreal Engine

Isso pressupõe que você já tenha baixado o Deadline Cloud.

1. Crie ou abra a pasta que você usa para seus Unreal Engine projetos.
2. Abra a linha de comando e execute os seguintes 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 baixar o plug-inUnreal Engine, abra a pasta do Unreal Engine projeto e inicie o `deadline-cloud-forunreal/test_projects/pull_ue_plugin.bat`.

Isso coloca os arquivos do plug-in em `C://LocalProjectsUnrealDeadlineCloudTest/Plugins/UnrealDeadline CloudService`.

4. Para baixar o remetente, abra a `UnrealDeadlineCloudService` pasta e execute. **`deadline-cloud-forunreal/ test_projects/Plugins/UnrealDeadlineCloudService/ install_unreal_submitter.bat`**
5. Para iniciar o remetente a partir deUnreal Engine, conclua as seguintes etapas:
  - a. Escolha Editar > Configurações do projeto.
  - b. Na barra de pesquisa, insira **movie render pipeline**.
  - c. Ajuste as seguintes configurações do Movie Render Pipeline:
    - i. Em Default Remote Executor, digite**MoviePipelineDeadlineCloudRemote Executor**.
    - ii. Em Default Executor Job, insira **MoviePipelineDeadlineCloudExecutorJob**

- iii. Em Default Job Settings Classes, escolha o sinal de adição e, em seguida, insira **DeadlineCloudRenderStepSetting**.

Com essas configurações, você pode escolher o plug-in Deadline Cloud em Unreal Engine.

## Use a fazenda

Se você seguiu todas as instruções de introdução, configurou tudo o que precisa para começar a enviar trabalhos da estação de trabalho local para a fazenda e depois monitorar esses trabalhos e recursos. Para obter mais informações sobre o envio de todos os tipos de trabalhos ou monitoramento, consulte os tópicos relacionados abaixo.

- [Trabalhos](#)
- [Usando o monitor](#)

# Usando o monitor Deadline Cloud

O monitor AWS Deadline Cloud fornece uma visão geral de seus trabalhos de computação visual. Você pode usá-lo para monitorar e gerenciar trabalhos, visualizar a atividade dos trabalhadores nas frotas, monitorar orçamentos e uso e baixar os resultados de um trabalho.

Cada fila tem um monitor de tarefas que mostra o status das tarefas, etapas e tarefas. O monitor fornece maneiras de gerenciar trabalhos diretamente do monitor. Você pode fazer alterações de priorização, cancelar trabalhos e reenqueuear trabalhos.

O monitor do Deadline Cloud tem uma tabela que mostra o status resumido de um trabalho, ou você pode selecionar um trabalho para ver registros de tarefas detalhados que ajudam a solucionar problemas com um trabalho.

Você pode usar o monitor do Deadline Cloud para baixar os resultados para o local em sua estação de trabalho que foi especificado quando o trabalho foi criado.

O monitor Deadline Cloud também ajuda você a monitorar o uso e gerenciar custos. Para ter mais informações, consulte [Gerenciamento de orçamentos e uso do Deadline Cloud](#).

## Tópicos

- [Compartilhe o URL do monitor do Deadline Cloud](#)
- [Abra o monitor Deadline Cloud](#)
- [Veja detalhes da fila e da frota no Deadline Cloud](#)
- [Visualize e gerencie trabalhos, etapas e tarefas no Deadline Cloud](#)
- [Veja os detalhes do trabalho no Deadline Cloud](#)
- [Veja uma etapa no Deadline Cloud](#)
- [Exibir uma tarefa no Deadline Cloud](#)
- [Exibir registros no Deadline Cloud](#)
- [Baixe a saída finalizada no Deadline Cloud](#)

## Compartilhe o URL do monitor do Deadline Cloud

Ao configurar o serviço Deadline Cloud, por padrão, você cria uma URL que abre o monitor do Deadline Cloud para sua conta. Use esse URL para abrir o monitor em seu navegador ou em seu

desktop. Compartilhe o URL com outros usuários para que eles possam acessar o monitor do Deadline Cloud.

Antes que um usuário possa abrir o monitor do Deadline Cloud, você deve conceder acesso ao usuário. Para conceder acesso, adicione o usuário à lista de usuários autorizados do monitor ou adicione-o a um grupo com acesso ao monitor. Para ter mais informações, consulte [Gerenciando usuários no Deadline Cloud](#).

Para compartilhar o URL do monitor

1. Abra o [console do Deadline Cloud](#).
2. Em Começar, escolha Ir para o painel do Deadline Cloud.
3. No painel de navegação, selecione Dashboard (Painel).
4. Na seção Visão geral da conta, escolha Detalhes da conta.
5. Copie e envie o URL com segurança para qualquer pessoa que precise acessar o monitor do Deadline Cloud.

## Abra o monitor Deadline Cloud

Você pode abrir o monitor do Deadline Cloud de qualquer uma das seguintes formas:

- Console — Faça login AWS Management Console e abra o console do Deadline Cloud.
- Web — Acesse a URL do monitor que você criou ao configurar o Deadline Cloud.
- Monitor — Use o monitor Deadline Cloud para desktop.

Ao usar o console, você deve ser capaz de entrar AWS usando uma AWS Identity and Access Management identidade e, em seguida, entrar no monitor com AWS IAM Identity Center credenciais. Se você tiver apenas as credenciais do IAM Identity Center, deverá fazer login usando o URL do monitor ou o aplicativo de desktop.

Para abrir o monitor do Deadline Cloud (web)

1. Usando um navegador, abra a URL do monitor que você criou ao configurar o Deadline Cloud.
2. Faça login com suas credenciais de usuário.

## Para abrir o monitor do Deadline Cloud (console)

1. Abra o [console do Deadline Cloud](#).
2. No painel de navegação, selecione Fazendas.
3. Selecione uma fazenda e escolha Gerenciar trabalhos para abrir a página de monitoramento do Deadline Cloud.
4. Faça login com suas credenciais de usuário.

## Para abrir o monitor do Deadline Cloud (desktop)

1. Abra o [console do Deadline Cloud](#).

- ou -

Abra o monitor Deadline Cloud - web a partir da URL do monitor.

2.
  - No console do Deadline Cloud, faça o seguinte:
    1. No monitor, escolha Ir para o painel do Deadline Cloud e, em seguida, escolha Downloads no menu à esquerda.
    2. No monitor Deadline Cloud, escolha a versão do monitor para seu desktop.
    3. Escolha Baixar.
  - No monitor Deadline Cloud - web, faça o seguinte:
    - No menu à esquerda, escolha Configuração da estação de trabalho. Se o item de configuração da estação de trabalho não estiver visível, use a seta para abrir o menu à esquerda.
    - Escolha Baixar.
    - Em Selecionar um sistema operacional, escolha seu sistema operacional.
3. Baixe o monitor Deadline Cloud - desktop.
4. Depois de baixar e instalar o monitor, abra-o no seu computador.
  - Se esta é a primeira vez que você abre o monitor do Deadline Cloud, você deve fornecer a URL do monitor e criar um nome de perfil. Em seguida, você faz login no monitor com suas credenciais do Deadline Cloud.
  - Depois de criar um perfil, você abre o monitor selecionando um perfil. Talvez seja necessário inserir suas credenciais do Deadline Cloud.



## Veja detalhes da fila e da frota no Deadline Cloud

Você pode usar o monitor Deadline Cloud para visualizar a configuração das filas e frotas em sua fazenda. Você também pode usar o monitor para ver uma lista dos trabalhos em uma fila ou dos trabalhadores em uma frota.

Você deve ter VIEWING permissão para visualizar os detalhes da fila e da frota. Se os detalhes não aparecerem, entre em contato com o administrador para obter as permissões corretas.

Para ver os detalhes da fila

1. [Abra o monitor Deadline Cloud.](#)
2. Na lista de fazendas, escolha a fazenda que contém a fila na qual você está interessado.
3. Na lista de filas, escolha uma fila para exibir seus detalhes. Para comparar a configuração de duas ou mais filas, marque mais de uma caixa de seleção.
4. Para ver uma lista de trabalhos na fila, escolha o nome da fila na lista de filas ou no painel de detalhes.

Se o monitor já estiver aberto, você poderá selecionar a fila na lista Filas no painel de navegação esquerdo.

Para visualizar os detalhes da frota

1. [Abra o monitor Deadline Cloud.](#)
2. Na lista de fazendas, escolha a fazenda que contém a frota na qual você está interessado.
3. Em Recursos agrícolas, escolha Frotas.
4. Na lista de frotas, escolha uma frota para exibir seus detalhes. Para comparar a configuração de duas ou mais frotas, marque mais de uma caixa de seleção.
5. Para ver uma lista de trabalhadores na frota, escolha o nome da frota na lista de frotas ou no painel de detalhes.

Se o monitor já estiver aberto, você poderá selecionar a frota na lista de frotas no painel de navegação esquerdo.

## Visualize e gerencie trabalhos, etapas e tarefas no Deadline Cloud

Quando você seleciona uma fila, a seção de monitoramento de trabalhos do monitor do Deadline Cloud mostra os trabalhos nessa fila, as etapas do trabalho e as tarefas em cada etapa. Ao selecionar um trabalho, etapa ou tarefa, você pode usar o menu Ações para gerenciar cada um.

Para abrir o monitor de tarefas, siga as etapas para visualizar uma fila e selecione a tarefa, etapa ou tarefa com a qual trabalhar. [Veja detalhes da fila e da frota no Deadline Cloud](#)

Para trabalhos, etapas e tarefas, você pode fazer o seguinte:

- Altere o status para Enfileirado, Bem-sucedido, Falha ou Cancelado.
- Baixe a saída processada do trabalho, etapa ou tarefa.
- Copie a ID do trabalho, etapa ou tarefa.

Para o trabalho selecionado, você pode:

- Arquive o trabalho.
- Modifique as propriedades da tarefa, como alterar a priorização ou visualizar dependências passo a passo.
- Veja detalhes adicionais usando os parâmetros do trabalho.

Para obter mais informações, consulte [Veja os detalhes do trabalho no Deadline Cloud](#).

Para cada etapa, você pode:

- Visualize as dependências da etapa. As dependências de uma etapa devem ser concluídas antes da execução da etapa.

Para obter detalhes, consulte [Veja uma etapa no Deadline Cloud](#).

Para cada tarefa, você pode:

- Visualize os registros da tarefa.
- Visualize os parâmetros da tarefa.

Para ter mais informações, consulte [Exibir uma tarefa no Deadline Cloud](#).

## Veja os detalhes do trabalho no Deadline Cloud

A página Job Monitor no monitor Deadline Cloud fornece o seguinte:

- Uma visão geral do progresso de um trabalho.
- Uma visão das etapas e tarefas que compõem o trabalho.

Escolha um trabalho na lista para ver uma lista de etapas do trabalho e, em seguida, escolha uma etapa na lista de etapas para visualizar as tarefas do trabalho. Depois de escolher um item, você pode usar o menu Ações desse item para ver os detalhes.

Para ver os detalhes do trabalho

1. Siga as etapas para ver uma fila. [Veja detalhes da fila e da frota no Deadline Cloud](#)
2. No painel de navegação, selecione a fila para a qual você enviou seu trabalho.
3. Selecione um trabalho usando um dos seguintes métodos:
  - a. Na lista de trabalhos, selecione um trabalho para ver seus detalhes.
  - b. No campo de pesquisa, insira qualquer texto associado ao trabalho, como o nome do trabalho ou o usuário que criou o trabalho. Nos resultados exibidos, selecione o trabalho que você deseja visualizar.

Os detalhes de um trabalho incluem as etapas do trabalho e as tarefas em cada etapa. Você pode usar o menu Ações para fazer o seguinte:

- Altere o status do trabalho.
- Visualize e modifique as propriedades de uma tarefa. Você pode visualizar as dependências entre as etapas do trabalho e alterar a prioridade do trabalho. Geralmente, trabalhos com maior prioridade são concluídos mais cedo.
- Visualize os parâmetros do trabalho que foram definidos quando o trabalho foi enviado.
- Baixe a saída de um trabalho. Quando você baixa a saída de uma tarefa, ela contém toda a saída gerada pelas etapas e tarefas da tarefa.

## Veja uma etapa no Deadline Cloud

Use o monitor AWS Deadline Cloud para visualizar as etapas em seus trabalhos de processamento. No Monitor de tarefas, a lista Etapas mostra a lista de etapas que compõem a tarefa selecionada. Quando você seleciona uma etapa, a lista de tarefas mostra as tarefas na etapa.

Para ver uma etapa

1. Siga as etapas [Veja os detalhes do trabalho no Deadline Cloud](#) para ver uma lista de trabalhos.
2. Na lista Jobs (Tarefas), selecione uma tarefa.
3. Selecione uma etapa na lista Etapas.

Você pode usar o menu Ações para fazer o seguinte:

- Altere o status da etapa.
- Faça o download da saída da etapa. Quando você baixa a saída de uma etapa, ela contém toda a saída gerada pelas tarefas na etapa.
- Visualize as dependências de uma etapa. A tabela de dependências mostra uma lista de etapas que devem ser concluídas antes do início da etapa selecionada e uma lista de etapas que estão aguardando a conclusão dessa etapa.

## Exibir uma tarefa no Deadline Cloud

Use o monitor AWS Deadline Cloud para visualizar as tarefas em seus trabalhos de processamento. No Job Monitor, a lista Tarefas mostra as tarefas que compõem a etapa selecionada na lista Etapas.

Para ver uma tarefa

1. Siga as etapas [Veja os detalhes do trabalho no Deadline Cloud](#) para ver uma lista de trabalhos.
2. Na lista Jobs (Tarefas), selecione uma tarefa.
3. Selecione uma etapa na lista Etapas.
4. Selecione uma tarefa na lista Tarefas.

Você pode usar o menu Ações para fazer o seguinte:

- Altere o status da tarefa.

- Visualize os registros de tarefas. Para ter mais informações, consulte [Exibir registros no Deadline Cloud](#).
- Visualize os parâmetros que foram definidos quando a tarefa foi criada.
- Faça o download da saída da tarefa. Quando você baixa a saída de uma tarefa, ela contém somente a saída gerada pela tarefa selecionada.

## Exibir registros no Deadline Cloud

Os registros fornecem informações detalhadas sobre o status e o processamento das tarefas. No monitor do AWS Deadline Cloud, você pode ver os dois tipos de registros a seguir:

- Os registros da sessão detalham o cronograma das ações, incluindo:
  - Ações de configuração, como sincronização de anexos e carregamento do ambiente de software
  - Executando uma tarefa ou um conjunto de tarefas
  - Ações de encerramento, como desligar o ambiente de um trabalhador

Uma sessão inclui o processamento de pelo menos uma tarefa e pode incluir várias tarefas. Os registros de sessão também mostram informações sobre o tipo de instância, vCPU e memória do Amazon Elastic Compute Cloud (Amazon EC2). Os registros de sessão também incluem um link para o registro do trabalhador usado na sessão.

- Os registros do trabalhador fornecem detalhes sobre o cronograma das ações que um trabalhador processa durante seu ciclo de vida. Os registros do trabalhador podem conter informações sobre várias sessões.

Você pode baixar os registros da sessão e do trabalhador para poder examiná-los offline.

Para ver os registros da sessão

1. Siga as etapas [Veja os detalhes do trabalho no Deadline Cloud](#) para ver uma lista de trabalhos.
2. Na lista Jobs (Tarefas), selecione uma tarefa.
3. Selecione uma etapa na lista Etapas.
4. Selecione uma tarefa na lista Tarefas.
5. No menu Ações, escolha Exibir registros.

A seção Cronogramas mostra um resumo das ações da tarefa. Para ver mais tarefas executadas na sessão e ver as ações de encerramento da sessão, escolha Exibir registros de todas as tarefas.

Para visualizar os registros do trabalhador de uma tarefa

1. Siga as etapas [Veja os detalhes do trabalho no Deadline Cloud](#) para ver uma lista de trabalhos.
2. Na lista Jobs (Tarefas), selecione uma tarefa.
3. Selecione uma etapa na lista Etapas.
4. Selecione uma tarefa na lista Tarefas.
5. No menu Ações, escolha Exibir registros.
6. Escolha Informações da sessão.
7. Escolha Exibir registro do trabalhador.

Para ver os registros dos trabalhadores a partir dos detalhes da frota

1. Siga as etapas [Veja detalhes da fila e da frota no Deadline Cloud](#) para ver uma frota.
2. Selecione uma ID de trabalhador na lista de trabalhadores.
3. No menu Ações, escolha Exibir registros do trabalhador.

## Baixe a saída finalizada no Deadline Cloud


Depois que um trabalho for concluído, você poderá usar o monitor AWS Deadline Cloud para baixar os resultados para sua estação de trabalho. O arquivo de saída é armazenado com o nome e o local que você especificou ao criar o trabalho.

Os arquivos de saída são armazenados indefinidamente. Para reduzir os custos de armazenamento, considere criar uma configuração de ciclo de vida do S3 para o bucket Amazon S3 da sua fila. Para obter mais informações, consulte [Gerenciando seu ciclo de vida de armazenamento no Guia do usuário do Amazon Simple Storage Service](#).

Para baixar a saída finalizada de um trabalho, etapa ou tarefa

1. Siga as etapas [Veja os detalhes do trabalho no Deadline Cloud](#) para ver uma lista de trabalhos.
2. Selecione o trabalho, a etapa ou a tarefa para a qual você deseja baixar a saída.

- Se você selecionar um trabalho, poderá baixar toda a saída de todas as tarefas em todas as etapas desse trabalho.
  - Se você selecionar uma etapa, poderá baixar toda a saída de todas as tarefas dessa etapa.
  - Se você selecionar uma tarefa, poderá baixar a saída dessa tarefa individual.
3. No menu Ações, escolha Baixar saída.
  4. A saída será baixada para o local definido quando o trabalho foi enviado.

 Note

Atualmente, o download da saída usando o menu só é suportado por Windows Linux e. Se você tiver um Mac e escolher o item de menu Baixar saída, uma janela mostrará o AWS CLI comando que você pode usar para baixar a saída renderizada.

# Fazendas Deadline Cloud

Um farm é um contêiner para filas que gerenciam trabalhos e frotas de recursos computacionais que realizam tarefas.

## Tópicos

- [Crie uma fazenda](#)
- [Excluir uma fazenda](#)
- [Editar uma fazenda](#)

## Crie uma fazenda

1. No [console do Deadline Cloud](#), escolha Ir para o painel.
2. Na seção Fazendas do painel do Deadline Cloud, escolha Ações → Criar fazenda.
  - Como alternativa, no painel do lado esquerdo, escolha Fazendas e outros recursos e, em seguida, escolha Criar fazenda.
3. Adicione um nome para sua fazenda.
4. Em Descrição, insira a descrição da fazenda. Uma descrição clara pode ajudá-lo a identificar rapidamente o propósito da sua fazenda.
5. (Opcional) Por padrão, seus dados são criptografados com uma chave que AWS possui e gerencia para sua segurança. Você pode escolher Personalizar configurações de criptografia (avançadas) para usar uma chave existente ou criar uma nova que você gerencie.

Se você optar por personalizar as configurações de criptografia usando a caixa de seleção, insira um AWS KMS ARN ou crie um AWS KMS novo escolhendo Criar nova chave KMS.

6. (Opcional) Escolha Adicionar nova tag para adicionar uma ou mais tags à sua fazenda.
7. Escolha Criar fazenda. Após a criação, sua fazenda é exibida.

## Excluir uma fazenda

1. No painel do Deadline Cloud, escolha Fazendas e outros recursos.
2. Na lista de fazendas, selecione a fazenda ou fazendas que você deseja excluir e escolha Excluir.



## Editar uma fazenda

1. No painel do Deadline Cloud, escolha Fazendas e outros recursos.
2. Na lista de fazendas, selecione a fazenda ou fazendas que você deseja excluir e escolha Editar.
3. Na janela de edição exibida, altere o nome ou a descrição da fazenda e escolha Salvar alterações.

# Filas do Deadline Cloud

Uma fila é um recurso da fazenda que gerencia e processa trabalhos.

Para trabalhar com filas, você já deve ter um monitor e uma fazenda configurados.

## Tópicos

- [Criar uma fila](#)
- [Crie um ambiente de fila](#)
- [Excluir uma fila](#)
- [Editar uma fila](#)
- [Associe uma fila e uma frota](#)

## Criar uma fila

1. No painel do [console do Deadline Cloud](#), selecione a fazenda para a qual você deseja criar uma fila.
  - Como alternativa, no painel do lado esquerdo, escolha Fazendas e outros recursos e selecione a fazenda para a qual você deseja criar uma fila.
2. Na guia Filas, escolha Criar fila.
3. Insira um nome para sua fila.
4. Em Descrição, insira a descrição da fila. Uma descrição ajuda você a identificar a finalidade da sua fila.
5. Para anexos de trabalho, você pode criar um novo bucket do Amazon S3 ou escolher um bucket do Amazon S3 existente.
  - a. Para criar um novo bucket do Amazon S3
    - i. Selecione Criar novo repositório de tarefas.
    - ii. Insira um nome para o bucket. Recomendamos dar um nome ao bucketdeadlinecloud-job-attachments-[MONITORNAME].
    - iii. Insira um prefixo raiz para definir ou alterar a localização raiz da fila.
  - b. Para escolher um bucket Amazon S3 existente

- i. Selecione Escolher um bucket do S3 existente > Procurar no S3.
  - ii. Selecione o bucket do S3 para sua fila na lista de buckets disponíveis.
6. (Opcional) Para associar sua fila a uma frota gerenciada pelo cliente, selecione Habilitar associação com frotas gerenciadas pelo cliente.
7. Se você habilitar a associação com frotas gerenciadas pelo cliente, deverá concluir as etapas a seguir.

**⚠ Important**

É altamente recomendável especificar usuários e grupos para a funcionalidade de execução como. Caso contrário, isso degradará a postura de segurança de sua fazenda, pois os trabalhos podem então fazer tudo o que o agente do trabalhador pode fazer. Para obter mais informações sobre os possíveis riscos de segurança, consulte [Executar trabalhos como usuários e grupos](#).

- a. Para Executar como usuário:

Para fornecer credenciais para os trabalhos da fila, selecione Usuário configurado em fila.

Ou, para optar por não definir suas próprias credenciais e executar trabalhos como usuário do agente de trabalho, selecione Usuário do agente de trabalho.

- b. (Opcional) Em Executar como credenciais de usuário, insira um nome de usuário e um nome de grupo para fornecer credenciais para os trabalhos da fila.

Se você estiver usando uma Windows frota, deverá criar um AWS Secrets Manager segredo que contenha a senha do usuário Run as. Siga estas instruções para criar o segredo. Substitua *jobuser* pelo nome do jobRunAsUser.

- i. Abra PowerShell ou use um prompt de comando como administrador.
- ii. Criar o usuário

```
net user jobuser /add
```

- iii. Defina a senha.

```
net user jobuser *
```

- iv. Crie um perfil local e um diretório inicial para o usuário. Execute o comando a seguir e digite a senha do usuário quando solicitado.

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

8. Exigir um orçamento ajuda a gerenciar os custos da sua fila. Selecione Não exigir um orçamento ou Exigir um orçamento.
9. Sua fila requer permissão para acessar o Amazon S3 em seu nome. Você pode criar uma nova função de serviço ou usar uma função de serviço existente. Se você não tiver uma função de serviço existente, crie e use uma nova função de serviço.
  - a. Para usar uma função de serviço existente, selecione Escolher uma função de serviço e, em seguida, selecione uma função no menu suspenso.
  - b. Para criar uma nova função de serviço, selecione Criar e usar uma nova função de serviço e, em seguida, insira um nome e uma descrição da função.
10. (Opcional) Para adicionar variáveis de ambiente ao ambiente de fila, escolha Adicionar nova variável de ambiente e, em seguida, insira um nome e um valor para cada variável adicionada.
11. (Opcional) Escolha Adicionar nova tag para adicionar uma ou mais tags à sua fila.
12. Para criar um ambiente de Conda fila padrão, mantenha a caixa de seleção marcada. Para saber mais sobre ambientes de fila, consulte [Criar um ambiente de fila](#). Se você estiver criando uma fila para uma frota gerenciada pelo cliente, desmarque a caixa de seleção.
13. Selecione Criar fila.

## Crie um ambiente de fila

Um ambiente de fila é um conjunto de variáveis e comandos de ambiente que configuram os trabalhadores da frota. Você pode usar ambientes de fila para fornecer aplicativos de software, variáveis de ambiente e outros recursos para trabalhos na fila.

Ao criar uma fila, você tem a opção de criar um ambiente de Conda fila padrão. Esse ambiente fornece às frotas gerenciadas por serviços acesso a pacotes para aplicativos e renderizadores de DCC de parceiros. Para ter mais informações, consulte [Ambiente de Conda fila padrão](#).

Você pode adicionar ambientes de fila usando o console ou editando diretamente o modelo json ou YAML. Este procedimento descreve como criar um ambiente com o console.

1. Para adicionar um ambiente de fila a uma fila, navegue até a fila e selecione a guia Ambientes de fila.
2. Escolha Ações e, em seguida, Criar novo com formulário.
3. Insira um nome e uma descrição para o ambiente de filas.
4. Escolha Adicionar nova variável de ambiente e, em seguida, insira um nome e um valor para cada variável adicionada.
5. (Opcional) Insira uma prioridade para o ambiente de fila. A prioridade indica a ordem em que esse ambiente de fila será executado no trabalhador. Ambientes de fila de maior prioridade serão executados primeiro.
6. Escolha Criar ambiente de fila.

## Ambiente de Conda fila padrão

Ao criar uma fila associada a uma frota gerenciada por serviços, você tem a opção de adicionar um ambiente de fila padrão que suporte o download e [Conda](#) a instalação de pacotes em um ambiente virtual para seus trabalhos.

Conda fornece pacotes de canais. Um canal é um local onde os pacotes são armazenados. O Deadline Cloud fornece um canal que hospeda pacotes que oferecem suporte a aplicativos e renderizadores de DCC parceiros. `deadline-cloud` Os pacotes são:

- Liquidificador
  - `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`

Quando você envia um trabalho para uma fila com o Conda ambiente padrão, o ambiente adiciona dois parâmetros ao trabalho. Esses parâmetros especificam os Conda pacotes e canais a serem usados para configurar o ambiente do trabalho antes que as tarefas sejam processadas. Os parâmetros são:

- `CondaPackages`— uma lista separada por espaços das [especificações de pacotes correspondentes](#), como `blender=3.6` ou `numpy>1.22`. O padrão é vazio para ignorar a criação de um ambiente virtual.
- `CondaChannels`— uma lista separada por espaços de [Conda canais](#) `deadline-cloud`, como `conda-forge`, ou `s3://DOC-EXAMPLE-BUCKET/conda/channel`. O padrão é `deadline-cloud` um canal disponível para frotas gerenciadas por serviços que fornece aplicativos e renderizadores de DCC parceiros.

Quando você usa um remetente integrado para enviar um trabalho do seu DCC para o Deadline Cloud, o remetente preenche o valor do `CondaPackages` parâmetro com base no aplicativo e no remetente do DCC. Por exemplo, se você estiver usando o Blender, o `CondaPackage` parâmetro será definido como `blender=3.6.* blender-openjd=0.4.*`

## Excluir uma fila

### Warning

Você não poderá recuperar os trabalhos em uma fila se excluir a fila. A exclusão da fila também exclui os trabalhos nessa fila.

1. No painel do Deadline Cloud, escolha Fazendas e outros recursos.
2. Na lista de fazendas, selecione a fazenda que contém a fila a ser excluída.
3. Selecione a fila e, em seguida, escolha Excluir.
4. Na janela de confirmação, escolha Excluir. Sua fila e todos os trabalhos na fila são excluídos.

## Editar uma fila

1. No painel do Deadline Cloud, escolha Fazendas e outros recursos.
2. Na lista de fazendas, selecione a fazenda que contém a fila para edição.

3. Selecione a fila e, em seguida, escolha Editar.
4. Você pode editar o nome, a descrição, o requisito de orçamento, a opção Executar como usuário e a função de serviço atribuída. Você também pode associar uma frota existente à sua fila.
5. Escolha Salvar alterações.

## Associe uma fila e uma frota

1. Selecione a fila que você deseja associar a uma frota.
2. Para selecionar uma frota para associar à sua fila, escolha Associar frotas.
3. Escolha o menu suspenso Selecionar frotas. Uma lista das frotas disponíveis é exibida.
4. Na lista de frotas disponíveis, marque a caixa de seleção ao lado da frota ou frotas que você deseja associar à sua fila.
5. Selecione Associar. O status da associação da frota agora deve ser Associado.

# Gerencie frotas do Deadline Cloud

Esta seção explica como gerenciar frotas gerenciadas por serviços (SMF) e frotas gerenciadas pelo cliente (CMF) para o Deadline Cloud.

Você pode configurar dois tipos de frotas do Deadline Cloud:

- As frotas gerenciadas por serviços são frotas de trabalhadores que têm configurações padrão fornecidas por esse serviço, o Deadline Cloud. Essas configurações padrão foram projetadas para serem eficientes e econômicas.
- As frotas gerenciadas pelo cliente (CMFs) são frotas de trabalhadores que você gerencia. Um CMF pode residir na AWS infraestrutura, no local ou em um data center co-localizado. Um CMF fornece controle e responsabilidade totais da frota. Isso inclui provisionamento, operações, gerenciamento e descomissionamento de trabalhadores na frota.

## Tópicos

- [Gerencie frotas gerenciadas pelo serviço Deadline Cloud](#)
- [Gerencie frotas gerenciadas pelo cliente do Deadline Cloud](#)

## Gerencie frotas gerenciadas pelo serviço Deadline Cloud

As frotas gerenciadas por serviços são frotas de trabalhadores que têm configurações padrão fornecidas pelo Deadline Cloud. Essas configurações padrão foram projetadas para serem eficientes e econômicas.

1. Para criar uma frota gerenciada por serviços (SMF), navegue até a fazenda na qual você deseja criar a frota.
2. Selecione a guia Frotas.
3. Selecione Create fleet (Criar frota).
4. Insira um nome para sua frota.
5. Insira uma Descrição. Uma descrição clara pode ajudá-lo a identificar rapidamente a finalidade da sua frota.
6. Selecione o tipo de frota gerenciada por serviços.



7. Escolha a opção de mercado de instâncias spot ou sob demanda para sua frota. As instâncias spot são uma capacidade sem reserva que você pode usar com desconto, mas pode ser interrompida por solicitações sob demanda. As instâncias sob demanda têm um preço por segundo, mas não têm compromisso de longo prazo e não serão interrompidas. Por padrão, as frotas usam instâncias spot.
8. Opcional Defina o número máximo de instâncias para escalar a frota de forma que a capacidade esteja disponível para os trabalhos na fila. Recomendamos que você deixe o número mínimo de instâncias em **0** para garantir que a frota libere todas as instâncias quando nenhum trabalho estiver na fila.
9. Para obter acesso ao serviço para sua frota, selecione uma função existente ou crie uma nova função. Uma função de serviço fornece credenciais às instâncias da frota, concedendo-lhes permissão para processar trabalhos, e aos usuários no monitor, para que possam ler as informações do registro.
10. Escolha Próximo.
11. Insira as vCPUs mínimas e máximas de que você precisa para sua frota.
12. Insira a memória mínima e máxima de que você precisa para sua frota.
13. Opcional Você pode optar por permitir ou excluir tipos de instância específicos da sua frota para garantir que somente esses tipos de instância sejam usados para essa frota.
14. Opcional: Você pode especificar o tamanho do volume gp3 do Amazon Elastic Block Store (Amazon EBS) que será anexado aos trabalhadores dessa frota. Para obter mais informações, consulte o [guia do usuário do EBS](#).
15. Escolha Próximo.
16. Opcional Defina os requisitos personalizados do trabalhador que definam as características dessa frota que podem ser combinadas com os requisitos personalizados do host especificados nos envios de trabalhos. Um exemplo é um tipo de licença específico se você planeja conectar sua frota ao seu próprio servidor de licenças.
17. Escolha Próximo.
18. Opcional Para associar sua frota a uma fila, selecione uma fila no menu suspenso. Se a fila for configurada com o ambiente de Conda fila padrão, sua frota receberá automaticamente pacotes que oferecem suporte a aplicativos e renderizadores de DCC parceiros. Para obter uma lista dos pacotes fornecidos, consulte [Ambiente de Conda fila padrão](#).
19. Escolha Próximo.
20. Opcional Para adicionar uma etiqueta à sua frota, escolha Adicionar nova etiqueta e, em seguida, insira a chave e o valor dessa etiqueta.

21. Escolha Próximo.
22. Revise as configurações da sua frota e escolha Criar frota. Após a criação, sua frota é exibida.

## Compatibilidade do VFX Reference Platform

VFX Reference Platform é uma plataforma alvo comum para o setor de efeitos visuais. Para usar a instância padrão do Amazon EC2 de frota gerenciada por serviços executando o Amazon Linux 2023 com software compatível com o., você deve ter em mente VFX Reference Platform as seguintes considerações ao usar uma frota gerenciada por serviços.

O VFX Reference Platform é atualizado anualmente. Essas considerações sobre o uso de um AL2023, incluindo frotas gerenciadas pelo serviço Deadline Cloud, são baseadas nas plataformas de referência do ano civil (CY) de 2022 a 2024. Para ter mais informações, consulte [VFX Reference Platform](#).

### Note

Se você estiver criando um custom Amazon Machine Image (AMI) para uma frota gerenciada pelo cliente, você pode adicionar esses requisitos ao preparar a instância do Amazon EC2.

Para usar o software VFX Reference Platform compatível em uma instância AL2023 do Amazon EC2, considere o seguinte:

- A versão glibc instalada com o AL2023 é compatível para uso em tempo de execução, mas não para criar software compatível com o VFX Reference Platform CY2024 ou anterior.
- O Python 3.9 e 3.11 são fornecidos com a frota gerenciada por serviços, tornando-a compatível com CY2022 e CY2024. VFX Reference Platform O Python 3.7 e 3.10 não são fornecidos na frota gerenciada por serviços. O software que os requer deve fornecer a instalação do Python na fila ou no ambiente de trabalho.
- Alguns componentes da biblioteca Boost fornecidos na frota gerenciada por serviços são da versão 1.75, que não é compatível com o. VFX Reference Platform Se seu aplicativo usa o Boost, você deve fornecer sua própria versão da biblioteca para fins de compatibilidade.
- A atualização 3 do Intel TBB é fornecida na frota gerenciada por serviços. Isso é compatível com VFX Reference Platform CY2022, CY2023 e CY2024.
- Outras bibliotecas com versões especificadas pelo não VFX Reference Platform são fornecidas pela frota gerenciada pelo serviço. Você deve fornecer à biblioteca qualquer aplicativo usado em

uma frota gerenciada por serviços. Para obter uma lista de bibliotecas, consulte a [plataforma de referência](#).

## Gerencie frotas gerenciadas pelo cliente do Deadline Cloud

Esta seção explica como gerenciar uma frota gerenciada pelo cliente (CMF) para o Deadline Cloud.

Os CMFs são frotas de trabalhadores que você gerencia. Um CMF pode residir na AWS infraestrutura, no local ou em um data center co-localizado. Um CMF fornece controle e responsabilidade totais da frota. Isso inclui provisionamento, operações, gerenciamento e descomissionamento de trabalhadores na frota.

### Tópicos

- [Crie uma frota gerenciada pelo cliente](#)
- [Instalação e configuração do host de trabalho](#)
- [Gerencie o acesso aos segredos dos usuários de tarefas do Windows](#)
- [Instale e configure o software necessário para trabalhos](#)
- [Configurando credenciais AWS](#)
- [Criar uma Amazon Machine Image](#)
- [Crie uma infraestrutura de frota com um grupo do Amazon EC2 Auto Scaling](#)
- [Conecte frotas gerenciadas pelo cliente a um endpoint de licença](#)

## Crie uma frota gerenciada pelo cliente


Para criar uma frota gerenciada pelo cliente (CMF), conclua as etapas a seguir.

### Deadline Cloud console

Para usar o console do Deadline Cloud para criar uma frota gerenciada pelo cliente


1. Abra o [console](#) do Deadline Cloud.
2. Selecione Fazendas. Uma lista das fazendas disponíveis é exibida.
3. Selecione o nome da Fazenda na qual você deseja trabalhar.
4. Selecione a guia Frotas.
5. Selecione Create fleet (Criar frota).

6. Insira um nome para sua frota.
7. (Opcional) Insira uma descrição para sua frota.
8. Selecione Gerenciado pelo cliente para o tipo de frota.
9. Selecione um tipo de Auto Scaling. Para obter mais informações, consulte [Usar EventBridge para lidar com eventos do Auto Scaling](#).
  - Sem escalabilidade: você está criando uma frota local e quer optar por não participar do Deadline Cloud Auto Scaling.
  - Recomendações de escalabilidade: Você está criando uma frota do Amazon Elastic Compute Cloud (Amazon EC2).
10. Selecione o acesso ao serviço da sua frota.
  - a. Recomendamos usar a opção Criar e usar uma nova função de serviço para cada frota para um controle de permissões mais granular. Essa opção é selecionada por padrão.
  - b. Você também pode usar uma função de serviço existente selecionando Escolher uma função de serviço.
11. Revise suas seleções e escolha Avançar.
12. Selecione um sistema operacional para sua frota. Todos os trabalhadores de uma frota devem ter um sistema operacional comum.
13. Selecione a arquitetura da CPU do host.
14. Selecione os seguintes requisitos de hardware para os funcionários hospedados nessa frota.
  - a. Selecione os requisitos mínimos e máximos de hardware de vCPU e memória para atender às demandas de carga de trabalho de suas frotas.
  - b. (Opcional) Selecione o requisito de GPU e insira as GPUs mínima e máxima.
15. Revise suas seleções e escolha Avançar.
16. (Opcional) Defina os requisitos personalizados do trabalhador.
17. Usando o menu suspenso, selecione uma ou mais filas para associar à frota.

 Note

Recomendamos associar uma frota somente a filas que estejam todas no mesmo limite de confiança. Isso garante um forte limite de segurança entre a execução de trabalhos no mesmo trabalhador.

18. Revise as associações de filas e selecione Avançar.
19. (Opcional) Para o ambiente de fila padrão do Conda, criaremos um ambiente para sua fila que instalará os pacotes Conda solicitados pelos trabalhos.

 Note

O ambiente de fila Conda é usado para instalar pacotes Conda solicitados por trabalhos. Normalmente, você deve desmarcar o ambiente de filas Conda nas filas associadas aos CMFs porque os CMFs não terão os comandos Conda necessários instalados por padrão.

20. (Opcional) Adicione tags ao seu CMF. Para obter mais informações, consulte Como [marcar seus AWS recursos](#).
21. Revise a configuração da sua frota e faça as alterações.
22. Selecione Create fleet (Criar frota).
23. Selecione a guia Frotas e anote a ID da frota.

## AWS CLI

Para usar o AWS CLI para criar uma frota gerenciada pelo cliente

1. Abra AWS CLI o.
2. Edite `fleet-trust-policy.json`.
  - a. Adicione a seguinte política do IAM, substituindo o texto em *ITÁLICO* pelo ID da sua AWS conta e pelo ID do farm do 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. Salve as alterações.

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

a. Adicione a seguinte política do 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. Salve as alterações.

4. Adicione uma função do IAM para os trabalhadores da sua frota usarem.

```

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. Edite `create-fleet-request.json`.

a. Adicione a seguinte política do IAM, substituindo o texto em **ITÁLICO** pelos valores do CMF.

**Note**

Você pode encontrar o ***ROLE\_ARN*** no `create-cmf-fleet.json`

Para o ***OS\_FAMILY***, você deve escolher um `doslinux`, `macos` ou `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. Salve as alterações.

6. Crie sua frota.

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

## Instalação e configuração do host de trabalho

Um host de trabalho se refere a uma máquina host que executa um funcionário do Deadline Cloud. Esta seção explica como configurar o host de trabalho e configurá-lo de acordo com suas necessidades específicas. Cada host de trabalho executa um programa chamado agente de trabalho. O agente do trabalhador é responsável por:

- Gerenciando o ciclo de vida do trabalhador.
- Sincronizando o trabalho atribuído, seu progresso e resultados.
- Monitorando o trabalho em execução.
- Encaminhando registros para destinos configurados.



Recomendamos que você use o agente de trabalho do Deadline Cloud fornecido. O agente de trabalho é de código aberto e incentivamos solicitações de recursos, mas você também pode desenvolver e personalizar para atender às suas necessidades.

Para concluir as tarefas nas seções a seguir, você precisa do seguinte:

## Linux

- Uma instância Linux baseada no Amazon Elastic Compute Cloud (Amazon EC2). Recomendamos o Amazon Linux 2023.
- `sudo` privilégios.
- Python 3.9 ou superior.

## Windows

- Uma instância Windows baseada no Amazon Elastic Compute Cloud (Amazon EC2). Nós recomendamos Windows Server 2022.
- Acesso do administrador ao host do trabalhador
- Python 3.9 ou superior instalado para todos os usuários

## Crie e configure um ambiente virtual Python

Você pode criar um ambiente virtual Python Linux se tiver instalado o Python 3.9 ou superior e o colocado no seu `PATH`

Para criar e ativar um ambiente virtual Python

1. Abra AWS CLI o.
2. Crie e ative um ambiente virtual Python.

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

## Instale o agente Deadline Cloud Worker

Depois de configurar seu Python e criar um ambiente virtualLinux, instale os pacotes Python do agente Deadline Cloud Worker.

Para instalar os pacotes Python do agente de trabalho

1. Abra um terminal do .
  - a. AtivadoLinux, abra um terminal como root usuário (ou usesudo/su)
  - b. AtivadoWindows, abra um prompt de comando ou PowerShell terminal do administrador.
2. Baixe e instale os pacotes do agente Deadline Cloud Worker do PyPI:

### Note

AtivadoWindows, os arquivos do agente devem ser instalados no diretório global de pacotes de sites do Python. Atualmente, não há suporte para ambientes virtuais Python.

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

## Configurar o agente Deadline Cloud Worker

Você pode definir as configurações do agente Deadline Cloud Worker de três maneiras.

Recomendamos que você use o sistema operacional configurado por meio de `install-deadline-worker`.

Argumentos da linha de comando — Você pode especificar argumentos ao executar o agente de trabalho do Deadline Cloud na linha de comando. Algumas configurações não estão disponíveis por meio de argumentos de linha de comando. Para ver todos os argumentos de linha de comando disponíveis, digite `deadline-worker-agent --help` para ver todos os argumentos de linha de comando disponíveis.

Variáveis de ambiente — Você pode configurar o agente de trabalho do Deadline Cloud definindo a variável de ambiente começando com `DEADLINE_WORKER_`. Por exemplo, você pode usar `export DEADLINE_WORKER_VERBOSE=true` para definir a saída do agente de trabalho como detalhada. Para obter mais exemplos e informações, consulte `/etc/amazon/deadline/`

`worker.toml.example` on Linux or `C:\ProgramData\Amazon\Deadline\Config\worker.toml.example` on Windows.

Arquivo de configuração — Quando você instala o agente de trabalho, ele cria um arquivo de configuração localizado em `/etc/amazon/deadline/worker.toml` on Linux ou `C:\ProgramData\Amazon\Deadline\Config\worker.toml` on Windows. O agente de trabalho carrega esse arquivo de configuração quando ele é iniciado. Você pode usar o arquivo de configuração de exemplo (`/etc/amazon/deadline/worker.toml.example` ativado Linux ou `C:\ProgramData\Amazon\Deadline\Config\worker.toml.example` ativado Windows) para adaptar o arquivo de configuração padrão do agente de trabalho às suas necessidades específicas.

Por fim, recomendamos que você ative o desligamento automático do agente de trabalho. Isso permite que a frota de trabalhadores aumente quando necessário e seja encerrada quando o trabalho de renderização for concluído. O escalonamento automático ajuda a garantir que você use os recursos somente conforme necessário.

Para ativar o desligamento automático

Como **root** usuário:

- Instale o agente de trabalho com parâmetros **--allow-shutdown**.

Linux

Digite:

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

Windows

Digite:

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

## Crie usuários e grupos de trabalho

Esta seção descreve o relacionamento necessário de usuário e grupo entre o usuário do agente e o `jobRunAsUser` definido em suas filas.

O agente do Deadline Cloud Worker deve ser executado como um usuário dedicado específico do agente no host. Você deve configurar a `jobRunAsUser` propriedade das filas do Deadline Cloud para que os trabalhadores executem os trabalhos de fila como um usuário e grupo específicos do sistema operacional. Isso significa que você pode controlar as permissões compartilhadas do sistema de arquivos que seus trabalhos têm. Ele também fornece um importante limite de segurança entre seus trabalhos e o usuário do agente de trabalho.

### Linuxusuários e grupos de trabalho

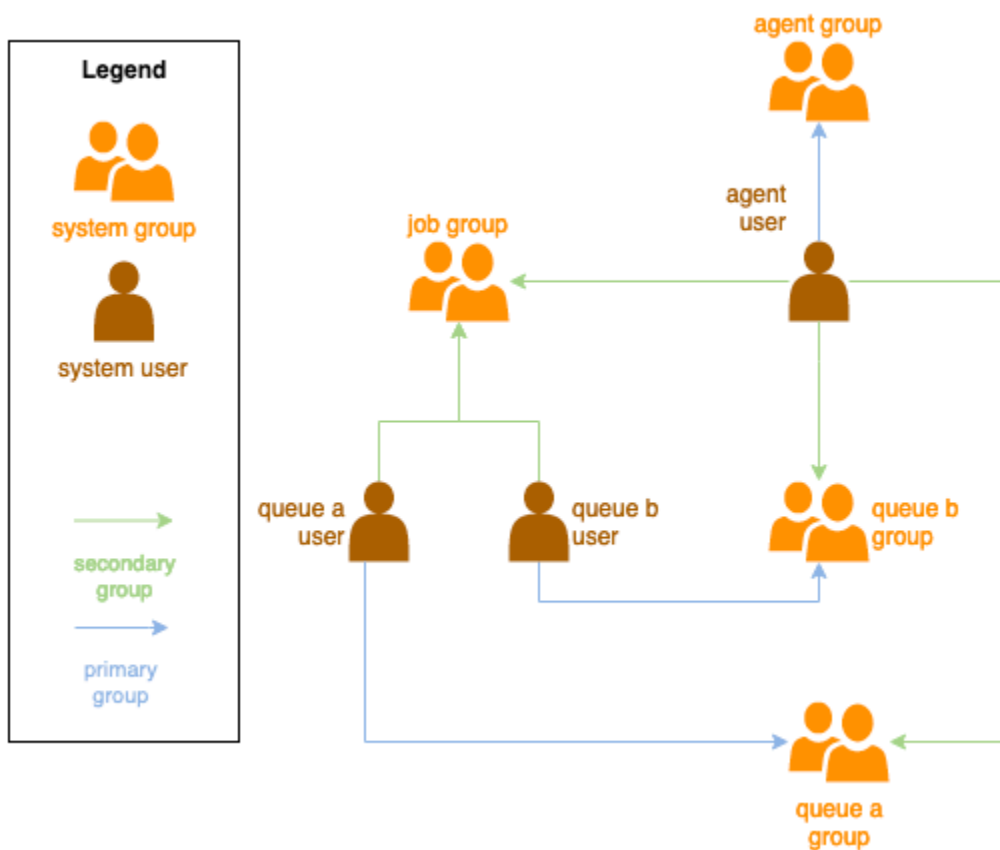
Para configurar seu agente-usuário e `jobRunAsUser` garantir que você atenda aos seguintes requisitos:

- Há um grupo para cada um `jobRunAsUser`, e é o grupo principal para os correspondentes `jobRunAsUser`.
- O usuário-agente pertence ao grupo principal das `jobRunAsUser` filas em que o trabalhador obtém trabalho. Para melhores práticas de segurança, recomendamos isso como um grupo secundário do agente-usuário. Esse grupo compartilhado permite que o agente de trabalho disponibilize arquivos para o trabalho enquanto ele está em execução.
- A `jobRunAsUser` não pertence ao grupo principal do agente-usuário. Para obter as melhores práticas de segurança:
  - Arquivos confidenciais gravados pelo agente de trabalho pertencem ao grupo principal do agente.
  - Se a `jobRunAsUser` pertencer a esse grupo, os arquivos que o agente de trabalho grava poderão ser acessados pelos trabalhos enviados à fila em execução no trabalhador.
- A AWS região padrão deve corresponder à região da fazenda à qual o trabalhador pertence. Para obter mais informações, consulte [Configurações e configurações do arquivo de credenciais](#).

Isso deve ser aplicado a:

- O agente-usuário
- Todas as `jobRunAsUser` contas de fila do trabalhador
- O agente-usuário pode executar `sudo` comandos como o. `jobRunAsUser`

O diagrama a seguir ilustra a relação entre o usuário agente e os `jobRunAsUser` usuários e grupos das filas associadas à frota.



## Usuários do Windows

Para usar um Windows usuário como o `jobRunAsUser`, ele deve atender aos seguintes requisitos:

- Todos os `jobRunAsUser` usuários da fila devem existir.
- Suas senhas devem corresponder ao valor do segredo especificado no `JobRunAsUser` campo da fila. Para obter instruções, consulte a etapa 7 em [Criar uma fila](#).
- O usuário-agente deve ser capaz de fazer login como esses usuários.

## Gerencie o acesso aos segredos dos usuários de tarefas do Windows

Ao configurar uma fila com um Windows `jobRunAsUser`, você deve especificar um segredo do AWS Secrets Manager. Espera-se que o valor desse segredo seja um objeto codificado em JSON do formato:

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

Para que os trabalhadores executem trabalhos conforme a fila está configurada `jobRunAsUser`, a função do IAM da frota deve ter permissões para obter o valor do segredo. Se o segredo for criptografado usando uma chave KMS gerenciada pelo cliente, a função do IAM da frota também deverá ter permissões para descriptografar usando a chave KMS.

É altamente recomendável seguir o princípio do menor privilégio para esses segredos. Isso significa que o acesso para buscar o valor secreto do `jobRunAsUser` → `windows` → de uma fila `passwordArn` deve ser:

- concedido a uma função de frota quando uma associação fila-frota é criada entre a frota e a fila
- revogado de uma função de frota quando uma associação fila-frota é excluída entre a frota e a fila

Além disso, o AWS segredo do Secrets Manager contendo a `jobRunAsUser` senha deve ser excluído quando não estiver mais sendo usado.

## Conceder acesso a uma senha secreta

As frotas do Deadline Cloud exigem acesso à `jobRunAsUser` senha armazenada no segredo da senha da fila quando a fila e a frota estão associadas. Recomendamos usar a política de recursos do AWS Secrets Manager para conceder acesso às funções da frota. Se você seguir rigorosamente essa diretriz, será mais fácil determinar quais funções da frota têm acesso ao segredo.

Para conceder acesso ao segredo

1. Abra o console do AWS Secret Manager para ver o segredo.
2. Na seção “Permissões de recursos”, adicione uma declaração de política no formato:

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

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

## Revogar o acesso a uma senha secreta

Quando uma frota não precisar mais acessar uma fila, remova o acesso à senha secreta da fila `jobRunAsUser`. Recomendamos usar a política de recursos do AWS Secrets Manager para conceder acesso às funções da frota. Se você seguir rigorosamente essa diretriz, será mais fácil determinar quais funções da frota têm acesso ao segredo.

Para revogar o acesso ao segredo

1. Abra o console do AWS Secret Manager para ver o segredo.
2. Na seção Permissões de recursos, remova a declaração de política do formulário:

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

## Instale e configure o software necessário para trabalhos

Depois de configurar o agente de trabalho do Deadline Cloud, você pode preparar o host do trabalhador com qualquer software necessário para executar trabalhos.

Quando você envia um trabalho para uma fila com um associado `jobRunAsUser`, o trabalho é executado como esse usuário. Todos os comandos devem estar disponíveis no PATH desse usuário.

No Linux, você pode especificar o PATH para um usuário em uma das seguintes opções:

- deles `~/.bashrc` ou `~/.bash_profile`
- arquivos de configuração do sistema, como `/etc/profile.d/*` e `/etc/profile`
- scripts de inicialização do shell: `/etc/bashrc`.

No Windows, você pode especificar o PATH para um usuário em uma das seguintes opções:

- suas variáveis de ambiente específicas do usuário
- as variáveis de ambiente de todo o sistema

## Instale adaptadores de ferramentas de criação de conteúdo digital

O Deadline Cloud fornece aplicativos de criação de conteúdo digital (DCC) com suporte de integração primário. Para usar essas integrações em uma frota gerenciada pelo cliente, você deve instalar o software DCC e os adaptadores.

Para instalar adaptadores DCC em uma frota gerenciada pelo cliente

1. Abra o terminal a.
  - a. No Linux, abra um terminal como root usuário (ou `usesudo/su`)
  - b. No Windows, abra um prompt de comando ou PowerShell terminal do administrador.
2. Instale os pacotes do adaptador Deadline Cloud.

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



## Configurando credenciais AWS

Esta seção explica como configurar as AWS credenciais.

Essa fase inicial do ciclo de vida do trabalhador é acelerada. Nessa fase, o software do agente de trabalho cria um trabalhador em sua frota e obtém AWS credenciais da função de sua frota para operações futuras.

### AWS credentials for Amazon EC2

Para configurar AWS credenciais para o Amazon EC2


1. Abra o console IAM em <https://console.aws.amazon.com/iam/>.
2. Selecione Funções no painel de navegação e, em seguida, Criar função.
3. Selecione o AWS serviço.
4. Selecione EC2 como serviço ou caso de uso e, em seguida, selecione Avançar.
5. Anexe a política AWSDeadlineCloud-WorkerHost AWS gerenciada.

### On-premise AWS credentials

Para configurar AWS credenciais locais

1. Abra o console IAM em <https://console.aws.amazon.com/iam/>.
2. Selecione Funções no painel de navegação e, em seguida, Criar função.
3. Selecione Conta da AWS e, em seguida, selecione Avançar.
4. Anexe a política AWSDeadlineCloud-WorkerHost AWS gerenciada.
5. Gere acesso e chaves secretas do AWS IAM para o usuário do IAM:
  - a. Para IAM Role Anywhere, consulte [IAM Roles Anywhere](#).
  - b. Para obter a maneira mais segura de configurar credenciais no host, consulte [Obter credenciais de segurança temporárias do AWS Identity and Access Management Roles Anywhere](#).
  - c. Você também pode usar a CLI como autenticação alternativa. Para obter mais informações, consulte [Autenticar com credenciais de usuário do IAM](#).
6. Armazene essas chaves no arquivo de AWS credenciais do agente-usuário no sistema de arquivos do host do trabalhador.


- a. No Linux, isso está localizado em `~/.aws/credentials`
- b. No Windows, ele está localizado em `%USERPROFILE%\aws\credentials`

 Note

As credenciais só devem ser acessadas pelo nome de usuário do sistema operacional (`deadline-worker-agent`) que instalou o agente de trabalho.

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


7. Altere o `deadline-worker-agent` proprietário e as permissões.

 Note

Se você alterou o nome do usuário (`deadline-worker-agent`) do sistema operacional ao instalar o agente de trabalho, use esse nome em vez disso.

## Criar uma Amazon Machine Image

Para criar um Amazon Machine Image (AMI) para usar em uma frota gerenciada pelo cliente (CMF) do Amazon Elastic Compute Cloud (Amazon EC2), conclua as tarefas nesta seção. Você deve criar uma instância do Amazon EC2 antes de continuar. Para obter mais informações, consulte [Inicie sua instância](#) no Guia do usuário do Amazon EC2 para instâncias Linux.

 Important

A criação de um AMI cria um snapshot dos volumes anexados à instância do Amazon EC2. Qualquer software instalado na instância persiste, portanto, instâncias, que são reutilizadas quando você executa instâncias a partir do. AMI Recomendamos adotar uma estratégia de correção e atualizar regularmente qualquer software novo AMI com atualizado antes de aplicá-lo à sua frota.

## Prepare a instância do Amazon EC2

Antes de criar um AMI, você deve excluir o estado do trabalhador. O estado do trabalhador persiste entre os lançamentos do agente de trabalho. Se esse estado persistir no AMI, todas as instâncias executadas a partir dele compartilharão o mesmo estado.

Também recomendamos que você exclua todos os arquivos de log existentes. Os arquivos de log podem permanecer em uma instância do Amazon EC2 quando você prepara a AMI. A exclusão desses arquivos minimiza a confusão ao diagnosticar possíveis problemas nas frotas de trabalhadores que usam a AMI.

Você também deve habilitar o serviço de sistema do agente de trabalho para que o agente do Deadline Cloud Worker seja iniciado quando o Amazon EC2 for iniciado.

Por fim, recomendamos que você ative o desligamento automático do agente de trabalho. Isso permite que a frota de trabalhadores aumente quando necessário e seja encerrada quando o trabalho de renderização for concluído. Esse escalonamento automático ajuda a garantir que você use os recursos somente conforme necessário.

Para preparar a instância do Amazon EC2

1. Abra o console do Amazon EC2.
2. Iniciar uma instância do Amazon EC2. Para obter mais informações, consulte [Executar sua instância](#).
3. Configure o host para se conectar ao seu provedor de identidade (IdP) e, em seguida, monte qualquer sistema de arquivos compartilhado necessário.
4. Siga os tutoriais para [Instale o agente Deadline Cloud Worker](#), em seguida [Configurar agente de trabalho](#), e [Crie usuários e grupos de trabalho](#)
5. Se você estiver preparando um AMI baseado no Amazon Linux 2023 para executar software compatível com a VFX Reference Platform, precisará atualizar vários requisitos. Para mais informações, consulte [Compatibilidade do VFX Reference Platform](#).
6. Abra um terminal.
  - a. No Linux, abra um terminal como root usuário (ou usesudo/su)
  - b. No Windows, abra um prompt de comando ou PowerShell terminal do administrador.
7. Certifique-se de que o serviço de trabalho não esteja em execução e configurado para iniciar na inicialização:

- a. No Linux, execute

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

- b. No Windows, execute

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

8. Exclua o estado do trabalhador.

- a. No Linux, execute

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

- b. No Windows, execute

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

9. Exclua os arquivos de log.


- a. No Linux, execute

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

- b. No Windows, execute

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

10. No Windows, é recomendável executar o aplicativo Amazon EC2Launch Settings encontrado no menu Iniciar para concluir a preparação final do host e o desligamento da instância.

 Note

Você DEVE escolher Desligar sem Sysprep e nunca escolher Desligar com Sysprep. Desligar com o Sysprep fará com que todos os usuários locais se tornem inutilizáveis. Para obter mais informações, consulte [a seção Antes de começar do tópico Criar uma AMI personalizada do Guia do usuário para instâncias do Windows](#).

## Construa o AMI

Para construir o AMI

1. Abra o console do Amazon EC2.
2. Selecione Instâncias no painel de navegação e, em seguida, selecione sua instância.
3. Escolha Estado da instância e, em seguida, Parar instância.
4. Depois que a instância for interrompida, escolha Ações.
5. Escolha Imagem e modelos e, em seguida, Criar imagem.
6. Insira o nome da imagem.
7. (Opcional) Insira uma descrição para sua imagem.
8. Escolha Criar imagem.

## Crie uma infraestrutura de frota com um grupo do Amazon EC2 Auto Scaling

Esta seção explica como criar uma frota do Amazon EC2 Auto Scaling.

Use o modelo AWS CloudFormation YAML abaixo para criar um grupo do Amazon EC2 Auto Scaling (Auto Scaling), uma Amazon Virtual Private Cloud (Amazon VPC) com duas sub-redes, um perfil de instância e uma função de acesso à instância. Eles são necessários para iniciar a instância usando o Auto Scaling nas sub-redes.

Você deve revisar e atualizar a lista de tipos de instância para atender às suas necessidades de renderização.

Para criar uma frota do Amazon EC2 Auto Scaling

1. Abra o AWS CloudFormation console em <https://console.aws.amazon.com/cloudformation>.
2. Crie um CloudFormation modelo com parâmetros Farm ID, Fleet ID, AMI ID e.

```
AWSTemplateFormatVersion: 2010-09-09
Description: Amazon Deadline Cloud customer-managed fleet
Parameters:
  FarmId:
    Type: String
    Description: Farm ID
  FleetId:
```

```

    Type: String
    Description: Fleet ID
  AMIID:
    Type: String
    Description: AMI ID for launching Workers
  Resources:
    deadlineVPC:
      Type: 'AWS::EC2::VPC'
      Properties:
        CidrBlock: 100.100.0.0/16
    deadlineWorkerSecurityGroup:
      Type: 'AWS::EC2::SecurityGroup'
      Properties:
        GroupDescription: !Join
          - ' '
          - - Security Group created for deadline 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
```



```
--fleet-id FLEET_ID \  
--configuration file://configuration.json
```

- Exemplo de CreateFleet comando:

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

A seguir está um exemplo de `configuration.json` uso nos comandos da CLI acima (`--configuration file://configuration.json`).

- Para ativar o Auto Scaling em sua frota, você deve definir o modo como `EVENT_BASED_AUTO_SCALING`
- Esses `workerCapabilities` são os valores padrão atribuídos ao CMF quando você o criou. Você pode alterar esses valores se precisar aumentar os recursos disponíveis para seu CMF.

Depois de configurar o modo de frota, o Deadline Cloud começa a emitir eventos de recomendação de tamanho de frota para essa frota.

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



```
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

```

## Conecte frotas gerenciadas pelo cliente a um endpoint de licença

O servidor de licenças baseado no uso do AWS Deadline Cloud (Deadline Cloud) fornece licenças sob demanda para produtos selecionados de terceiros. Isso permite que você pague conforme o uso. Você só é alterado pelo tempo que usa.

O servidor de licenças baseado no uso do Deadline Cloud pode ser usado com qualquer tipo de frota, desde que os funcionários do Deadline Cloud possam se comunicar com o servidor de licenças. Isso é configurado automaticamente em frotas gerenciadas por serviços. Essa configuração só é necessária para frotas gerenciadas pelo cliente.

Para criar o servidor de licenças, você precisa do seguinte:

- Um grupo de segurança para a VPC da sua fazenda que permite tráfego para licenças de terceiros.
- Uma função AWS Identity and Access Management (IAM) com uma política anexada que permite acesso às operações de endpoint da licença Deadline Cloud.

## Tópicos

- [Etapa 1: criar um grupo de segurança](#)
- [Etapa 2: configurar o endpoint da licença](#)
- [Etapa 3: Conectar um aplicativo de renderização a um endpoint](#)

## Etapa 1: criar um grupo de segurança

Use o console Amazon VPC (<https://console.aws.amazon.com/vpc/>) para criar um grupo de segurança para a VPC da sua fazenda. Configure o grupo de segurança para permitir as seguintes regras de entrada:

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

A origem de cada regra de entrada é o grupo de segurança do trabalhador da frota.

Para obter mais informações sobre a criação de um grupo de segurança, consulte [Criar um grupo de segurança](#) no guia do usuário da Amazon Virtual Private Cloud.

## Etapa 2: configurar o endpoint da licença

Um endpoint de licença fornece acesso aos servidores de licenças para produtos de terceiros. As solicitações de licença são enviadas para o endpoint da licença. O endpoint os encaminha para o servidor de licenças apropriado. O servidor de licenças rastreia os limites e direitos de uso. Há uma cobrança para cada endpoint de licença que você criar. Para obter mais informações, consulte [Preços da Amazon VPC](#).



Você pode criar seu endpoint de licença a partir do AWS Command Line Interface com as permissões apropriadas. Para saber a política necessária para criar um endpoint de licença, consulte [Política para permitir a criação de um endpoint de licença](#).

Você pode usar o AWS CloudShell (<https://console.aws.amazon.com/cloudshell/>) ou qualquer outro AWS CLI ambiente para configurar o endpoint da licença usando os AWS Command Line Interface comandos a seguir.

1. Crie o endpoint da licença. Substitua o ID do grupo de segurança, o ID da sub-rede e o ID da VPC pelos valores que você criou anteriormente. Se você usar várias sub-redes, separe-as com espaços.

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

2. Confirme se o endpoint foi criado com sucesso com o comando a seguir. Lembre-se do nome DNS do VPC endpoint.

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

3. Veja uma lista dos produtos medidos disponíveis:

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

4. Adicione produtos medidos ao endpoint da licença com o comando a seguir.

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

Você pode remover um produto de um endpoint de licença com o `remove-metered-product` comando:

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

Você pode excluir um endpoint de licença com o `delete-license-endpoint` comando:

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

### Etapa 3: Conectar um aplicativo de renderização a um endpoint

Depois que o endpoint da licença é configurado, os aplicativos o usam da mesma forma que usam um servidor de licenças de terceiros. Normalmente, você configura o servidor de licenças para o aplicativo definindo uma variável de ambiente ou outra configuração do sistema, como uma chave de registro do Microsoft Windows, como uma porta e endereço do servidor de licenças.

Para obter o nome DNS do endpoint da licença, use o comando a seguir AWS CLI .

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

Ou você pode usar o Amazon VPC Console (<https://console.aws.amazon.com/vpc/>) para identificar o VPC endpoint criado pela API Deadline Cloud na etapa anterior.

#### Exemplos de configuração

##### Example — Autodesk Maya e Arnold

Defina a variável de ambiente `ADSKFLEX_LICENSE_FILE` como:

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

#### Note

Para Windows trabalhadores, use ponto e vírgula (;) em vez de dois pontos (:) para separar os pontos finais.

##### Example — Autodesk 3ds Max

Defina a variável de ambiente `ADSKFLEX_LICENSE_FILE` como:

```
2704@VPC_Endpoint_DNS_Name
```

## Example — Fundação Nuke

Defina a variável de ambiente `foundry_LICENSE` como `6101@VPC_Endpoint_DNS_Name` Para testar se o licenciamento está funcionando corretamente, você pode executar o Nuke em um terminal:

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

## Example — SideFX Houdini, Mantra e Karma

Execute o seguinte 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 testar se o licenciamento está funcionando corretamente, você pode renderizar uma cena do Houdini por meio deste comando:

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

# Gerenciando usuários no Deadline Cloud

AWS O Deadline Cloud usa AWS IAM Identity Center para gerenciar usuários e grupos. O IAM Identity Center é um serviço de login único baseado em nuvem que pode ser integrado ao seu provedor de login único (SSO) corporativo. Com a integração, os usuários podem fazer login com a conta da empresa.

O Deadline Cloud habilita o IAM Identity Center por padrão, e é necessário configurar e usar o Deadline Cloud. Para obter mais informações, consulte [Gerenciar sua fonte de identidade](#).

O proprietário da sua organização AWS Organizations é responsável por gerenciar os usuários e grupos que têm acesso ao seu monitor do Deadline Cloud. Você pode criar e gerenciar esses usuários e grupos usando o IAM Identity Center ou o console do Deadline Cloud. Para obter mais informações, consulte [O que é o AWS Organizations](#).

Você cria e remove usuários e grupos que podem usar o monitor para gerenciar fazendas, filas e frotas usando o console do Deadline Cloud. Quando você adiciona um usuário ao Deadline Cloud, ele deve redefinir a senha usando o IAM Identity Center antes de obter acesso.

## Tópicos

- [Gerencie usuários e grupos para o monitor](#)
- [Gerencie usuários e grupos para fazendas, filas e frotas](#)

## Gerencie usuários e grupos para o monitor

O proprietário de uma organização pode usar o console do Deadline Cloud para gerenciar os usuários e grupos que têm acesso ao monitor do Deadline Cloud. Você pode escolher entre usuários e grupos existentes do IAM Identity Center ou adicionar novos usuários e grupos a partir do console.

1. Faça login AWS Management Console e abra o [console](#) do Deadline Cloud. Na página principal, na seção Começar, escolha Configurar o Deadline Cloud ou Ir para o painel.
2. No painel de navegação esquerdo, escolha Gerenciamento de usuários. Por padrão, a guia Grupos é selecionada.

Dependendo da ação a ser tomada, escolha a guia Grupos ou a guia Usuários.


## Monitor groups

Para criar um grupo

1. Escolha Criar grupo.
2. Insira o nome do grupo. O nome deve ser exclusivo entre os grupos em sua organização do IAM Identity Center.

Para remover um grupo

1. Selecione o grupo a ser removido.
2. Escolha Remover.
3. Na caixa de diálogo de confirmação, escolha Remover grupo.

 Note

Você está removendo o grupo do IAM Identity Center. Os membros do grupo não podem mais entrar na Deadline Cloud nem acessar os recursos da fazenda.

## Monitor users


Como adicionar usuários

1. Escolha a guia Users.
2. Escolha Adicionar usuários.
3. Insira o nome, endereço de e-mail e nome de usuário do novo usuário.
4. Se desejar, escolha um ou mais grupos do IAM Identity Center aos quais adicionar o novo usuário.
5. Escolha Enviar convite para enviar ao novo usuário um e-mail com instruções para ingressar na sua organização do IAM Identity Center.

Para remover um usuário

1. Selecione o usuário que você deseja remover do seu monitor.
2. Escolha Remover.

3. Na caixa de diálogo de confirmação, escolha Remover usuário.

 Note

Você está removendo o usuário do IAM Identity Center. O usuário não pode mais entrar no monitor do Deadline Cloud nem acessar os recursos da fazenda.

## Gerencie usuários e grupos para fazendas, filas e frotas

1. Se ainda não o fez, faça login AWS Management Console e abra o [console](#) do Deadline Cloud.
2. No painel de navegação esquerdo, escolha Fazendas e outros recursos.
3. Selecione a fazenda a ser gerenciada. Escolha o nome da fazenda para abrir a página de detalhes. Você pode pesquisar a fazenda usando a barra de pesquisa.
4. Para gerenciar uma fila ou frota, escolha a guia Filas ou Frotas e, em seguida, escolha a fila ou frota a ser gerenciada.
5. Escolha a guia Gerenciamento de acesso. Por padrão, a guia Grupos é selecionada. Para gerenciar usuários, mova o botão para Usuários.

Dependendo da ação a ser tomada, escolha a guia Grupos ou a guia Usuários.

Para definições de nível de acesso, consulte [Permissões](#).

### Groups

Para adicionar grupos

1. Selecione a opção Grupos.
2. Escolha Add Group (Adicionar grupo).
3. No menu suspenso, selecione os grupos a serem adicionados.
4. Para o nível de acesso do grupo, escolha uma das seguintes opções:
  - Visualizador
  - Contributor (Colaborador)
  - Gerente
  - Proprietário

## 5. Escolha Adicionar.

### Para remover grupos

1. Selecione os grupos a serem removidos.
2. Escolha Remover.
3. No diálogo de confirmação, escolha Remove.

## Users

### Como adicionar usuários

1. Para adicionar um usuário, escolha Adicionar usuário.
2. No menu suspenso, selecione os usuários a serem adicionados à sua fazenda.
3. Para o nível de acesso do usuário, escolha uma das seguintes opções:
  - Visualizador
  - Contributor (Colaborador)
  - Gerente
  - Proprietário
4. Escolha Adicionar. Os usuários são adicionados à sua fazenda.

### Para remover um usuário

1. Selecione o usuário a ser removido.
2. Na caixa de diálogo de confirmação Remover, escolha Remover. Em seguida, o usuário é removido da fazenda selecionada.

Você também pode adicionar ou remover permissões de farm para usuários e grupos usando o console do IAM Identity Center em <https://console.aws.amazon.com/singlesignon/>.

# Trabalhos do Deadline Cloud

Um trabalho é um conjunto de instruções que o AWS Deadline Cloud usa para agendar e executar trabalhos com os trabalhadores disponíveis. Ao criar um trabalho, você escolhe a fazenda e a fila para onde enviar o trabalho. Você também fornece um arquivo JSON ou YAML que fornece as instruções para os trabalhadores processarem. O Deadline Cloud aceita modelos de trabalho que seguem a especificação Open Job Description (OpenJD) para descrever trabalhos. Para obter mais informações, consulte a [documentação do Open Job Description](#) no GitHub site.

Um trabalho consiste em:

- **Etapas** — Define o script a ser executado nos trabalhadores. As etapas podem ter requisitos como memória mínima de trabalho ou outras etapas que precisam ser concluídas primeiro. Cada etapa tem uma ou mais tarefas.
- **Tarefas** — Uma unidade de trabalho enviada a um trabalhador para ser executada. Uma tarefa é uma combinação do script e dos parâmetros de uma etapa, como o número do quadro, que são usados no script. O trabalho estará concluído quando todas as tarefas estiverem concluídas em todas as etapas.
- **Ambientes** — Configure e elimine instruções compartilhadas por várias etapas ou tarefas.

Você pode criar um trabalho de qualquer uma das seguintes formas:

- Use um remetente do Deadline Cloud.
- Crie um pacote de tarefas e use a [interface de linha de comando do Deadline Cloud](#) (CLI do Deadline Cloud).
- Use o AWS SDK.
- Use o AWS Command Line Interface (AWS CLI).

Um remetente é um plug-in para seu software de criação de conteúdo digital (DCC) que gerencia a criação de um trabalho na interface do seu software DCC. Depois de criar o trabalho, você usa o remetente para enviá-lo ao Deadline Cloud para processamento. Nos bastidores, o remetente cria um modelo de trabalho do OpenJD que descreve o trabalho. Ao mesmo tempo, ele carrega seus arquivos de ativos em um bucket do Amazon Simple Storage Service (Amazon S3). Para reduzir o tempo necessário para enviar arquivos, somente os arquivos que foram alterados desde a última vez em que você enviou arquivos são enviados para o Amazon S3.



Para criar seus próprios scripts e pipelines para enviar trabalhos para o Deadline Cloud, você pode usar a CLI do Deadline Cloud, AWS o SDK ou AWS CLI o to call operações para criar, obter, visualizar e listar trabalhos. Os tópicos a seguir explicam como usar a CLI do Deadline Cloud.

A CLI do Deadline Cloud é instalada junto com o remetente do Deadline Cloud. Para ter mais informações, consulte [Configurar remetentes do Deadline Cloud](#).

## Tópicos

- [Envio de trabalhos com a CLI do Deadline Cloud](#)
- [Agendamento de trabalhos no Deadline Cloud](#)
- [Estados de trabalho na CLI do Deadline Cloud](#)
- [Modificando trabalhos no Deadline Cloud](#)
- [Como o Deadline Cloud processa trabalhos](#)
- [Solução de problemas de trabalhos do Deadline](#)

## Envio de trabalhos com a CLI do Deadline Cloud

Para enviar um trabalho usando a interface de linha de comando do Deadline Cloud (CLI do Deadline Cloud), use o `deadline bundle submit` comando.

Os trabalhos são enviados às filas. Se você ainda não configurou uma fazenda e uma fila, use o console do Deadline Cloud (<https://console.aws.amazon.com/https://console.aws.amazon.com/deadlinecloud/home>) para configurar uma fazenda e uma fila e ver o ID da fazenda e da fila. Para obter mais informações, consulte [Definir detalhes da fazenda](#) e [Definir detalhes da fila](#).

Para definir a fazenda e a fila padrão para a CLI do Deadline Cloud, use o comando a seguir. Ao definir os padrões, você pode usar os comandos da CLI do Deadline Cloud sem especificar uma fazenda ou fila. No exemplo a seguir, substitua *farmId* e *queueId* por suas próprias informações:

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

Para especificar as etapas e tarefas em um trabalho, crie um modelo de trabalho do OpenJD. Para obter mais informações, consulte [Template Schemas \[Versão: 2023-09\]](#) no repositório de especificações do Open Job Description. GitHub

O exemplo a seguir é um modelo de trabalho YAML. Ele define um trabalho com duas etapas e cinco tarefas por etapa.

```
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 criar um trabalho, crie uma nova pasta chamada `sample_job` e salve o arquivo de modelo na nova pasta como `template.yaml`. Você envia o trabalho com o seguinte comando da CLI do Deadline Cloud:

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

A resposta do comando contém um identificador para o trabalho. Lembre-se do ID para que você possa verificar o status do trabalho posteriormente.

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

`jobId`

Há opções adicionais que você pode usar ao enviar um trabalho. Para ter mais informações, consulte [Mais opções para enviar trabalhos com a CLI do Deadline Cloud](#).

## Mais opções para enviar trabalhos com a CLI do Deadline Cloud

O comando da CLI do `deadline bundle submit` Deadline Cloud fornece opções que você pode usar para especificar informações adicionais para um trabalho. Os exemplos a seguir mostram como:

- Especifique os parâmetros usados ao processar o modelo de trabalho.
- Anexe arquivos e pastas em um ambiente compartilhado a um trabalho.
- Defina o número máximo de falhas de tarefas antes que um trabalho seja cancelado.
- Defina o número máximo de novas tentativas para uma tarefa.

### Parâmetros de trabalho

A `parameters` opção define o valor de um parâmetro de trabalho quando você cria o trabalho. O modelo de trabalho define o campo e a `parameters` opção define o valor. Um parâmetro pode ter um valor padrão. Se um valor for especificado para o parâmetro, o valor especificado substituirá o valor padrão.

O modelo de trabalho a seguir define o `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
```

O comando a seguir define o valor do `TestParameter` para “Hello AWS”:

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

## Perfis de armazenamento

Os perfis de armazenamento ajudam no compartilhamento de arquivos entre trabalhadores com sistemas operacionais diferentes. Crie um perfil de armazenamento usando o console do Deadline Cloud. Em seguida, use o `storage-profile-id` parâmetro para usar o perfil de armazenamento. Para ter mais informações, consulte [Armazenamento compartilhado no Deadline Cloud](#).

Para definir o perfil de armazenamento para envios de trabalhos, usando a CLI do Deadline Cloud, use o comando a seguir para definir `storage-profile-id` o parâmetro de configuração:

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

## Máximo de tarefas com falha

A `max-failed-tasks-count` opção define o número máximo de tarefas que podem falhar antes que todo o trabalho falhe e todas as tarefas restantes sejam marcadas `CANCELED`. O valor padrão é 100.

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

## Máximo de tentativas de tarefas com falha

A `max-retries-per-task` opção define o número máximo de vezes que uma tarefa é repetida antes de falhar. Quando uma tarefa é repetida, ela é colocada no `READY` estado. O valor padrão é 5.

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

# Agendamento de trabalhos no Deadline Cloud

Depois que um trabalho é criado, AWS o Deadline Cloud o programa para ser processado em uma ou mais frotas associadas a uma fila. A frota que processa uma tarefa específica é escolhida com base nos recursos configurados para a frota e nos requisitos do host de uma etapa específica.

Os trabalhos são programados em uma ordem de prioridade de melhor esforço, da maior para a menor. Quando dois trabalhos têm a mesma prioridade, o trabalho mais antigo é agendado primeiro.

As seções a seguir fornecem detalhes do processo de agendamento de um trabalho.

## Determine a compatibilidade da frota

Depois que um trabalho é criado, o Deadline Cloud verifica os requisitos do host para cada etapa do trabalho em relação às capacidades das frotas associadas à fila para a qual o trabalho foi enviado. Se uma frota atender aos requisitos do anfitrião, o trabalho será colocado no READY estado.

Se alguma etapa do trabalho tiver requisitos que não possam ser atendidos por uma frota associada à fila, o status da etapa será definido como `NOT_COMPATIBLE`. Além disso, as demais etapas do trabalho são canceladas.

As capacidades de uma frota são definidas no nível da frota. Mesmo que um trabalhador em uma frota atenda aos requisitos do trabalho, ele não receberá tarefas do trabalho se sua frota não atender aos requisitos do trabalho.

O modelo de tarefa a seguir tem uma etapa que especifica os requisitos de host para a etapa:

```
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
```

Esse trabalho pode ser programado para uma frota com os seguintes recursos:

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

Esse trabalho não pode ser programado para uma frota com nenhum dos seguintes recursos:

```
{
  "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.
```

## Dimensionamento da frota

Quando um trabalho é atribuído a uma frota gerenciada de serviços compatível, a frota é escalada automaticamente. O número de trabalhadores na frota varia com base no número de tarefas disponíveis para a frota executar.

Quando um trabalho é atribuído a uma frota gerenciada pelo cliente, os trabalhadores podem já existir ou podem ser criados usando o escalonamento automático baseado em eventos. Para obter mais informações, consulte [Use EventBridge para lidar com eventos de auto scaling no Guia](#) do usuário do Amazon EC2 Auto Scaling.

## Sessões

As tarefas em um trabalho são divididas em uma ou mais sessões. Os trabalhadores executam as sessões para configurar o ambiente, executar as tarefas e, em seguida, destruir o ambiente. Cada sessão é composta por uma ou mais ações que um trabalhador deve realizar.

Quando um trabalhador conclui as ações da seção, ações adicionais da sessão podem ser enviadas ao trabalhador. O funcionário reutiliza os ambientes e os anexos de trabalho existentes na sessão para concluir as tarefas com mais eficiência.

Os anexos de trabalho são criados pelo remetente que você usa, como parte do pacote de trabalhos da CLI do Deadline Cloud. Você também pode criar anexos de trabalho usando a `--attachments` opção do comando `create-job` AWS CLI. Os ambientes são definidos em dois lugares: ambientes de fila anexados a uma fila específica e ambientes de etapas de trabalho definidos no modelo de trabalho.

Há quatro tipos de ação de sessão:

- `syncInputJobAttachments`— Faz o download dos anexos do trabalho de entrada para o trabalhador.
- `envEnter`— Executa as `onEnter` ações para um ambiente.
- `taskRun`— Executa as `onRun` ações de uma tarefa.
- `envExit`— Executa as `onExit` ações para um ambiente.

O modelo de trabalho a seguir tem um ambiente de etapas. Ele tem uma `onEnter` definição para configurar o ambiente de etapas, uma `onRun` definição que define a tarefa a ser executada e uma `onExit` definição para derrubar o ambiente de etapas. As sessões criadas para esse trabalho incluirão uma `envEnter` ação, uma ou mais `taskRun` ações e, em seguida, uma `envExit` ação.

```
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 }}
```

## Dependências de etapas

O Deadline Cloud suporta a definição de dependências entre as etapas para que uma etapa espere até que outra seja concluída antes de começar. Você pode definir mais de uma dependência para uma etapa. Uma etapa com uma dependência não é agendada até que todas as dependências estejam concluídas.

Se o modelo de trabalho definir uma dependência circular, o trabalho será rejeitado e o status do trabalho será definido como `CREATE_FAILED`.

O modelo de trabalho a seguir cria um trabalho com duas etapas. StepB depende de StepA. StepB só é executado após StepA ser concluído com sucesso.

Depois que o trabalho é criado, StepA está no `READY` estado e StepB está no `PENDING` estado. Depois de StepA terminar, StepB se muda para o `READY` estado. Se StepA falhar ou StepA for cancelado, StepB passa para o `CANCELED` estado.

Você pode definir uma dependência em várias etapas. Por exemplo, StepC depende de ambos StepA e StepB, StepC não começará até que as outras duas etapas terminem.

```
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 trabalho na CLI do Deadline Cloud

Este tópico descreve como usar a interface de linha de comando do AWS Deadline Cloud (CLI do Deadline Cloud) para visualizar o status de um trabalho ou etapa. Se você quiser usar o monitor do Deadline Cloud para ver o status dos trabalhos ou etapas, consulte [Visualize e gerencie trabalhos, etapas e tarefas no Deadline Cloud](#).

Você pode ver o status de um trabalho usando o comando da CLI do `deadline job get --job-id` Deadline Cloud. A resposta aos comandos inclui o status do trabalho ou etapa e o número de tarefas em cada status de processamento.

Quando você envia um trabalho pela primeira vez, o status é `CREATE_IN_PROGRESS`. Se o trabalho passar nas verificações de validação, seu status mudará para `CREATE_COMPLETE`. Caso contrário, o status muda para `CREATE_FAILED`.

Alguns motivos possíveis pelos quais um trabalho pode falhar nas verificações de validação incluem o seguinte:

- O modelo de trabalho não segue a especificação do OpenJD.
- O trabalho contém muitas etapas.
- O trabalho contém muitas tarefas totais.

Para ver as cotas para o número máximo de etapas e tarefas em um trabalho, use o console Service Quotas. Para ter mais informações, consulte [Cotas para Deadline Cloud](#).

Também pode haver um erro de serviço interno que impeça a criação de um trabalho. Se isso acontecer, o código de status do trabalho será `INTERNAL_ERROR` e o campo da mensagem de status fornecerá uma explicação mais detalhada.

Use o seguinte comando da CLI do Deadline Cloud para ver os detalhes de um trabalho. No exemplo a seguir, *jobID* substitua por suas próprias informações:

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

A resposta do `deadline job get` comando é a seguinte:

```
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 tarefa em um trabalho ou etapa tem um status. Os status das tarefas são combinados para fornecer um status geral para trabalhos e etapas. O número de tarefas em cada estado é relatado no `taskRunStatusCounts` campo da resposta.

O status de um trabalho ou etapa depende do status de suas tarefas. O status é determinado pelas tarefas que têm esses status, em ordem. Os status das etapas são determinados da mesma forma que o status do trabalho.

A lista a seguir descreve os status:

#### NOT\_COMPATIBLE

O trabalho não é compatível com a fazenda porque não há frotas que possam concluir uma das tarefas do trabalho.

#### RUNNING

Um ou mais trabalhadores estão executando tarefas a partir do trabalho. Desde que haja pelo menos uma tarefa em execução, o trabalho é marcado `RUNNING`.

#### ASSIGNED

Um ou mais trabalhadores recebem tarefas no trabalho como sua próxima ação. O ambiente, se houver, está configurado.

#### STARTING

Um ou mais trabalhadores estão configurando o ambiente para executar tarefas.

#### SCHEDULED

As tarefas do trabalho são agendadas para um ou mais trabalhadores como a próxima ação do trabalhador.

#### READY

Pelo menos uma tarefa do trabalho está pronta para ser processada.

## INTERRUPTING

Pelo menos uma tarefa no trabalho está sendo interrompida. Interrupções podem ocorrer quando você atualiza manualmente o status do trabalho. Isso também pode acontecer em resposta a uma interrupção devido às mudanças de preço spot do Amazon Elastic Compute Cloud (Amazon EC2).

## FAILED

Uma ou mais tarefas no trabalho não foram concluídas com êxito.

## CANCELED

Uma ou mais tarefas no trabalho foram canceladas.

## SUSPENDED

Pelo menos uma tarefa no trabalho foi suspensa.

## PENDING

Uma tarefa no trabalho está aguardando a disponibilidade de outro recurso.

## SUCCEEDED

Todas as tarefas do trabalho foram processadas com sucesso.

## Modificando trabalhos no Deadline Cloud

Você pode usar os seguintes `update` comandos AWS Command Line Interface (AWS CLI) para modificar a configuração de um trabalho ou definir o status de destino de um trabalho, etapa ou tarefa:

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

Nos exemplos de `update` comandos a seguir, substitua cada um *user input placeholder* por suas próprias informações.

Você também pode usar o monitor do Deadline Cloud para modificar a configuração de um trabalho. Para ter mais informações, consulte [Visualize e gerencie trabalhos, etapas e tarefas no Deadline Cloud](#).

### Example — Solicitar um trabalho

Todas as tarefas na tarefa mudam para o READY status, a menos que haja dependências de etapas. As etapas com dependências mudam para uma READY ou à PENDING medida que são restauradas.

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

### Example — Cancelar um trabalho

Todas as tarefas no trabalho que não têm o status SUCCEEDED ou FAILED estão marcadas CANCELED.

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

### Example — Marcar que um trabalho falhou

Todas as tarefas no trabalho que têm o status permanecem SUCCEEDED inalteradas. Todas as outras tarefas estão marcadas FAILED.

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

### Example — Marque um trabalho bem-sucedido

Todas as tarefas do trabalho são transferidas para o SUCCEEDED estado.

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

### Example — Suspende um emprego

As tarefas no trabalho no FAILED estado SUCCEEDDCANCELED, ou não mudam. Todas as outras tarefas estão marcadas SUSPENDED.

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

### Example — Mudar a prioridade de um trabalho

Atualiza a prioridade de um trabalho para alterar a ordem em que ele está agendado. Os trabalhos de maior prioridade geralmente são agendados primeiro.

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

### Example — Alterar o número de tarefas com falha permitidas

Atualiza o número máximo de tarefas com falha que o trabalho pode ter antes que as tarefas restantes sejam canceladas.

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

### Example — Alterar o número de novas tentativas de tarefas permitidas

Atualiza o número máximo de tentativas de uma tarefa antes que a tarefa falhe. Uma tarefa que tenha atingido o número máximo de novas tentativas não pode ser colocada novamente na fila até que esse valor seja aumentado.

```
aws deadline update-job \  
--farm-id farmID \  
--queue-id queueID \  
--max-attempts 200
```

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

### Example — Arquivar um trabalho

Atualiza o status do ciclo de vida do trabalho para. ARCHIVED Os trabalhos arquivados não podem ser agendados nem modificados. Você só pode arquivar um trabalho que esteja no SUSPENDED estado FAILED,CANCELED,SUCCEEDED,, ou.

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

### Example — Recoloque uma etapa na fila

Todas as tarefas na etapa mudam para o READY estado, a menos que haja dependências de etapas. As tarefas em etapas com dependências mudam para READY ouPENDING, e a tarefa é restaurada.

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

### Example — Cancelar uma etapa

Todas as tarefas na etapa que não têm o status SUCCEEDED ou FAILED estão marcadasCANCELED.

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

### Example — Marcar uma etapa que falhou

Todas as tarefas na etapa que têm o status permanecem SUCCEEDED inalteradas. Todas as outras tarefas estão marcadasFAILED.



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

### Example — Marque uma etapa bem-sucedida

Todas as tarefas na etapa estão marcadas SUCCEEDED.

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

### Example — Suspende uma etapa

As tarefas na etapa do FAILED estado SUCCEEDED CANCELED,, ou não mudam. Todas as outras tarefas estão marcadas SUSPENDED.

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

### Example — Alterar o status de uma tarefa

Quando você usa o comando da CLI do update-task Deadline Cloud, a tarefa muda para o status especificado.

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

```
--task-id taskID \  
--target-task-run-status SUCCEEDED | SUSPENDED | CANCELED | FAILED | PENDING
```

## Como o Deadline Cloud processa trabalhos

Para processar um trabalho, o AWS Deadline Cloud usa o modelo de trabalho Open Job Description (OpenJD) para determinar os recursos necessários. O Deadline Cloud seleciona um trabalhador adequado para uma etapa das frotas associadas à sua fila. O trabalhador selecionado atende a todos os atributos de capacidade necessários para a etapa.

Em seguida, o Deadline Cloud envia instruções aos trabalhadores para configurar uma sessão para a etapa. O software necessário para a etapa deve estar disponível na instância do trabalhador para que o trabalho seja executado. O serviço pode abrir sessões com vários trabalhadores se as configurações de escalonamento da frota tiverem capacidade.

Você pode configurar o software em um Amazon Machine Image (AMI) ou seu funcionário pode carregar o software em tempo de execução a partir de um repositório ou gerenciador de pacotes. Você pode usar ambientes de fila, trabalho ou etapa para implantar o software de sua preferência.

O serviço Deadline Cloud usa o modelo OpenJD para determinar as etapas necessárias para o trabalho e as tarefas necessárias para cada etapa. Algumas etapas dependem de outras etapas, então o Deadline Cloud determina a ordem para concluir as etapas. Em seguida, o Deadline Cloud envia as tarefas de cada etapa para os trabalhadores processarem. Quando uma tarefa é concluída, o serviço envia outra tarefa na mesma sessão, ou o trabalhador pode iniciar uma nova sessão.

Você pode acompanhar o progresso do trabalho no monitor do Deadline Cloud, na interface de linha de comando do Deadline Cloud (CLI do Deadline Cloud) ou no AWS CLI. Para obter mais informações sobre como usar o monitor, consulte [Usando o monitor Deadline Cloud](#). Para obter mais informações sobre como usar a CLI do Deadline Cloud, consulte [Estados de trabalho na CLI do Deadline Cloud](#).

Depois que todas as tarefas em cada etapa forem concluídas, o trabalho estará concluído e a saída estará pronta para ser baixada na sua estação de trabalho. Mesmo que o trabalho não tenha sido concluído, a saída de cada etapa e tarefa concluída estará disponível para download.

O Deadline Cloud remove os trabalhos 120 dias após o envio. Quando um trabalho é removido, todas as etapas e tarefas associadas ao trabalho também são removidas. Se você precisar executar novamente o trabalho, envie o modelo do OpenJD para o trabalho novamente.

# Solução de problemas de trabalhos do Deadline

Para obter informações sobre problemas comuns com trabalhos no AWS Deadline Cloud, consulte os tópicos a seguir.

## Tópicos

- [Por que a criação do meu emprego falhou?](#)
- [Por que meu trabalho não é compatível?](#)
- [Por que meu trabalho está pronto?](#)
- [Por que meu trabalho falhou?](#)
- [Por que minha etapa está pendente?](#)

## Por que a criação do meu emprego falhou?

Alguns motivos possíveis pelos quais um trabalho pode falhar nas verificações de validação incluem o seguinte:

- O modelo de trabalho não segue a especificação do OpenJD.
- O trabalho contém muitas etapas.
- O trabalho contém muitas tarefas totais.
- Houve um erro de serviço interno que impede a criação do trabalho.

Para ver as cotas para o número máximo de etapas e tarefas em um trabalho, use o console Service Quotas. Para ter mais informações, consulte [Cotas para Deadline Cloud](#).

## Por que meu trabalho não é compatível?

Os motivos comuns pelos quais os trabalhos não são compatíveis com filas incluem o seguinte:

- Nenhuma frota está associada à fila para a qual o trabalho foi enviado. Abra o monitor do Deadline Cloud e verifique se a fila tem frotas associadas. Para obter mais informações sobre como visualizar filas, consulte [Veja detalhes da fila e da frota no Deadline Cloud](#).
- O trabalho tem requisitos de host que não são satisfeitos por nenhuma das frotas associadas à fila. Para verificar, compare a `hostRequirements` entrada no modelo de trabalho com a configuração das frotas em sua fazenda. Certifique-se de que uma das frotas atenda aos requisitos do anfitrião.

Para obter mais informações sobre compatibilidade de frotas, consulte [Determine a compatibilidade da frota](#). Para ver a configuração da frota, consulte [Veja detalhes da fila e da frota no Deadline Cloud](#).

## Por que meu trabalho está pronto?

Os possíveis motivos para que seu emprego pareça estar preso no READY estado incluem o seguinte:

- A contagem máxima de trabalhadores para frotas associadas à fila é definida como zero. Para verificar, consulte [Veja detalhes da fila e da frota no Deadline Cloud](#).
- Há um trabalho de maior prioridade na fila. Para verificar, consulte [Veja detalhes da fila e da frota no Deadline Cloud](#).
- Para frotas gerenciadas pelo cliente, verifique a configuração do auto scaling. Para ter mais informações, consulte [Escale automaticamente sua frota do Amazon EC2 com o recurso de recomendação de escala Deadline Cloud](#).

## Por que meu trabalho falhou?

Um trabalho pode falhar por vários motivos. Para pesquisar o problema, abra o monitor do Deadline Cloud e escolha o trabalho com falha. Escolha uma tarefa que falhou e, em seguida, visualize os registros da tarefa. Para obter instruções, consulte [Exibir registros no Deadline Cloud](#).

- Se você ver erros de licença ou receber uma marca d'água que ocorre porque o software não tem uma licença válida, certifique-se de que o funcionário possa se conectar ao servidor de licenças necessário. Para ter mais informações, consulte [Conecte frotas gerenciadas pelo cliente a um endpoint de licença](#).

## Por que minha etapa está pendente?

As etapas podem permanecer no PENDING estado quando uma ou mais de suas dependências não estiverem concluídas. Você pode verificar o estado das dependências usando o monitor Deadline Cloud. Para obter instruções, consulte [Veja uma etapa no Deadline Cloud](#).

# Armazenamento de arquivos para Deadline Cloud

Os trabalhadores devem ter acesso aos locais de armazenamento que contêm os arquivos de entrada necessários para processar um trabalho e aos locais que armazenam a saída. AWS O Deadline Cloud oferece duas opções para locais de armazenamento:

- Com os anexos de trabalho, o Deadline Cloud transfere os arquivos de entrada e saída de seus trabalhos entre uma estação de trabalho e os funcionários do Deadline Cloud. Para permitir as transferências de arquivos, o Deadline Cloud usa um bucket do Amazon Simple Storage Service (Amazon S3) em seu. Conta da AWS

Ao usar anexos de trabalho com uma frota gerenciada por serviços, você pode configurar um sistema de arquivos virtual (VFS) na sua rede privada virtual (VPN). Então, os trabalhadores podem carregar arquivos somente quando necessário.

- Com o armazenamento compartilhado, você usa o compartilhamento de arquivos com seu sistema operacional para fornecer acesso aos arquivos.

Ao usar armazenamento compartilhado multiplataforma, você pode criar um perfil de armazenamento para que os trabalhadores possam mapear o caminho para os arquivos entre dois sistemas operacionais diferentes.

## Tópicos

- [Anexos de trabalho no Deadline Cloud](#)
- [Armazenamento compartilhado no Deadline Cloud](#)

## Anexos de trabalho no Deadline Cloud

Os anexos de trabalho permitem que você transfira arquivos entre sua estação de trabalho e o Deadline Cloud. AWS Com os anexos de trabalho, você não precisa configurar manualmente um bucket do Amazon S3 para seus arquivos. Em vez disso, ao criar uma fila com o console do Deadline Cloud, você escolhe o bucket para seus anexos de trabalho.

Na primeira vez que você envia um trabalho para o Deadline Cloud, todos os arquivos do trabalho são transferidos para o Deadline Cloud. Para envios subsequentes, somente os arquivos que foram alterados são transferidos, economizando tempo e largura de banda.

Depois que o processamento estiver concluído, você poderá baixar o resultado na página de detalhes do trabalho ou usando o comando CLI `deadline job download-output` do Deadline Cloud.

Você pode usar o mesmo bucket do S3 para várias filas. Defina um prefixo raiz diferente para cada fila para organizar os anexos no bucket.

Ao criar uma fila com o console, você pode escolher uma função existente AWS Identity and Access Management (IAM) ou fazer com que o console crie uma nova função. Se o console criar a função, ele definirá permissões para acessar o bucket especificado para a fila. Se você escolher uma função existente, deverá conceder permissões à função para acessar o bucket do S3.

## Criptografia para buckets S3 de anexo de tarefas

Por padrão, os arquivos anexos do Job são criptografados automaticamente em seu bucket do S3. Essa abordagem ajuda a proteger suas informações contra acesso não autorizado. Você não precisa fazer nada para que seus arquivos sejam criptografados com as chaves fornecidas pelo Deadline Cloud. Para obter mais informações, consulte [O Amazon S3 agora criptografa automaticamente todos os novos objetos](#) no Guia do usuário do Amazon S3.

Você pode usar sua própria AWS Key Management Service chave gerenciada pelo cliente para criptografar o bucket do S3 que contém seus anexos de trabalho. Para fazer isso, você deve modificar a função do IAM da fila associada ao bucket para permitir o acesso ao AWS KMS key.

Para abrir o editor de políticas do IAM para a função de fila

1. Faça login AWS Management Console e abra o [console](#) do Deadline Cloud. Na página principal, na seção Começar, escolha Exibir fazendas.
2. Na lista de fazendas, escolha a fazenda que contém a fila a ser modificada.
3. Na lista de filas, escolha a fila a ser modificada.
4. Na seção Detalhes da fila, escolha a função de serviço para abrir o console do IAM para a função de serviço.

Em seguida, conclua o procedimento a seguir.

Para atualizar a política de funções com permissão para AWS KMS

1. Na lista de políticas de permissões, escolha a política para a função.

2. Na seção Permissões definidas nesta política, escolha Editar.
3. Escolha Adicionar nova instrução.
4. Copie e cole a política a seguir no editor. Mude o *Region* *accountID*, e *keyID* para seus próprios valores.

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

5. Escolha Próximo.
6. Revise as alterações na política e, quando estiver satisfeito, escolha Salvar alterações.

## Gerenciando anexos de tarefas em buckets do S3

O Deadline Cloud armazena os arquivos anexos do trabalho necessários para seu trabalho em um bucket do S3. Esses arquivos se acumulam com o tempo, levando ao aumento dos custos do Amazon S3. Para reduzir custos, você pode aplicar uma configuração de ciclo de vida do S3 ao seu bucket do S3. Essa configuração pode excluir automaticamente os arquivos no bucket. Como o bucket do S3 está na sua conta, você pode optar por modificar ou remover a configuração do ciclo de vida do S3 a qualquer momento. Para obter mais informações, consulte [Exemplos de configuração do ciclo de vida do S3](#) no Guia do usuário do Amazon S3.

Para uma solução mais granular de gerenciamento de buckets do S3, você pode configurar seus objetos Conta da AWS para expirar em um bucket do S3 com base na última vez em que eles foram acessados. Para obter mais informações, consulte [Expiração de objetos do Amazon S3 com base na data do último acesso para reduzir](#) custos AWS no blog de arquitetura.

## Sistema de arquivos virtual Deadline Cloud

O suporte do sistema de arquivos virtual para anexos de tarefas no AWS Deadline Cloud permite que o software cliente dos funcionários se comunique diretamente com o Amazon Simple Storage

Service. Os trabalhadores podem carregar arquivos somente quando necessário, em vez de baixar todos os arquivos antes do processamento. Os arquivos são armazenados localmente. Essa abordagem evita o download de ativos usados mais de uma vez várias vezes. Todos os arquivos são removidos após a conclusão do trabalho.

- O sistema de arquivos virtual fornece um aumento significativo no desempenho para perfis de trabalho específicos. Em geral, subconjuntos menores do total de arquivos com frotas maiores de trabalhadores mostram os maiores benefícios. Pequenos números de arquivos com menos trabalhadores têm tempos de processamento aproximadamente equivalentes.
- O suporte ao sistema de arquivos virtual está disponível somente para Linux trabalhadores em frotas gerenciadas por serviços.
- O sistema de arquivos virtual Deadline Cloud suporta as seguintes operações, mas não é compatível com POSIX:
  - Arquivocreate,delete,open,close,read,write,,append,truncate,rename,move,copy,stat,fsy e falloc
  - Diretório createdelete,rename,move,,copy, e stat
- O sistema de arquivos virtual foi projetado para reduzir a transferência de dados e melhorar o desempenho quando suas tarefas acessam somente parte de um grande conjunto de dados e não é otimizado para todas as cargas de trabalho. Você deve testar sua carga de trabalho antes de executar trabalhos de produção.

## Ativar suporte ao VFS

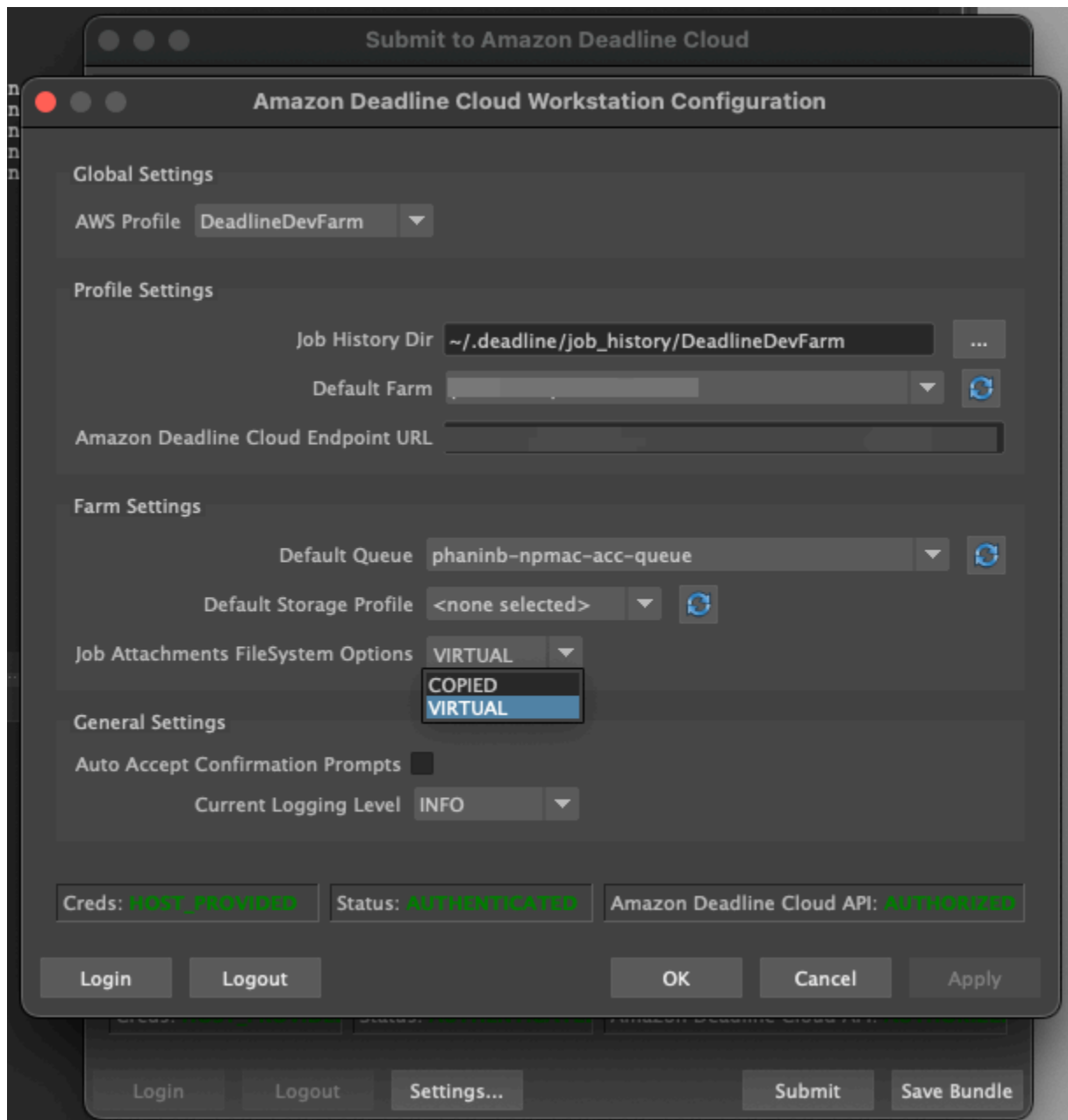
O suporte ao sistema de arquivos virtual (VFS) está habilitado para cada trabalho. Uma tarefa retorna à estrutura padrão de anexos de tarefas nos seguintes casos:

- Um perfil de instância de trabalho não oferece suporte a um sistema de arquivos virtual.
- Problemas impedem o lançamento do processo do sistema de arquivos virtual.
- O sistema de arquivos virtual não pode ser montado.

Para habilitar o suporte ao sistema de arquivos virtual usando o remetente

1. Ao enviar um trabalho, escolha o botão Configurações para abrir o painel de configuração da estação de trabalho AWS Deadline Cloud.
2. No menu suspenso de opções do sistema de arquivos Job attachments, escolha VIRTUAL.





3. Para salvar suas alterações, escolha OK.

Para habilitar o suporte ao sistema de arquivos virtual usando o AWS CLI

- Use o comando a seguir ao enviar um trabalho salvo:

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

Para verificar se o sistema de arquivos virtual foi lançado com sucesso para um trabalho específico, revise seus registros no Amazon CloudWatch Logs. Procure as seguintes mensagens:

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

Se o registro contiver a seguinte mensagem, o suporte ao sistema de arquivos virtual será desativado:

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

## Solução de problemas de suporte ao sistema de arquivos virtual

Você pode visualizar os registros do seu sistema de arquivos virtual usando o monitor Deadline Cloud. Para obter instruções, consulte [Exibir registros no Deadline Cloud](#).

Os registros do sistema de arquivos virtual também são enviados para o grupo CloudWatch Logs associado à fila compartilhada com a saída do agente de trabalho.

## Armazenamento compartilhado no Deadline Cloud

Para usar o armazenamento compartilhado, os trabalhadores usam o sistema de compartilhamento de arquivos do sistema operacional para acessar um espaço de armazenamento compartilhado para a entrada e saída de seus trabalhos.

O método real que você usa para compartilhar arquivos depende do seu sistema operacional e da forma como você implementa o armazenamento compartilhado na sua rede. Você é responsável por configurar o compartilhamento de arquivos e garantir que ele atenda às suas necessidades.

Se você estiver usando uma solução de compartilhamento de arquivos entre sistemas, poderá usar perfis de armazenamento para mapear localizações de arquivos entre Linux e sistemas de Windows arquivos.

## Perfis de armazenamento no Deadline Cloud

Um perfil de armazenamento permite que você configure fazendas usando armazenamento compartilhado multiplataforma. Um perfil de armazenamento mapeia caminhos entre sistemas operacionais para trabalhos processados em trabalhadores com um sistema operacional diferente da estação de trabalho da qual foram enviados.

Os perfis de armazenamento são necessários quando você usa uma frota gerenciada pelo cliente com uma mistura de sistemas operacionais entre estações de trabalho e trabalhadores. Os perfis de armazenamento não são compatíveis com frotas gerenciadas por serviços.

Depois de criar um perfil de armazenamento, você deve conceder acesso às filas e frotas que usam o perfil.

Para criar um perfil de armazenamento

1. Abra o [console do Deadline Cloud](#).
2. Em Começar, escolha Ir para o painel do Deadline Cloud.
3. Escolha uma fazenda e, em seguida, escolha a guia Perfis de armazenamento.
4. Escolha Criar perfil de armazenamento.
5. Escolha um sistema operacional no menu suspenso.
6. Forneça um nome para o perfil. Um nome claro ajuda você a escolher o perfil de armazenamento a ser usado ao enviar trabalhos.
7. Para o nome do caminho, insira a localização raiz dos dados do trabalho na estação de trabalho da qual você envia trabalhos.
8. Escolha um tipo de armazenamento:
  - Local se refere aos locais dos arquivos que não são compartilhados entre o trabalhador e a estação de trabalho. Eles são enviados como anexos de trabalho.
  - Compartilhado se refere ao armazenamento compartilhado entre o trabalhador e a estação de trabalho. Os arquivos no armazenamento compartilhado não são enviados como anexos do trabalho.
9. Forneça um caminho de localização do sistema de arquivos. Esse é o diretório raiz dos dados do seu trabalho.
10. Escolha Criar.

Depois de criar um perfil de armazenamento, você deve modificar suas filas e frotas gerenciadas pelo cliente para usar o novo perfil. Para permitir o acesso a um perfil de armazenamento, use o procedimento a seguir depois de concluir o procedimento anterior.

Para permitir que filas e frotas gerenciadas pelo cliente usem um perfil de armazenamento

1. Escolha a guia Filas ou Frotas.

2. Escolha a fila ou a frota a ser modificada.
3. Escolha Modificar perfis de armazenamento.
4. Selecione o perfil de armazenamento a ser permitido e os locais do sistema de arquivos desse perfil.
5. Escolha Salvar alterações.

# Gerenciamento de orçamentos e uso do Deadline Cloud

O gerenciador de orçamento e o explorador de uso do AWS Deadline Cloud são ferramentas de gerenciamento de custos que fornecem o custo aproximado do uso do Deadline Cloud com base nas informações disponíveis sobre variáveis de custo. As ferramentas de gerenciamento de custos não garantem o valor devido pelo uso real do Deadline Cloud e de outros AWS serviços.

Para ajudar você a gerenciar os custos do Deadline Cloud, você pode usar os seguintes recursos:

- Gerente de orçamento — Com o gerente de orçamento do Deadline Cloud, você pode criar e editar orçamentos para ajudar a gerenciar os custos do projeto.
- Explorador de uso — Com o explorador de uso do Deadline Cloud, você pode ver quantos AWS recursos são usados e os custos estimados desses recursos.

## Suposições de custo

O cálculo básico usado pelas ferramentas de gerenciamento de custos do Deadline Cloud é:

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

- O tempo de execução é a soma de todas as tarefas em um trabalho, da hora de início até a hora de término.
- A taxa de computação é determinada pelos [preços do AWS Deadline Cloud](#) para frotas gerenciadas por serviços. Para frotas gerenciadas pelo cliente, a taxa de computação é estimada em \$1 por hora de trabalho.
- A taxa de licença é determinada pelo preço base da licença do Deadline Cloud. Níveis adicionais não estão incluídos. Para obter mais informações sobre preços de licenças, consulte [Preços do AWS Deadline Cloud](#).

A estimativa de custo das ferramentas de gerenciamento de custos do Deadline Cloud pode variar de seus custos reais por vários motivos. Os motivos comuns incluem:

- Recursos de propriedade do cliente e seus preços. Você pode optar por trazer seus próprios recursos, de AWS ou externamente, do local ou de outros provedores de nuvem. Os custos reais desses recursos não são calculados.
- Custos de trabalhadores ociosos. Para frotas com uma contagem mínima de instâncias maior que zero, os trabalhadores ociosos não são contabilizados nos cálculos.
- Créditos promocionais, descontos e contratos de preços personalizados. As ferramentas de gerenciamento de custos não contabilizam créditos promocionais, acordos de preços privados ou outros descontos. Você pode se qualificar para outros descontos que não fazem parte da estimativa.
- Armazenamento de ativos. O armazenamento de ativos não está incluído nas estimativas de custo e uso.
- Mudanças no preço. AWS oferece pay-as-you-go preços para a maioria dos serviços. Os preços podem mudar com o tempo. As ferramentas de gerenciamento de custos usam a maioria dos up-to-date preços disponíveis publicamente, mas pode haver atrasos após as mudanças.
- Impostos. As ferramentas de gerenciamento de custos não incluem impostos aplicados à nossa compra do serviço.
- Arredondamento. A ferramenta de gerenciamento de custos realiza o arredondamento matemático dos dados de preços.
- Moeda. As estimativas de custo são feitas em dólares americanos. As taxas de câmbio globais variam com o tempo. Se você traduzir estimativas para uma base monetária diferente na bolsa atual, as alterações na taxa de câmbio afetarão a estimativa.
- Licenciamento externo. Se você optar por usar licenças pré-adquiridas (traga sua própria licença), as ferramentas de gerenciamento de custos do Deadline Cloud não podem contabilizar esse custo.

## Usando o gerenciador de orçamento do Deadline Cloud

O gerenciador de orçamento do Deadline Cloud ajuda você a controlar os gastos com um determinado recurso, como fila, frota ou fazenda. Você pode criar valores e limites orçamentários e definir ações automatizadas para ajudar a reduzir ou interromper gastos adicionais em relação ao orçamento.

As seções a seguir fornecem as etapas para usar o gerenciador de orçamento do Deadline Cloud.

### Tópicos

- [Pré-requisito](#)

- [Gerenciador de orçamento de acesso](#)
- [Criar um orçamento](#)
- [Exibir um orçamento](#)
- [Editar um orçamento](#)
- [Desativar um orçamento](#)

## Pré-requisito

Para usar o gerenciador de orçamento do Deadline Cloud, você deve ter um nível de OWNER acesso. Para conceder OWNER permissão, siga as etapas em [Gerenciando usuários no Deadline Cloud](#).

## Gerenciador de orçamento de acesso

Para acessar o gerente de orçamento do Deadline Cloud, use o procedimento a seguir.

1. Faça login AWS Management Console e abra o [console](#) do Deadline Cloud.
2. Escolha Exibir fazendas.
3. Localize a fazenda sobre a qual você deseja obter informações e escolha Gerenciar trabalhos. O monitor do Deadline Cloud é aberto em uma nova guia.
4. No monitor do Deadline Cloud, no painel de navegação esquerdo, escolha Orçamentos.

A página de resumo do gerente de orçamento exibe uma lista dos orçamentos ativos e inativos:

- Os orçamentos ativos são rastreados em relação ao recurso selecionado (uma fila).
- Os orçamentos inativos expiraram ou foram cancelados por um usuário e não estão mais rastreando os custos em relação aos limites desse orçamento.

Depois de escolher um orçamento, a página de resumo do orçamento contém informações básicas sobre o orçamento. As informações fornecidas incluem nome do orçamento, status, recursos, porcentagem restante, valor restante, orçamento total, data de início e data de término.

## Criar um orçamento

Para criar um orçamento, use o procedimento a seguir.

1. Se ainda não o fez, faça login no AWS Management Console, abra o [console](#) do Deadline Cloud, escolha uma fazenda e escolha Gerenciar trabalhos.
2. Na página Gerenciador de orçamento, escolha Criar orçamento.
3. Na seção de detalhes, insira um nome de orçamento para o orçamento.
4. (Opcional) No campo de descrição, insira uma descrição clara e breve do orçamento.
5. Em Recurso, escolha a lista suspensa Fila para encontrar e selecionar a fila para a qual você deseja criar um orçamento.
6. Em Período, defina as datas de início e término do orçamento concluindo as seguintes etapas:
  - a. Em Data de início, insira a primeira data do controle do orçamento no formato AAAA/MM/DD ou escolha o ícone do calendário e selecione uma data.

A data de início padrão é a data em que o orçamento é criado.
  - b. Em Data de término, insira a última data do controle do orçamento no formato AAAA/MM/DD ou escolha o ícone do calendário e selecione uma data.

A data de término padrão é 120 dias a partir da data de início.
7. Em Valor do orçamento, insira o valor em dólares do orçamento.
8. (Opcional) Recomendamos que você crie alertas de limite. Na seção Limitar ações, você pode implementar ações automatizadas que ocorrem quando valores específicos permanecem no orçamento. Para fazer isso, conclua as seguintes etapas:
  - a. Escolha Adicionar nova ação.
  - b. Em Valor restante, insira o valor em dólares que você deseja iniciar a ação.
  - c. No menu suspenso Ação, escolha a ação que você deseja. As ações incluem:
    - Pare depois de terminar o trabalho atual — Todo o trabalho atualmente em execução quando o valor limite é atingido continua em execução (e incorre em custos) até ser concluído.
    - Interrompa imediatamente o trabalho — Todo o trabalho é cancelado imediatamente quando o valor limite é atingido.
  - d. Para criar alertas de limite adicionais, escolha Adicionar nova ação e repita as duas etapas anteriores.
9. Escolha Criar orçamento. A página do gerente de orçamento é exibida. O orçamento recém-criado é exibido na guia Orçamentos ativos.



## Exibir um orçamento

Depois de criar um orçamento, você pode ver o orçamento na página Gerenciador de orçamento. A partir daí, você pode ver o valor total do orçamento e o custo geral alocado para o orçamento específico.

Para visualizar um orçamento, use o procedimento a seguir.

1. Se ainda não o fez, faça login no AWS Management Console, abra o [console](#) do Deadline Cloud, escolha uma fazenda e escolha Gerenciar trabalhos.
2. Escolha Orçamentos no painel de navegação do lado esquerdo. A página Gerenciador de orçamento é exibida.
3. Para exibir um orçamento ativo, escolha a guia Orçamentos ativos e escolha o nome do orçamento que você deseja exibir. A página de detalhes do orçamento é exibida.
4. Para visualizar os detalhes do orçamento de um orçamento expirado, escolha a guia Orçamentos inativos. Em seguida, escolha o nome do orçamento que você deseja visualizar. A página de detalhes do orçamento é exibida.

## Editar um orçamento

Você pode editar qualquer orçamento ativo. Para editar um orçamento ativo, use o procedimento a seguir.

1. Se ainda não o fez, faça login no AWS Management Console, abra o [console](#) do Deadline Cloud, escolha uma fazenda e escolha Gerenciar trabalhos.
2. Na página Gerenciador de Orçamento, na guia Orçamentos ativos, escolha o botão ao lado do orçamento que você deseja editar.
3. No menu suspenso Ações no canto superior direito, selecione Editar orçamento.
4. Faça as alterações desejadas e escolha Atualizar orçamento.

## Desativar um orçamento

Você pode desativar qualquer orçamento ativo. A desativação de um orçamento altera seu status de Ativo para Inativo. Quando um orçamento é desativado, ele não rastreia mais um recurso até o valor desse orçamento.

Para desativar um orçamento, use o procedimento a seguir.

1. Se ainda não o fez, faça login no AWS Management Console, abra o [console](#) do Deadline Cloud, escolha uma fazenda e escolha Gerenciar trabalhos.
2. Na página Gerenciador de orçamento, na guia Orçamentos ativos, escolha o botão ao lado do orçamento que você deseja desativar.
3. No menu suspenso Ações no canto superior direito, selecione Desativar orçamento. Em alguns instantes, o orçamento selecionado mudará de Ativo para Inativo e passará da guia Orçamentos Ativos para a guia Orçamentos Inativos.

## Usando o explorador de uso do Deadline Cloud

Com o explorador de uso do Deadline Cloud, você pode ver métricas em tempo real sobre a atividade que acontece em cada fazenda. Você pode analisar os custos da fazenda por diferentes variáveis, como fila, trabalho, produto licenciado ou tipos de instância. Selecione vários períodos de tempo para ver o uso durante um período específico e veja as tendências de uso ao longo do tempo. Você também pode ver uma análise detalhada dos pontos de dados selecionados, permitindo uma análise mais detalhada das métricas. O uso pode ser mostrado por tempo (minutos e horas) ou por custo (\$ USD).

As seções a seguir mostram as etapas para acessar e usar o explorador de uso do Deadline Cloud.

### Tópicos

- [Pré-requisito](#)
- [Abra o explorador de uso](#)
- [Use o explorador de uso](#)

## Pré-requisito

Para usar o explorador de uso do Deadline Cloud, você deve ter uma MANAGER ou outra permissão de OWNER fazenda. Para ter mais informações, consulte [Gerencie usuários e grupos para fazendas, filas e frotas](#).

## Abra o explorador de uso

Para abrir o explorador de uso do Deadline Cloud, use o procedimento a seguir.

1. Faça login AWS Management Console e abra o [console](#) do Deadline Cloud.

2. Para ver todas as fazendas disponíveis, escolha Exibir fazendas.
3. Localize a fazenda sobre a qual você deseja obter informações e escolha Gerenciar trabalhos. O monitor do Deadline Cloud é aberto em uma nova guia.
4. No monitor do Deadline Cloud, no menu à esquerda, selecione Explorador de uso.

## Use o explorador de uso

Na página do explorador de uso, você pode selecionar parâmetros específicos nos quais os dados podem ser exibidos. Por padrão, você vê o uso total em tempo (horas e minutos) nos últimos 7 dias. Você pode alterar esses parâmetros e as informações exibidas mudam dinamicamente de acordo com as configurações dos parâmetros.

Você pode agrupar os resultados com base na fila, no trabalho, no uso da computação, no tipo de instância ou no produto da licença. Se você escolher um produto licenciado, os custos serão calculados para licenças específicas. Para todos os outros grupos, o tempo é calculado somando o tempo gasto para cada tarefa ser executada.

O explorador de uso retorna somente 100 resultados com base nos critérios de filtro que você definiu. Os resultados são listados em ordem decrescente pela data e hora de criação. Se houver mais de 100 resultados, você receberá uma mensagem de erro. Você pode refinar sua consulta para reduzir o número de resultados:

- Selecione um intervalo de tempo menor
- Selecione menos filas
- Selecione um agrupamento diferente, como agrupamento por fila em vez de trabalho

### Tópicos

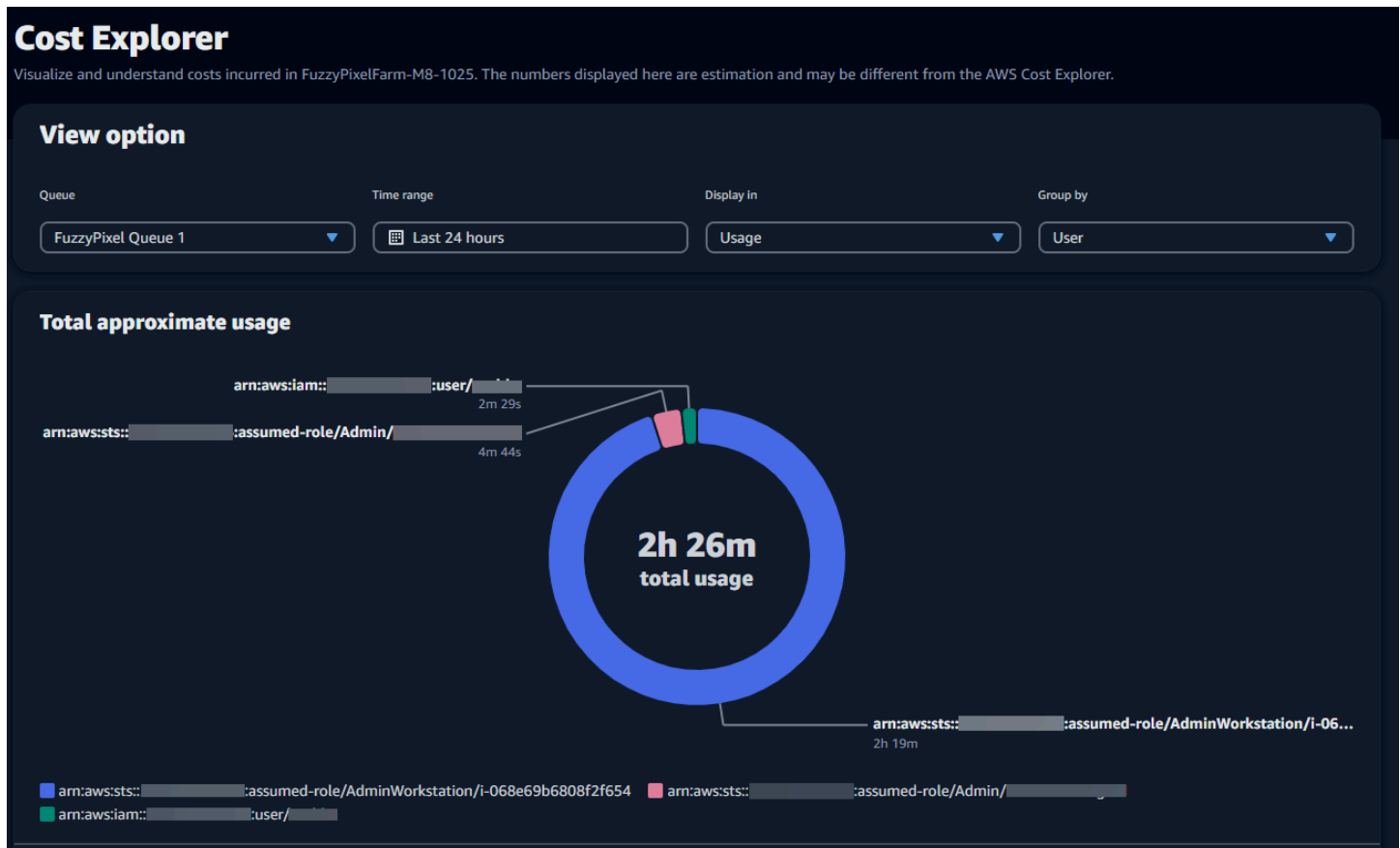
- [Use gráficos visuais para revisar dados](#)
- [Veja um detalhamento das métricas](#)
- [Exibir o tempo de execução aproximado das filas](#)

## Use gráficos visuais para revisar dados

Você pode revisar os dados em um formato visual para identificar tendências e áreas potenciais que possam precisar de mais análise ou atenção. O Explorador de Uso oferece um gráfico circular que exibe o uso e o custo gerais com a opção de agrupar os totais em subtotaís menores.

**Note**

O gráfico exibe apenas os cinco principais resultados com outros resultados combinados em uma seção “outros”. Você pode ver todos os resultados na seção de detalhamento abaixo do gráfico.



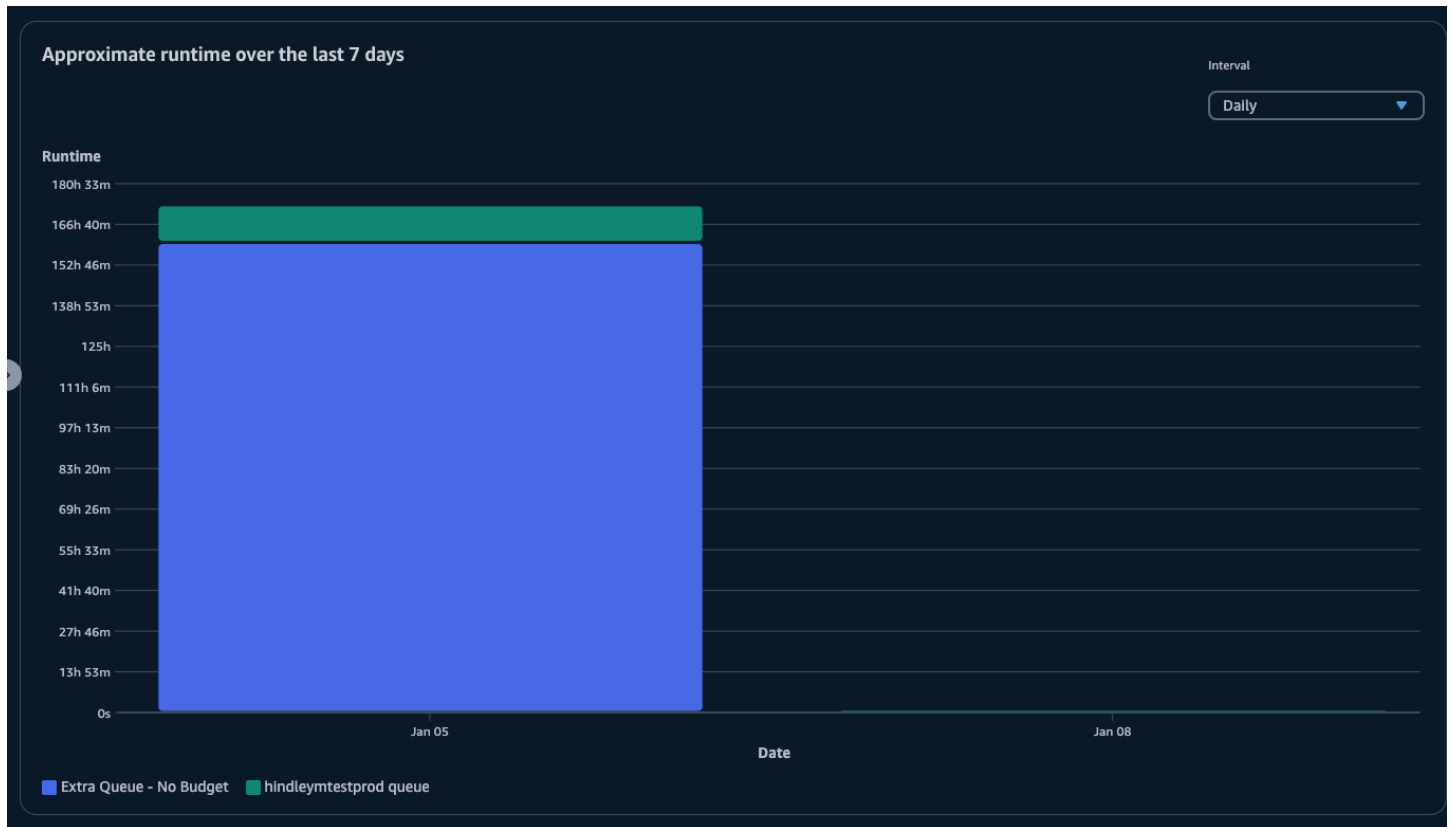
## Veja um detalhamento das métricas

Abaixo do gráfico circular, o explorador de uso oferece uma análise mais detalhada de métricas específicas, que mudarão à medida que os parâmetros mudarem. Por padrão, cinco resultados são exibidos no explorador de uso. Você pode percorrer os resultados usando as setas de paginação na seção de detalhamento.

Por padrão, a avaria é minimizada. Para expandir e exibir os resultados, selecione a seta Exibir todos os detalhes. Para baixar o detalhamento, escolha Baixar dados.

## Exibir o tempo de execução aproximado das filas

Você também pode visualizar o tempo de execução aproximado de suas filas com base nos diferentes intervalos que você especificar. As opções de intervalo são horárias, diárias, semanais e mensais. Depois de selecionar um intervalo, o gráfico exibe o tempo de execução aproximado de suas filas.



## Gerenciamento de custos

AWS O Deadline Cloud fornece orçamentos e o explorador de uso para ajudá-lo a controlar e visualizar os custos de seus trabalhos. No entanto, o Deadline Cloud usa outros AWS serviços, como o Amazon S3. Os custos desses serviços não são refletidos nos orçamentos do Deadline Cloud ou no explorador de uso e são cobrados separadamente com base no uso. Dependendo de como você configura o Deadline Cloud, você pode usar os seguintes AWS serviços, além de outros:

Serviço	Página de preços
CloudWatch Registros da Amazon	<a href="#">Preços do Amazon CloudWatch Logs</a>

Serviço	Página de preços
Amazon Elastic Compute Cloud	<a href="#">Preços do Amazon Elastic Compute Cloud</a>
AWS Key Management Service	<a href="#">Definição de preço do AWS Key Management Service</a>
AWS PrivateLink	<a href="#">Definição de preço do AWS PrivateLink</a>
Amazon Simple Storage Service	<a href="#">Preços do Amazon Simple Storage Service</a>
Amazon Virtual Private Cloud	<a href="#">Preços da Amazon Virtual Private Cloud</a>

## Melhores práticas de gerenciamento de custos

Usar as melhores práticas a seguir pode ajudá-lo a entender e controlar seus custos ao usar o Deadline Cloud e as compensações que você pode fazer entre custo e eficiência.

### Note

O custo final do uso do Deadline Cloud depende da interação entre vários AWS serviços, da quantidade de trabalho que você processa e de Região da AWS onde você executa seus trabalhos. As melhores práticas a seguir são diretrizes e podem não reduzir significativamente os custos.

## Práticas recomendadas para CloudWatch registros

O Deadline Cloud envia registros de trabalho e tarefas para o CloudWatch Logs. Você é cobrado por coletar, armazenar e analisar esses registros. Você pode reduzir custos registrando somente a quantidade mínima de dados necessária para monitorar suas tarefas.

Quando você cria uma fila ou frota, o Deadline Cloud cria um grupo de CloudWatch registros de registros com os seguintes nomes:

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

Por padrão, esses logs nunca expiram. Você pode ajustar a política de retenção dos grupos de registros para remover registros antigos e ajudar a reduzir os custos de armazenamento. Você também pode exportar logs para o Amazon S3. Os custos de armazenamento do Amazon S3 são mais baixos do que os do CloudWatch. Para obter mais informações, consulte [Como exportar dados de log para o Amazon S3](#).

## Melhores práticas do Amazon EC2

Você pode usar instâncias do Amazon EC2 para frotas gerenciadas por serviços e gerenciadas pelo cliente. Há três considerações:

- Para frotas gerenciadas por serviços, você pode optar por ter uma ou mais instâncias disponíveis o tempo todo, definindo a contagem mínima de trabalhadores para a frota. Quando você define a contagem mínima de trabalhadores acima de 0, a frota sempre tem esse número de trabalhadores em execução. Isso pode reduzir o tempo necessário para que o Deadline Cloud comece a processar trabalhos, mas você será cobrado pelo tempo ocioso da instância.
- Para frotas gerenciadas por serviços, defina um tamanho máximo para a frota. Isso limita o número de instâncias para as quais uma frota pode ser escalada automaticamente. As frotas não crescerão além desse tamanho, mesmo que haja mais trabalhos aguardando para serem processados.
- Para frotas gerenciadas por serviços e gerenciadas pelo cliente, você pode especificar os tipos de instância do Amazon EC2 em suas frotas. Usar instâncias menores custa menos por minuto, mas pode levar mais tempo para concluir um trabalho. Por outro lado, uma instância maior custa mais por minuto, mas pode reduzir o tempo de conclusão de um trabalho. Entender as demandas que seus trabalhos impõem a uma instância pode ajudar a reduzir seus custos.
- Quando possível, escolha instâncias spot do Amazon EC2 para sua frota. As instâncias spot estão disponíveis por um preço reduzido, mas podem ser interrompidas por solicitações sob demanda. As instâncias sob demanda são cobradas por segundo e não são interrompidas.

## Práticas recomendadas para AWS KMS

Por padrão, o Deadline Cloud criptografa seus dados com uma chave AWS própria. Você não será cobrado por essa chave.

Você pode optar por usar uma chave gerenciada pelo cliente para criptografar seus dados. Quando você usa sua própria chave, você é cobrado com base em como sua chave é usada. Se você usar uma chave existente, esse será um custo adicional para o uso adicional.

## Práticas recomendadas para AWS PrivateLink

Você pode usar AWS PrivateLink para criar uma conexão entre sua VPC e o Deadline Cloud usando um endpoint de interface. Ao criar uma conexão, você pode chamar todas as ações da Deadline Cloud API. Você é cobrado por hora por cada endpoint criado. Se você usa PrivateLink, você deve criar pelo menos três endpoints e, dependendo da sua configuração, você pode precisar de até cinco.

## Melhores práticas para o Amazon S3

O Deadline Cloud usa o Amazon S3 para armazenar ativos para processamento, anexos de trabalhos, saída e registros. Para reduzir os custos associados ao Amazon S3, reduza a quantidade de dados que você armazena. Algumas sugestões:

- Armazene somente ativos que estão em uso no momento ou que serão usados em breve.
- Use uma [configuração de ciclo de vida do S3](#) para excluir automaticamente arquivos não utilizados de um bucket do S3.

## Melhores práticas para Amazon VPC

Ao usar o licenciamento baseado no uso para sua frota gerenciada pelo cliente, você cria um endpoint de licença do Deadline Cloud, que é um endpoint da Amazon VPC criado em sua conta. Esse endpoint é cobrado por hora. Para reduzir custos, remova os endpoints quando você não estiver usando licenças baseadas no uso.



# Segurança em Deadline Cloud

A segurança na nuvem AWS é a maior prioridade. Como AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre você AWS e você. O [modelo de responsabilidade compartilhada](#) descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que é executada Serviços da AWS no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte dos Programas de Conformidade Programas de [AWS](#) de . Para saber mais sobre os programas de conformidade aplicáveis AWS Deadline Cloud, consulte [Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS em Escopo por Programa](#) .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS service (Serviço da AWS) que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar Deadline Cloud. Os tópicos a seguir mostram como configurar para atender Deadline Cloud aos seus objetivos de segurança e conformidade. Você também aprenderá a usar outros Serviços da AWS que o ajudem a monitorar e proteger seus Deadline Cloud recursos.

## Tópicos

- [Proteção de dados em Deadline Cloud](#)
- [Identity and Access Management na Deadline Cloud](#)
- [Validação de conformidade para Deadline Cloud](#)
- [Resiliência em Deadline Cloud](#)
- [Segurança da infraestrutura no Deadline Cloud](#)
- [Análise de configuração e vulnerabilidade no Deadline Cloud](#)
- [Prevenção contra o ataque do “substituto confuso” em todos os serviços](#)
- [Acesso AWS Deadline Cloud usando um endpoint de interface \(\)AWS PrivateLink](#)
- [Melhores práticas de segurança para o Deadline Cloud](#)

# Proteção de dados em Deadline Cloud

O modelo de [responsabilidade AWS compartilhada modelo](#) se aplica à proteção de dados em AWS Deadline Cloud. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para obter mais informações sobre a privacidade de dados, consulte as [Perguntas Frequentes sobre Privacidade de Dados](#). Para obter mais informações sobre a proteção de dados na Europa, consulte a postagem do blog [AWS LGPD e Modelo de Responsabilidade Compartilhada](#) no AWS Blog de Segurança.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS disponíveis, consulte [Federal Information Processing Standard \(FIPS\) 140-2](#).

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com Deadline Cloud ou Serviços da AWS usa o console, a API ou AWS os SDKs. AWS CLI Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico.

Se você fornecer um URL para um servidor externo, recomendamos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

## Tópicos

- [Criptografia em repouso](#)
- [Criptografia em trânsito](#)
- [Gerenciamento de chaves](#)
- [Privacidade do tráfego entre redes](#)
- [Optar por não participar](#)

## Criptografia em repouso

AWS Deadline Cloud protege dados confidenciais criptografando-os em repouso usando chaves de criptografia armazenadas em [AWS Key Management Service \(AWS KMS\)](#). A criptografia em repouso está disponível em todos os Regiões da AWS lugares Deadline Cloud disponíveis.

Criptografar dados significa que dados confidenciais salvos em discos não podem ser lidos por um usuário ou aplicativo sem uma chave válida. Somente uma parte com uma chave gerenciada válida pode descriptografar os dados.

Para obter informações sobre como Deadline Cloud usar AWS KMS a criptografia de dados em repouso, consulte [Gerenciamento de chaves](#).

## Criptografia em trânsito

Para dados em trânsito, AWS Deadline Cloud usa o Transport Layer Security (TLS) 1.2 ou 1.3 para criptografar dados enviados entre o serviço e os trabalhadores. Exigimos TLS 1.2 e recomendamos TLS 1.3. Além disso, se você usa uma nuvem privada virtual (VPC), você pode usá-la AWS PrivateLink para estabelecer uma conexão privada entre sua VPC e. Deadline Cloud

## Gerenciamento de chaves

Ao criar uma nova fazenda, você pode escolher uma das seguintes chaves para criptografar os dados da sua fazenda:

- AWS chave KMS de propriedade — Tipo de criptografia padrão se você não especificar uma chave ao criar o farm. A chave KMS é de propriedade de AWS Deadline Cloud. Você não pode

visualizar, gerenciar ou usar chaves AWS próprias. No entanto, você não precisa realizar nenhuma ação para proteger as chaves que criptografam seus dados. Para obter mais informações, consulte [chaves AWS próprias](#) no guia do AWS Key Management Service desenvolvedor.

- Chave KMS gerenciada pelo cliente — Você especifica uma chave gerenciada pelo cliente ao criar uma fazenda. Todo o conteúdo da fazenda é criptografado com a chave KMS. A chave é armazenada em sua conta e é criada, de propriedade e gerenciada por você, e AWS KMS cobranças são aplicadas. Você tem controle total sobre a chave KMS. Você pode realizar tarefas como:
  - Estabelecendo e mantendo as principais políticas
  - Estabelecer e manter subsídios e IAM policies
  - Habilitar e desabilitar políticas de chaves
  - Adicionar etiquetas
  - Criar réplicas de chaves

Você não pode alternar manualmente uma chave de propriedade do cliente usada em uma Deadline Cloud fazenda. A rotação automática da chave é suportada.

Para obter mais informações, consulte [Chaves de propriedade do cliente](#) no Guia do AWS Key Management Service desenvolvedor.

Para criar uma chave gerenciada pelo cliente, siga as etapas para [Criar chaves simétricas gerenciadas pelo cliente](#) no Guia do AWS Key Management Service desenvolvedor.

## Como Deadline Cloud usar AWS KMS subsídios

Deadline Cloud exige uma [concessão](#) para usar sua chave gerenciada pelo cliente. Quando você cria uma fazenda criptografada com uma chave gerenciada pelo cliente, Deadline Cloud cria uma concessão em seu nome enviando uma [CreateGrant](#) solicitação AWS KMS para obter acesso à chave KMS que você especificou.

Deadline Cloud usa várias concessões. Cada concessão é usada por uma parte diferente Deadline Cloud que precisa criptografar ou descriptografar seus dados. Deadline Cloud também usa concessões para permitir o acesso a outros AWS serviços usados para armazenar dados em seu nome, como Amazon Simple Storage Service, Amazon Elastic Block Store ou OpenSearch.

Os subsídios que Deadline Cloud permitem gerenciar máquinas em uma frota gerenciada por serviços incluem um número de Deadline Cloud conta e uma função no, em `GranteePrincipal`

vez de um diretor de serviço. Embora não seja típico, isso é necessário para criptografar volumes do Amazon EBS para trabalhadores em frotas gerenciadas por serviços usando a chave KMS gerenciada pelo cliente especificada para a fazenda.

## Política de chaves gerenciada pelo cliente

As políticas de chaves controlam o acesso à chave gerenciada pelo cliente. Cada chave deve ter exatamente uma política de chaves que contenha declarações que determinem quem pode usar a chave e como usá-la. Ao criar sua chave gerenciada pelo cliente, você pode especificar uma política de chaves. Para obter mais informações, consulte [Managing access to customer managed keys](#) (Administrando o acesso a chaves gerenciadas pelo cliente) no Guia do desenvolvedor do AWS Key Management Service .

### Política mínima de IAM para CreateFarm

Para usar sua chave gerenciada pelo cliente para criar fazendas usando o console ou a operação de [CreateFarm](#) API, as seguintes operações de AWS KMS API devem ser permitidas:

- [kms:CreateGrant](#): Adiciona uma concessão a uma chave gerenciada pelo cliente. Concede acesso ao console a uma AWS KMS chave especificada. Para obter mais informações, consulte Como [usar subsídios](#) no guia do AWS Key Management Service desenvolvedor.
- [kms:Decrypt](#)— Deadline Cloud Permite descriptografar dados na fazenda.
- [kms:DescribeKey](#)— Fornece os detalhes da chave gerenciada pelo cliente Deadline Cloud para permitir a validação da chave.
- [kms:GenerateDataKey](#)— Permite Deadline Cloud criptografar dados usando uma chave de dados exclusiva.

A declaração de política a seguir concede as permissões necessárias para a CreateFarm operação.

```
{
  "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 mínima de IAM para operações somente de leitura

Usar sua chave gerenciada pelo cliente para Deadline Cloud operações somente de leitura, como obter informações sobre fazendas, filas e frotas. As seguintes operações de AWS KMS API devem ser permitidas:

- [kms:Decrypt](#)— Deadline Cloud Permite descriptografar dados na fazenda.
- [kms:DescribeKey](#)— Fornece os detalhes da chave gerenciada pelo cliente Deadline Cloud para permitir a validação da chave.

A declaração de política a seguir concede as permissões necessárias para operações somente para leitura.

```

{
  "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 mínima de IAM para operações de leitura e gravação

Para usar sua chave gerenciada pelo cliente para Deadline Cloud operações de leitura e gravação, como criar e atualizar fazendas, filas e frotas. As seguintes operações de AWS KMS API devem ser permitidas:

- [kms:Decrypt](#)— Deadline Cloud Permite descriptografar dados na fazenda.
- [kms:DescribeKey](#)— Fornece os detalhes da chave gerenciada pelo cliente Deadline Cloud para permitir a validação da chave.
- [kms:GenerateDataKey](#)— Permite Deadline Cloud criptografar dados usando uma chave de dados exclusiva.

A declaração de política a seguir concede as permissões necessárias para a CreateFarm operação.

```

{
  "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"
        }
      }
    }
  ]
}

```

```
}
```

## Monitorar suas chaves de criptografia

Ao usar uma chave gerenciada pelo AWS KMS cliente em suas Deadline Cloud fazendas, você pode usar [AWS CloudTrail](#) [Amazon CloudWatch Logs](#) para rastrear solicitações Deadline Cloud enviadas para AWS KMS.

### CloudTrail evento para bolsas

O CloudTrail evento de exemplo a seguir ocorre quando as concessões são criadas, normalmente quando você chama a CreateFleet operação CreateFarmCreateMonitor, ou.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIQDTESTANDEXAMPLE:SampleUser01",
    "arn": "arn:aws::sts::111122223333:assumed-role/Admin/SampleUser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE3",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE",
        "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 para decodificação

O CloudTrail evento de exemplo a seguir ocorre ao descriptografar valores usando a chave KMS gerenciada pelo cliente.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIQDTESTANDEXAMPLE:SampleUser01",
    "arn": "arn:aws::sts::111122223333:assumed-role/SampleRole/SampleUser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE",
        "arn": "arn:aws::iam::111122223333:role/SampleRole",
        "accountId": "111122223333",
        "userName": "SampleRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2024-04-23T18:46:51Z",
        "mfaAuthenticated": "false"
      }
    },
    "invokedBy": "deadline.amazonaws.com"
  },
  "eventTime": "2024-04-23T18:51:44Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "deadline.amazonaws.com",
  "userAgent": "deadline.amazonaws.com",
  "requestParameters": {
    "encryptionContext": {
      "aws:deadline:farmId": "farm-abcdef12345678900987654321fedcba",
      "aws:deadline:accountId": "111122223333",
      "aws-crypto-public-key": "AotL+SAMPLEVALUEiOMEXAMPLEEaaqNOTREALaGTESTONLY
+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-eeeeefffffff",
  "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 para criptografia

O CloudTrail evento de exemplo a seguir ocorre ao criptografar valores usando a chave KMS gerenciada pelo cliente.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAIQDTESTANDEXAMPLE:SampleUser01",
    "arn": "arn:aws::sts::111122223333:assumed-role/SampleRole/SampleUser01",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAIQDTESTANDEXAMPLE",
        "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-abcdef12345678900987654321fedcba",
      "aws:deadline:accountId": "111122223333",
      "aws-crypto-public-key": "AotL+SAMPLEVALUEiOMEXAMPLEEaaqNOTREALaGTESTONLY

+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"
}

```

## Excluindo uma chave KMS gerenciada pelo cliente

A exclusão de uma chave KMS gerenciada pelo cliente em AWS Key Management Service (AWS KMS) é destrutiva e potencialmente perigosa. Exclui irreversivelmente o material da chave e todos os metadados associados à chave. Depois que uma chave do KMS gerenciada pelo cliente é excluída, não é mais possível descriptografar os dados que foram criptografados com ela. Isso significa que os dados se tornam irrecuperáveis.

É por isso que AWS KMS oferece aos clientes um período de espera de até 30 dias antes de excluir a chave KMS. O período de espera padrão é de 30 dias.

### Sobre o período de espera

Como é destrutivo e potencialmente perigoso excluir uma chave KMS gerenciada pelo cliente, exigimos que você defina um período de espera de 7 a 30 dias. O período de espera padrão é de 30 dias.

No entanto, o período de espera real pode ser até 24 horas a mais do que o período programado. Para obter a data e a hora reais em que a chave será excluída, use a [DescribeKey](#) operação. Você também pode ver a data de exclusão agendada de uma chave no [console AWS KMS](#), na página de detalhes da chave, na seção Configuração geral. Observe o fuso horário.

Durante o período de espera, o status e o estado da chave gerenciada pelo cliente são Exclusão pendente.

- Uma chave KMS gerenciada pelo cliente que está com exclusão pendente não pode ser usada em nenhuma [operação criptográfica](#).
- AWS KMS não [gira as chaves de backup das chaves](#) KMS gerenciadas pelo cliente que estão pendentes de exclusão.

Para obter mais informações sobre como excluir uma chave KMS gerenciada pelo cliente, consulte [Excluir chaves mestras do cliente no Guia](#) do AWS Key Management Service desenvolvedor.

## Privacidade do tráfego entre redes

AWS Deadline Cloud oferece suporte à Amazon Virtual Private Cloud (Amazon VPC) para proteger conexões. A Amazon VPC fornece atributos que você pode usar para aumentar e monitorar a segurança da sua nuvem privada virtual (VPC).

Você pode configurar uma frota gerenciada pelo cliente (CMF) com instâncias do Amazon Elastic Compute Cloud (Amazon EC2) que são executadas dentro de uma VPC. Ao implantar endpoints Amazon VPC para AWS PrivateLink uso, o tráfego entre os trabalhadores em sua CMF e o endpoint permanece dentro Deadline Cloud da sua VPC. Além disso, você pode configurar sua VPC para restringir o acesso à Internet às suas instâncias.

Em frotas gerenciadas por serviços, os trabalhadores não podem ser acessados pela Internet, mas eles têm acesso à Internet e se conectam ao serviço pela Deadline Cloud Internet.

## Optar por não participar

AWS Deadline Cloud coleta determinadas informações operacionais para nos ajudar a desenvolver e melhorar Deadline Cloud. Os dados coletados incluem itens como seu ID de AWS conta e ID de usuário, para que possamos identificá-lo corretamente se você tiver um problema com Deadline Cloud o. Também coletamos informações Deadline Cloud específicas, como IDs de recursos (um FarmID ou QueueID quando aplicável), o nome do produto (por exemplo, JobAttachments WorkerAgent, e mais) e a versão do produto.

Você pode optar por não participar dessa coleta de dados usando a configuração do aplicativo. Cada computador que interage com Deadline Cloud, tanto as estações de trabalho do cliente quanto com os trabalhadores da frota, precisa optar por não participar separadamente.

### Deadline Cloud monitor - desktop

Deadline Cloud monitor - o desktop coleta informações operacionais, como quando ocorrem falhas e quando o aplicativo é aberto, para nos ajudar a saber quando você está tendo problemas com o aplicativo. Para optar por não coletar essas informações operacionais, acesse a página de configurações e desmarque Ativar a coleta de dados para medir o desempenho do Deadline Cloud Monitor.

Depois que você optar por não participar, o monitor do desktop não enviará mais os dados operacionais. Todos os dados coletados anteriormente são retidos e ainda podem ser usados para melhorar o serviço. Para obter mais informações, consulte [Perguntas frequentes sobre a privacidade de dados da](#) .

### AWS Deadline Cloud CLI e ferramentas

A AWS Deadline Cloud CLI, os remetentes e o agente de trabalho coletam informações operacionais, como quando ocorrem falhas e quando os trabalhos são enviados, para nos ajudar

a saber quando você está tendo problemas com esses aplicativos. Para cancelar a coleta dessas informações operacionais, use qualquer um dos seguintes métodos:

- No terminal, entre **deadline config set telemetry.opt\_out true**.

Isso excluirá a CLI, os remetentes e o agente de trabalho quando executados como o usuário atual.

- Ao instalar o Deadline Cloud agente de trabalho, adicione o argumento da linha de **--telemetry-opt-out** comando. Por exemplo, **./install.sh --farm-id \$FARM\_ID --fleet-id \$FLEET\_ID --telemetry-opt-out**.
- Antes de executar o agente de trabalho, a CLI ou o remetente, defina uma variável de ambiente: **DEADLINE\_CLOUD\_TELEMETRY\_OPT\_OUT=true**

Depois que você optar por não participar, as Deadline Cloud ferramentas não enviarão mais os dados operacionais. Todos os dados coletados anteriormente são retidos e ainda podem ser usados para melhorar o serviço. Para obter mais informações, consulte [Perguntas frequentes sobre a privacidade de dados da](#) .

## Identity and Access Management na Deadline Cloud

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) para usar os recursos do Deadline Cloud. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

### Tópicos

- [Público](#)
- [Autenticando com identidades](#)
- [Gerenciando acesso usando políticas](#)
- [Como o Deadline Cloud funciona com o IAM](#)
- [Exemplos de políticas baseadas em identidade para o Deadline Cloud](#)
- [AWS políticas gerenciadas para Deadline Cloud](#)

- [Solução de problemas de identidade e acesso ao AWS Deadline Cloud](#)

## Público

A forma como você usa o AWS Identity and Access Management (IAM) é diferente, dependendo do trabalho que você faz no Deadline Cloud.

**Usuário do serviço** — Se você usa o serviço Deadline Cloud para fazer seu trabalho, seu administrador fornecerá as credenciais e as permissões de que você precisa. À medida que você usa mais recursos do Deadline Cloud para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso no Deadline Cloud, consulte [Solução de problemas de identidade e acesso ao AWS Deadline Cloud](#).

**Administrador de serviços** — Se você é responsável pelos recursos do Deadline Cloud em sua empresa, provavelmente tem acesso total ao Deadline Cloud. É seu trabalho determinar quais recursos e recursos do Deadline Cloud seus usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com o Deadline Cloud, consulte [Como o Deadline Cloud funciona com o IAM](#).

**Administrador do IAM** — Se você é administrador do IAM, talvez queira saber detalhes sobre como criar políticas para gerenciar o acesso ao Deadline Cloud. Para ver exemplos de políticas baseadas em identidade do Deadline Cloud que você pode usar no IAM, consulte [Exemplos de políticas baseadas em identidade para o Deadline Cloud](#)

## Autenticando com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.



Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login em AWS, consulte [Como fazer login Conta da AWS](#) no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte [Assinatura de solicitações de AWS API](#) no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte [Autenticação multifator](#) no Guia AWS IAM Identity Center do usuário e [Utilizar a autenticação multifator \(MFA\) na AWS](#) no Guia do usuário do IAM.

## Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele puder executar. Para obter a lista completa das tarefas que exigem login como usuário raiz, consulte [Tarefas que exigem credenciais de usuário raiz](#) no Guia do Usuário do IAM.

## Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o AWS IAM Identity Center. Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte [“O que é o Centro de Identidade do IAM?”](#) no Guia do usuário AWS IAM Identity Center .

## Usuários e grupos do IAM

Um [usuário do IAM](#) é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos contar com credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte [Altere as chaves de acesso regularmente para casos de uso que exijam credenciais de longo prazo](#) no Guia do Usuário do IAM.

Um [grupo do IAM](#) é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdmins e conceder a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte [Quando criar um usuário do IAM \(em vez de um perfil\)](#) no Guia do usuário do IAM.

## Perfis do IAM

Uma [função do IAM](#) é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console [trocando de funções](#). Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para o uso de perfis, consulte [Utilizar perfis do IAM](#) no Guia do usuário do IAM.

Funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- **Acesso de usuário federado:** para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte [Criar um perfil para um provedor de identidades de terceiros](#) no Guia do Usuário do IAM. Se você usar o Centro de identidade do IAM, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o Centro de identidade do IAM correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte [Conjuntos de permissões](#) no Guia do usuário AWS IAM Identity Center .
- **Permissões temporárias para usuários do IAM** — um usuário ou um perfil do IAM pode presumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- **Acesso entre contas** — é possível usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) em outra conta acesse recursos em sua conta. Os perfis são a principal forma de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para saber a diferença entre funções e políticas baseadas em recursos para acesso entre contas, consulte [Acesso a recursos entre contas no IAM no Guia do usuário do IAM](#).
- **Acesso entre serviços** — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões do principal de chamada, usando um perfil de serviço ou um perfil vinculado a um serviço.
- **Sessões de acesso direto (FAS)** — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte [Encaminhar sessões de acesso](#).
- **Função de serviço:** um perfil de serviço é um [perfil do IAM](#) que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte [Criar um perfil para delegar permissões a um AWS service \(Serviço da AWS\)](#) no Guia do Usuário do IAM.

- **Função vinculada ao serviço** — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS). O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não editar as permissões para funções vinculadas ao serviço.
- **Aplicativos em execução no Amazon EC2** — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. É preferível fazer isso armazenando chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém o perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte [Utilizar um perfil do IAM para conceder permissões a aplicações em execução nas instâncias do Amazon EC2](#) no Guia do usuário do IAM.

Para saber se deseja usar perfis do IAM, consulte [Quando criar um perfil do IAM \(em vez de um usuário\)](#) no Guia do usuário do IAM.

## Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte [Visão geral das políticas JSON](#) no Guia do Usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissões para executar ações nos recursos que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

As políticas do IAM definem permissões para uma ação independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação

`iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

## Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte [Criando políticas do IAM](#) no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma política gerenciada ou uma política em linha, consulte [Escolher entre políticas gerenciadas e políticas em linha](#) no Guia do Usuário do IAM.

## Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve [especificar uma entidade principal](#) em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

## Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Para saber mais sobre ACLs, consulte [Visão geral da lista de controle de acesso \(ACL\)](#) no Guia do Desenvolvedor do Amazon Simple Storage Service.

## Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- **Limites de permissões:** um limite de permissões é um atributo avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade com seus limites de permissões. As políticas baseadas em recurso que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte [Limites de permissões para identidades do IAM](#) no Guia do Usuário do IAM.
- **Políticas de controle de serviço (SCPs)** — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente várias Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte [How SCPs work](#) (Como os SCPs funcionam) no Guia do usuário do AWS Organizations .
- **Políticas de sessão:** são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte [Políticas de sessão](#) no Guia do Usuário do IAM.

## Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte [Lógica de avaliação de políticas](#) no Guia do usuário do IAM.

## Como o Deadline Cloud funciona com o IAM

Antes de usar o IAM para gerenciar o acesso ao Deadline Cloud, saiba quais recursos do IAM estão disponíveis para uso com o Deadline Cloud.

Recursos do IAM que você pode usar com o AWS Deadline Cloud

Atributo do IAM	Suporte Deadline Cloud
<a href="#">Políticas baseadas em identidade</a>	Sim
<a href="#">Políticas baseadas em recursos</a>	Não
<a href="#">Ações das políticas</a>	Sim
<a href="#">Atributos de políticas</a>	Sim
<a href="#">Chaves de condição de política (específicas do serviço)</a>	Sim
<a href="#">ACLs</a>	Não
<a href="#">ABAC (tags em políticas)</a>	Sim
<a href="#">Credenciais temporárias</a>	Sim
<a href="#">Sessões de acesso direto (FAS)</a>	Sim
<a href="#">Perfis de serviço</a>	Sim
<a href="#">Perfis vinculados ao serviço</a>	Não

Para ter uma visão de alto nível de como o Deadline Cloud e outros Serviços da AWS funcionam com a maioria dos recursos do IAM, consulte [AWS os serviços que funcionam com o IAM](#) no Guia do usuário do IAM.

## Políticas baseadas em identidade para o Deadline Cloud

Suporta políticas baseadas em identidade	Sim
--	-----

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e perfis podem realizar, em quais recursos e em que condições. Para saber como criar uma política baseada em identidade, consulte [Criando políticas do IAM](#) no Guia do Usuário do IAM.

Com as políticas baseadas em identidade do IAM, é possível especificar ações ou recursos permitidos ou negados, assim como as condições sob as quais as ações são permitidas ou negadas. Você não pode especificar a entidade principal em uma política baseada em identidade porque ela se aplica ao usuário ou perfil ao qual ela está anexada. Para saber mais sobre todos os elementos que podem ser usados em uma política JSON, consulte [Referência de elementos da política JSON do IAM](#) no Guia do Usuário do IAM.

## Exemplos de políticas baseadas em identidade para o Deadline Cloud

Para ver exemplos de políticas baseadas em identidade do Deadline Cloud, consulte. [Exemplos de políticas baseadas em identidade para o Deadline Cloud](#)

## Políticas baseadas em recursos dentro do Deadline Cloud

Oferece compatibilidade com políticas baseadas em recursos	Não
--	-----

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de perfil do IAM e as políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para



o recurso ao qual a política está anexada, a política define quais ações um principal especificado pode executar nesse recurso e em que condições. Você deve [especificar uma entidade principal](#) em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Para permitir o acesso entre contas, você pode especificar uma conta inteira ou as entidades do IAM em outra conta como a entidade principal em uma política baseada em atributo. Adicionar uma entidade principal entre contas à política baseada em recurso é apenas metade da tarefa de estabelecimento da relação de confiança. Quando o principal e o recurso são diferentes Contas da AWS, um administrador do IAM na conta confiável também deve conceder permissão à entidade principal (usuário ou função) para acessar o recurso. Eles concedem permissão ao anexar uma política baseada em identidade para a entidade. No entanto, se uma política baseada em recurso conceder acesso a uma entidade principal na mesma conta, nenhuma política baseada em identidade adicional será necessária. Para obter mais informações, consulte [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.

## Ações políticas para o Deadline Cloud

Oferece compatibilidade com ações de políticas	Sim
--	-----

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Action` de uma política JSON descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome da operação de AWS API associada. Existem algumas exceções, como ações somente de permissão, que não têm uma operação de API correspondente. Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista das ações do Deadline Cloud, consulte [Ações definidas pelo AWS Deadline Cloud](#) na Referência de Autorização do Serviço.

As ações políticas no Deadline Cloud usam o seguinte prefixo antes da ação:

```
deadline
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [  
  "deadline:action1",  
  "deadline:action2"  
]
```

Para ver exemplos de políticas baseadas em identidade do Deadline Cloud, consulte [Exemplos de políticas baseadas em identidade para o Deadline Cloud](#)

## Recursos de políticas para o Deadline Cloud

Oferece compatibilidade com recursos de políticas	Sim
---	-----

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento de política JSON `Resource` especifica o objeto ou os objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu [nome do recurso da Amazon \(ARN\)](#). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem compatibilidade com permissões em nível de recurso, como operações de listagem, use um curinga (\*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para ver uma lista dos tipos de recursos do Deadline Cloud e seus ARNs, consulte [Recursos definidos pelo AWS Deadline Cloud](#) na Referência de autorização de serviço. Para saber com quais ações você pode especificar o ARN de cada recurso, consulte [Ações definidas pelo AWS Deadline Cloud](#).

Para ver exemplos de políticas baseadas em identidade do Deadline Cloud, consulte [Exemplos de políticas baseadas em identidade para o Deadline Cloud](#)

## Chaves de condição de política para o Deadline Cloud

Suporta chaves de condição de política específicas de serviço	Sim
---	-----

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos, e em que condições.

O elemento `Condition` (ou bloco `Condition`) permite que você especifique condições nas quais uma instrução estiver em vigor. O elemento `Condition` é opcional. É possível criar expressões condicionais que usem [agentes de condição](#), como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários elementos `Condition` em uma instrução ou várias chaves em um único `Condition` elemento, a AWS os avaliará usando uma operação lógica AND. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma OR operação lógica. Todas as condições devem ser atendidas antes que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, é possível conceder a um usuário do IAM permissão para acessar um atributo somente se ele estiver marcado com seu nome de usuário do IAM. Para obter mais informações, consulte [Elementos da política do IAM: variáveis e tags](#) no Guia do usuário do IAM.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver todas as chaves de condição AWS globais, consulte as [chaves de contexto de condição AWS global](#) no Guia do usuário do IAM.

Para ver uma lista das chaves de condição do Deadline Cloud, consulte [Chaves de condição do AWS Deadline Cloud](#) na Referência de autorização de serviço. Para saber com quais ações e recursos você pode usar uma chave de condição, consulte [Ações definidas pelo AWS Deadline Cloud](#).

Para ver exemplos de políticas baseadas em identidade do Deadline Cloud, consulte [Exemplos de políticas baseadas em identidade para o Deadline Cloud](#)

## ACLs na Deadline Cloud

Oferece compatibilidade com ACLs	Não
----------------------------------	-----

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou perfis da conta) têm permissões para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

## ABAC com Deadline Cloud

Oferece compatibilidade com ABAC (tags em políticas)	Sim
--	-----

O controle de acesso por atributo (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a entidades do IAM (usuários ou funções) e a vários AWS recursos. A marcação de entidades e atributos é a primeira etapa do ABAC. Em seguida, você cria políticas de ABAC para permitir operações quando a tag da entidade principal corresponder à tag do recurso que ela estiver tentando acessar.

O ABAC é útil em ambientes que estão crescendo rapidamente e ajuda em situações onde o gerenciamento de políticas se torna um problema.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no [elemento de condição](#) de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Se um serviço oferecer suporte às três chaves de condição para cada tipo de recurso, o valor será Sim para o serviço. Se um serviço oferecer suporte às três chaves de condição somente para alguns tipos de recursos, o valor será Parcial

Para obter mais informações sobre o ABAC, consulte [O que é ABAC?](#) no Guia do Usuário do IAM. Para visualizar um tutorial com etapas para configurar o ABAC, consulte [Utilizar controle de acesso baseado em atributos \(ABAC\)](#) no Guia do usuário do IAM.

## Usando credenciais temporárias com o Deadline Cloud

Oferece compatibilidade com credenciais temporárias	Sim
---	-----

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS funcionam com credenciais temporárias, consulte Serviços da AWS “[Trabalhe com o IAM](#)” no Guia do usuário do IAM.

Você está usando credenciais temporárias se fizer login AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre como alternar funções, consulte [Alternar para um perfil \(console\)](#) no Guia do usuário do IAM.

Você pode criar manualmente credenciais temporárias usando a AWS API AWS CLI ou. Em seguida, você pode usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para mais informações, consulte [Credenciais de segurança temporárias no IAM](#).

## Sessões de acesso direto para o Deadline Cloud

Suporte para o recurso Encaminhamento de sessões de acesso (FAS)	Sim
--	-----

Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado um principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte [Encaminhar sessões de acesso](#).

## Funções de serviço do Deadline Cloud

Oferece compatibilidade com funções de serviço	Sim
--	-----

O perfil de serviço é um [perfil do IAM](#) que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte [Criar um perfil para delegar permissões a um AWS service \(Serviço da AWS\)](#) no Guia do Usuário do IAM.

### Warning

Alterar as permissões de uma função de serviço pode interromper a funcionalidade do Deadline Cloud. Edite as funções de serviço somente quando o Deadline Cloud fornecer orientação para fazer isso.

## Funções vinculadas a serviços para o Deadline Cloud

Oferece suporte a perfis vinculados ao serviço	Não
--	-----

Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um [AWS service \(Serviço da AWS\)](#). O serviço pode presumir a função de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para perfis vinculados ao serviço.

Para obter detalhes sobre como criar ou gerenciar perfis vinculados a serviços, consulte [Serviços da AWS que funcionam com o IAM](#). Encontre um serviço na tabela que inclua um Yes na coluna Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

## Exemplos de políticas baseadas em identidade para o Deadline Cloud

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do Deadline Cloud. Eles também não podem realizar tarefas usando a AWS API AWS Management Console,

AWS Command Line Interface (AWS CLI) ou. Para conceder aos usuários permissão para executar ações nos recursos de que precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM aos perfis e os usuários podem presumir os perfis.

Para saber como criar uma política baseada em identidade do IAM usando esses exemplos de documento de política JSON, consulte [Criação de políticas do IAM](#) no Guia do Usuário do IAM.

Para obter detalhes sobre ações e tipos de recursos definidos pelo Deadline Cloud, incluindo o formato dos ARNs para cada um dos tipos de recursos, consulte [Ações, recursos e chaves de condição do AWS Deadline Cloud](#) na Referência de Autorização de Serviço.

## Tópicos

- [Melhores práticas de política](#)
- [Usando o console do Deadline Cloud](#)
- [Política para enviar trabalhos para uma fila](#)
- [Política para permitir a criação de um endpoint de licença](#)
- [Política para permitir o monitoramento de uma fila específica da fazenda](#)

## Melhores práticas de política

As políticas baseadas em identidade determinam se alguém pode criar, acessar ou excluir recursos do Deadline Cloud em sua conta. Essas ações podem incorrer em custos para sua Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece com as políticas AWS gerenciadas e passe para as permissões de privilégios mínimos — Para começar a conceder permissões aos seus usuários e cargas de trabalho, use as políticas AWS gerenciadas que concedem permissões para muitos casos de uso comuns. Eles estão disponíveis no seu Conta da AWS. Recomendamos que você reduza ainda mais as permissões definindo políticas gerenciadas pelo AWS cliente que sejam específicas para seus casos de uso. Para obter mais informações, consulte [Políticas gerenciadas pela AWS](#) ou [Políticas gerenciadas pela AWS para funções de trabalho](#) no Guia do Usuário do IAM.
- Aplique permissões de privilégio mínimo — ao definir permissões com as políticas do IAM, conceda apenas as permissões necessárias para executar uma tarefa. Você faz isso definindo as ações que podem ser executadas em atributos específicos sob condições específicas, também conhecidas como permissões de privilégio mínimo. Para obter mais informações sobre como usar

o IAM para aplicar permissões, consulte [Políticas e permissões no IAM](#) no Guia do Usuário do IAM.

- Use condições nas políticas do IAM para restringir ainda mais o acesso — você pode adicionar uma condição às políticas para limitar o acesso a ações e recursos. Por exemplo, você pode gravar uma condição de política para especificar que todas as solicitações devem ser enviadas usando SSL. Você também pode usar condições para conceder acesso às ações de serviço se elas forem usadas por meio de uma ação específica AWS service (Serviço da AWS), como AWS CloudFormation. Para obter mais informações, consulte [Elementos da política JSON do IAM: Condição](#) no Guia do usuário do IAM.
- Use o IAM Access Analyzer para validar suas políticas do IAM a fim de garantir permissões seguras e funcionais — o IAM Access Analyzer valida as políticas novas e existentes para que elas sigam a linguagem de política do IAM (JSON) e as práticas recomendadas do IAM. O IAM Access Analyzer oferece mais de 100 verificações de política e recomendações acionáveis para ajudá-lo a criar políticas seguras e funcionais. Para obter mais informações, consulte [Validação de políticas do IAM Access Analyzer](#) no Guia do Usuário do IAM.
- Exigir autenticação multifator (MFA) — Se você tiver um cenário que exija usuários do IAM ou um usuário root, ative Conta da AWS a MFA para obter segurança adicional. Para exigir MFA quando as operações de API forem chamadas, adicione condições de MFA às suas políticas. Para obter mais informações, consulte [Configuração de acesso à API protegido por MFA](#) no Guia do Usuário do IAM.

Para obter mais informações sobre as práticas recomendadas do IAM, consulte [Práticas Recomendadas de Segurança no IAM](#) no Guia do Usuário do IAM.

## Usando o console do Deadline Cloud

Para acessar o console do AWS Deadline Cloud, você deve ter um conjunto mínimo de permissões. Essas permissões devem permitir que você liste e visualize detalhes sobre os recursos do Deadline Cloud em seu Conta da AWS. Se você criar uma política baseada em identidade que seja mais restritiva do que as permissões mínimas necessárias, o console não funcionará como pretendido para entidades (usuários ou perfis) com essa política.

Você não precisa permitir permissões mínimas do console para usuários que estão fazendo chamadas somente para a API AWS CLI ou para a AWS API. Em vez disso, permita o acesso somente a ações que correspondam a operação de API que estiverem tentando executar.



Para garantir que usuários e funções ainda possam usar o console do Deadline Cloud, anexe também o Deadline Cloud *ConsoleAccess* ou a política *ReadOnly* AWS gerenciada às entidades. Para obter mais informações, consulte [Adicionando Permissões a um Usuário](#) no Guia do Usuário do IAM.

## Política para enviar trabalhos para uma fila

Neste exemplo, você cria uma política de escopo reduzido que concede permissão para enviar trabalhos para uma fila específica em uma fazenda 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 para permitir a criação de um endpoint de licença

Neste exemplo, você cria uma política de escopo reduzido que concede as permissões necessárias para criar e gerenciar endpoints de licença. Use essa política para criar o endpoint de licença para a VPC associada à sua fazenda.

```
{
  "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 para permitir o monitoramento de uma fila específica da fazenda

Neste exemplo, você cria uma política de escopo reduzido que concede permissão para monitorar trabalhos em uma fila específica para uma fazenda 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 gerenciadas para Deadline Cloud

Uma política AWS gerenciada é uma política autônoma criada e administrada por AWS. AWS as políticas gerenciadas são projetadas para fornecer permissões para muitos casos de uso comuns, para que você possa começar a atribuir permissões a usuários, grupos e funções.

Lembre-se de que as políticas AWS gerenciadas podem não conceder permissões de privilégio mínimo para seus casos de uso específicos porque elas estão disponíveis para uso de todos os AWS clientes. Recomendamos que você reduza ainda mais as permissões definindo [políticas gerenciadas pelo cliente da](#) específicas para seus casos de uso.

Você não pode alterar as permissões definidas nas políticas AWS gerenciadas. Se AWS atualizar as permissões definidas em uma política AWS gerenciada, a atualização afetará todas as identidades principais (usuários, grupos e funções) às quais a política está anexada. AWS é mais provável que atualize uma política AWS gerenciada quando uma nova AWS service (Serviço da AWS) é lançada ou novas operações de API são disponibilizadas para serviços existentes.

Para obter mais informações, consulte [Políticas gerenciadas pela AWS](#) no Guia do usuário do IAM.

### AWS política gerenciada: AWSDeadlineCloud-FleetWorker

Você pode anexar a `AWSDeadlineCloud-FleetWorker` política às suas identidades AWS Identity and Access Management (IAM).

Essa política concede aos trabalhadores dessa frota as permissões necessárias para se conectar e receber tarefas do serviço.

#### Detalhes de permissão

Esta política inclui as seguintes permissões:

- `deadline`— Permite que os diretores gerenciem os trabalhadores em uma frota.

Para obter uma lista JSON dos detalhes da política, consulte [AWSDeadlineCloud- FleetWorker](#) no guia de referência da AWS Managed Policy.

## AWS política gerenciada: AWSDeadlineCloud-WorkerHost

É possível anexar a política `AWSDeadlineCloud-WorkerHost` a suas identidades do IAM.

Essa política concede as permissões necessárias para se conectar inicialmente ao serviço. Ele pode ser usado como um perfil de instância do Amazon Elastic Compute Cloud (Amazon EC2).

### Detalhes de permissão

Esta política inclui as seguintes permissões:

- `deadline`— Permite que os diretores criem trabalhadores.

Para obter uma lista JSON dos detalhes da política, consulte [AWSDeadlineCloud- WorkerHost](#) no guia de referência da AWS Managed Policy.

## AWS política gerenciada: AWSDeadlineCloud-UserAccessFarms

É possível anexar a política `AWSDeadlineCloud-UserAccessFarms` a suas identidades do IAM.

Essa política permite que os usuários acessem os dados da fazenda com base nas fazendas das quais são membros e em seu nível de associação.

### Detalhes de permissão

Esta política inclui as seguintes permissões:

- `deadline`— Permite que o usuário acesse os dados da fazenda.
- `ec2`— Permite que os usuários vejam detalhes sobre os tipos de instância do Amazon EC2.
- `identitystore`— Permite que os usuários vejam nomes de usuários e grupos.

Para obter uma lista JSON dos detalhes da política, consulte [AWSDeadlineCloud- UserAccess Farms](#) no guia de referência da AWS Managed Policy.

## AWS política gerenciada: AWSDeadlineCloud-UserAccessFleets

É possível anexar a política `AWSDeadlineCloud-UserAccessFleets` a suas identidades do IAM.

Essa política permite que os usuários acessem os dados da frota com base nas fazendas das quais são membros e em seu nível de associação.

#### Detalhes de permissão

Esta política inclui as seguintes permissões:

- `deadline`— Permite que o usuário acesse os dados da fazenda.
- `ec2`— Permite que os usuários vejam detalhes sobre os tipos de instância do Amazon EC2.
- `identitystore`— Permite que os usuários vejam nomes de usuários e grupos.

Para obter uma lista JSON dos detalhes da política, consulte [AWSDeadlineCloud- UserAccess Frotas](#) no guia de referência da AWS Managed Policy.

#### AWS política gerenciada: AWSDeadlineCloud-UserAccessJobs

É possível anexar a política `AWSDeadlineCloud-UserAccessJobs` a suas identidades do IAM.

Essa política permite que os usuários acessem os dados do trabalho com base nas fazendas das quais são membros e em seu nível de associação.

#### Detalhes de permissão

Esta política inclui as seguintes permissões:

- `deadline`— Permite que o usuário acesse os dados da fazenda.
- `ec2`— Permite que os usuários vejam detalhes sobre os tipos de instância do Amazon EC2.
- `identitystore`— Permite que os usuários vejam nomes de usuários e grupos.

Para obter uma lista JSON dos detalhes da política, consulte [AWSDeadlineCloud- Vagas no UserAccess guia](#) de referência de políticas gerenciadas da AWS.

#### AWS política gerenciada: AWSDeadlineCloud-UserAccessQueues

É possível anexar a política `AWSDeadlineCloud-UserAccessQueues` a suas identidades do IAM.

Essa política permite que os usuários acessem os dados da fila com base nas fazendas das quais são membros e em seu nível de associação.

## Detalhes de permissão

Esta política inclui as seguintes permissões:

- `deadline`— Permite que o usuário acesse os dados da fazenda.
- `ec2`— Permite que os usuários vejam detalhes sobre os tipos de instância do Amazon EC2.
- `identitystore`— Permite que os usuários vejam nomes de usuários e grupos.

Para obter uma lista JSON dos detalhes da política, consulte [AWSDeadlineCloud-UserAccessQueues](#) no guia de referência da AWS Managed Policy.

## Atualizações do Deadline Cloud para políticas AWS gerenciadas

Veja detalhes sobre as atualizações das políticas AWS gerenciadas do Deadline Cloud desde que esse serviço começou a monitorar essas mudanças. Para receber alertas automáticos sobre alterações nessa página, assine o feed RSS na página de histórico de documentos do Deadline Cloud.

Alteração	Descrição	Data
O Deadline Cloud começou a monitorar as mudanças	O Deadline Cloud começou a monitorar as mudanças em suas políticas AWS gerenciadas.	2 de abril de 2024

## Solução de problemas de identidade e acesso ao AWS Deadline Cloud

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o Deadline Cloud e o IAM.

### Tópicos

- [Não estou autorizado a realizar uma ação no Deadline Cloud](#)
- [Não estou autorizado a realizar iam: PassRole](#)

- [Quero permitir que pessoas de fora da minha acessem meus Conta da AWS recursos do Deadline Cloud](#)

## Não estou autorizado a realizar uma ação no Deadline Cloud

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo `my-example-widget` fictício, mas não tem as permissões `deadline:GetWidget` fictícias.

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

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso `my-example-widget` usando a ação `deadline:GetWidget`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

## Não estou autorizado a realizar iam: PassRole

Se você receber um erro informando que não está autorizado a realizar a `iam:PassRole` ação, suas políticas devem ser atualizadas para permitir que você passe uma função para o Deadline Cloud.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, é preciso ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando um usuário do IAM chamado `marymajor` tenta usar o console para realizar uma ação no Deadline Cloud. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

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

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

## Quero permitir que pessoas de fora da minha acessem meus Conta da AWS recursos do Deadline Cloud

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem compatibilidade com políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Deadline Cloud é compatível com esses recursos, consulte [Como o Deadline Cloud funciona com o IAM](#).
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como [fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui](#) no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como [fornecer acesso Contas da AWS a terceiros](#) no Guia do usuário do IAM.
- Para saber como conceder acesso por meio da federação de identidades, consulte [Conceder acesso a usuários autenticados externamente \(federação de identidades\)](#) no Guia do usuário do IAM.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Acesso a [recursos entre contas no IAM no Guia do](#) usuário do IAM.

## Validação de conformidade para Deadline Cloud


Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte [Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS](#) e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de [AWS conformidade Programas AWS](#) de .



Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte [Baixar relatórios em AWS Artifact](#).

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- [Guias de início rápido sobre segurança e conformidade](#) — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.
- [Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services](#) — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

 Note

Nem todos Serviços da AWS são elegíveis para a HIPAA. Para mais informações, consulte a [Referência dos serviços qualificados pela HIPAA](#).

- AWS Recursos de <https://aws.amazon.com/compliance/resources/> de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- [AWS Guias de conformidade do cliente](#) — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- [Avaliação de recursos com regras](#) no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- [AWS Security Hub](#) — Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os recursos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a [Referência de controles do Security Hub](#).
- [Amazon GuardDuty](#) — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de

conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.

- [AWS Audit Manager](#)— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

## Resiliência em Deadline Cloud

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade. Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância. Com as zonas de disponibilidade, é possível projetar e operar aplicativos e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenters tradicionais.

Para obter mais informações sobre zonas de disponibilidade Regiões da AWS e zonas de disponibilidade, consulte [Infraestrutura AWS global](#).

AWS Deadline Cloud não faz backup dos dados armazenados em seu bucket S3 de anexos de trabalho. Você pode habilitar backups dos dados dos anexos do trabalho usando qualquer mecanismo de backup padrão do Amazon S3, [como](#) controle de versão do S3 ou [AWS Backup](#)

## Segurança da infraestrutura no Deadline Cloud

Como um serviço gerenciado, AWS o Deadline Cloud é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte [AWS Cloud Security](#). Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte [Proteção](#) de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar o Deadline Cloud pela rede. Os clientes devem oferecer suporte para:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com perfect forward secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou você pode usar o [AWS Security Token Service](#) (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

O Deadline Cloud não oferece suporte ao uso de políticas de endpoint de nuvem privada AWS PrivateLink virtual (VPC). Ele usa a política AWS PrivateLink padrão, que concede acesso total ao endpoint. Para obter mais informações, consulte [Política de endpoint padrão](#) no guia do AWS PrivateLink usuário.

## Análise de configuração e vulnerabilidade no Deadline Cloud

AWS lida com tarefas básicas de segurança, como sistema operacional (SO) convidado e aplicação de patches em bancos de dados, configuração de firewall e recuperação de desastres. Esses procedimentos foram revisados e certificados por terceiros certificados. Para obter mais detalhes, consulte os seguintes recursos da :

- [Modelo de responsabilidade compartilhada](#)
- [Amazon Web Services: visão geral do processo de segurança](#) (whitepaper)

AWS O Deadline Cloud gerencia tarefas em frotas gerenciadas por serviços ou pelo cliente:

- Para frotas gerenciadas por serviços, o Deadline Cloud gerencia o sistema operacional convidado.
- Para frotas gerenciadas pelo cliente, você é responsável por gerenciar o sistema operacional.

Para obter informações adicionais sobre configuração e análise de vulnerabilidades do AWS Deadline Cloud, consulte

- [Melhores práticas de segurança para o Deadline Cloud](#)

## Prevenção contra o ataque do “substituto confuso” em todos os serviços

“Confused deputy” é um problema de segurança no qual uma entidade sem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executá-la. Em AWS, a falsificação de identidade entre serviços pode resultar no problema confuso do deputado. A personificação entre

serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado de modo a usar suas permissões para atuar nos recursos de outro cliente de uma forma na qual ele não deveria ter permissão para acessar. Para evitar isso, a AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com entidades principais de serviço que receberam acesso aos recursos em sua conta.

Recomendamos usar as chaves de contexto de condição [aws:SourceAccount](#) global [aws:SourceArne](#) as chaves de contexto nas políticas de recursos para limitar as permissões que AWS Deadline Cloud concedem outro serviço ao recurso. Use `aws:SourceArn` se quiser apenas um recurso associado a acessibilidade de serviço. Use `aws:SourceAccount` se quiser permitir que qualquer recurso nessa conta seja associado ao uso entre serviços.

A maneira mais eficaz de se proteger contra o problema substituto confuso é usar a chave de contexto de condição global `aws:SourceArn` com o nome do recurso da Amazon (ARN) completo do recurso. Se você não souber o ARN completo do recurso ou especificar vários recursos, use a chave de condição de contexto global `aws:SourceArn` com caracteres curinga (\*) para as partes desconhecidas do ARN. Por exemplo, `.arn:aws:deadline:*:123456789012:*`

Se o valor de `aws:SourceArn` não contiver o ID da conta, como um ARN de bucket do Amazon S3, você deverá usar ambas as chaves de contexto de condição global para limitar as permissões.

O exemplo a seguir mostra como você pode usar as chaves de contexto de condição `aws:SourceAccount` global `aws:SourceArn` e as chaves de contexto Deadline Cloud para evitar o confuso problema substituto.

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

## Acesso AWS Deadline Cloud usando um endpoint de interface ()AWS PrivateLink

Você pode usar AWS PrivateLink para criar uma conexão privada entre sua VPC e AWS Deadline Cloud. Você pode acessar Deadline Cloud como se estivesse em sua VPC, sem o uso de um gateway de internet, dispositivo NAT, conexão VPN ou conexão AWS Direct Connect. As instâncias na sua VPC não precisam de endereços IP públicos para acessar o Deadline Cloud.

Você estabelece essa conectividade privada criando um endpoint de interface, desenvolvido pelo AWS PrivateLink. Criaremos um endpoint de interface de rede em cada sub-rede que você habilitar para o endpoint de interface. Estas são interfaces de rede gerenciadas pelo solicitante que servem como ponto de entrada para o tráfego destinado ao Deadline Cloud.

Para obter mais informações, consulte [Acessar os Serviços da AWS pelo AWS PrivateLink](#) no Guia do AWS PrivateLink .

## Considerações para Deadline Cloud

Antes de configurar um endpoint de interface para Deadline Cloud, consulte [Acessar um serviço da AWS usando um endpoint VPC de interface](#) no Guia AWS PrivateLink

Deadline Cloud suporta fazer chamadas para todas as suas ações de API por meio do endpoint da interface.

Por padrão, o acesso total ao Deadline Cloud é permitido por meio do endpoint da interface. Como alternativa, você pode associar um grupo de segurança às interfaces de rede do endpoint para controlar o tráfego Deadline Cloud por meio do endpoint da interface.

Deadline Cloud não oferece suporte a políticas de endpoint de VPC. Para obter mais informações, consulte [Controlar o acesso aos endpoints da VPC usando políticas de endpoint](#) no Guia AWS PrivateLink .

## Deadline Cloud endpoints

Deadline Cloud usa dois endpoints para acessar o serviço usando AWS PrivateLink.

Os trabalhadores usam o `com.amazonaws.region.deadline.scheduling` endpoint para obter tarefas da fila, relatar o progresso e enviar a Deadline Cloud saída da tarefa de volta. Se você estiver usando uma frota gerenciada pelo cliente, o endpoint de agendamento é o único endpoint que você precisa criar, a menos que esteja usando operações de gerenciamento. Por exemplo, se um trabalho criar mais trabalhos, você precisará habilitar o endpoint de gerenciamento para chamar a `CreateJob` operação.

O Deadline Cloud monitor usa o `com.amazonaws.region.deadline.management` para gerenciar os recursos em sua fazenda, como criar e modificar filas e frotas ou obter listas de trabalhos, etapas e tarefas.

Deadline Cloud também requer endpoints para os seguintes endpoints AWS de serviço:

- Deadline Cloud usa AWS STS para autenticar trabalhadores para que eles possam acessar os ativos do trabalho. Para obter mais informações sobre isso AWS STS, consulte [Credenciais de segurança temporárias no IAM](#) no Guia do AWS Identity and Access Management usuário.
- Se você configurar sua frota gerenciada pelo cliente em uma sub-rede sem conexão com a Internet, deverá criar um VPC endpoint para o CloudWatch Amazon Logs para que os trabalhadores possam gravar registros. Para obter mais informações, consulte [Monitoramento com CloudWatch](#).
- Se você usar anexos de trabalho, deverá criar um VPC endpoint para o Amazon Simple Storage Service (Amazon S3) para que os trabalhadores possam acessar os anexos. Para obter mais informações, consulte [Job attachments in. Deadline Cloud](#)

## Crie endpoints para Deadline Cloud

Você pode criar endpoints de interface para Deadline Cloud usar o console Amazon VPC ou AWS Command Line Interface o AWS CLI(). Para obter mais informações, consulte [Criar um endpoint de interface](#) no Guia do usuário do AWS PrivateLink .

Crie endpoints de gerenciamento e agendamento para Deadline Cloud usar os seguintes nomes de serviço. Substitua a *região* pela Região da AWS onde você implantou. Deadline Cloud

```
com.amazonaws.region.deadline.management
```

```
com.amazonaws.region.deadline.scheduling
```

Se você habilitar o DNS privado para os endpoints da interface, poderá fazer solicitações de API Deadline Cloud usando o nome DNS regional padrão. Por exemplo, `worker.deadline.us-east-1.amazonaws.com` para operações de trabalhadores ou `management.deadline.us-east-1.amazonaws.com` para todas as outras operações.

Você também deve criar um endpoint para AWS STS usar o seguinte nome de serviço:

```
com.amazonaws.region.sts
```

Se sua frota gerenciada pelo cliente estiver em uma sub-rede sem conexão com a Internet, você deverá criar um endpoint de CloudWatch registros usando o seguinte nome de serviço:

```
com.amazonaws.region.logs
```

Se você usar anexos de trabalho para transferir arquivos, deverá criar um endpoint do Amazon S3 usando o seguinte nome de serviço:

```
com.amazonaws.region.s3
```

## Melhores práticas de segurança para o Deadline Cloud

AWS O Deadline Cloud (Deadline Cloud) fornece vários recursos de segurança a serem considerados ao desenvolver e implementar suas próprias políticas de segurança. As melhores práticas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas melhores práticas podem não ser adequadas ou suficientes para o seu ambiente, trate-as como considerações úteis em vez de prescrições.

### Note

Para obter mais informações sobre a importância de muitos tópicos de segurança, consulte o [Modelo de Responsabilidade Compartilhada](#).

## Proteção de dados

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure contas individuais com AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados pessoais armazenados no Amazon Simple Storage Service (Amazon S3).
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou uma API, use um endpoint FIPS. Para obter mais informações sobre endpoints do FIPS, consulte [Federal Information Processing Standard \(FIPS\) 140-2](#).

É altamente recomendável que você nunca coloque informações de identificação confidenciais, como números de conta dos seus clientes, em campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com AWS o Deadline Cloud ou outro Serviços da AWS usando o console, a API ou AWS os SDKs. AWS CLI Todos os dados que você inserir no Deadline Cloud ou em outros serviços podem ser coletados para inclusão nos registros de diagnóstico. Ao fornecer um URL para um servidor externo, não inclua informações de credenciais no URL para validar a solicitação a esse servidor.

## AWS Identity and Access Management permissões

Gerencie o acesso aos AWS recursos usando usuários, funções AWS Identity and Access Management (IAM) e concedendo o mínimo de privilégios aos usuários. Estabeleça políticas e procedimentos de gerenciamento de credenciais para criar, distribuir, alternar e revogar AWS credenciais de acesso. Para obter mais informações, consulte [Práticas recomendadas de segurança no IAM](#) no Guia do usuário do IAM.



## Execute trabalhos como usuários e grupos

Ao usar a funcionalidade de fila no Deadline Cloud, é uma prática recomendada especificar um usuário do sistema operacional (OS) e seu grupo principal para que o usuário do sistema operacional tenha permissões de privilégio mínimo para os trabalhos da fila.

Quando você especifica “Executar como usuário” (e grupo), todos os processos para trabalhos enviados à fila serão executados usando esse usuário do sistema operacional e herdarão as permissões de sistema operacional associadas a esse usuário.

As configurações de frota e fila se combinam para estabelecer uma postura de segurança. No lado da fila, o “Job run as user” e o papel do IAM podem ser especificados para usar o sistema operacional e AWS as permissões para os trabalhos da fila. A frota define a infraestrutura (hosts de trabalho, redes, armazenamento compartilhado montado) que, quando associada a uma fila específica, executa trabalhos dentro da fila. Os dados disponíveis nos hosts de trabalho precisam ser acessados por trabalhos de uma ou mais filas associadas. Especificar um usuário ou grupo ajuda a proteger os dados nos trabalhos de outras filas, outros softwares instalados ou outros usuários com acesso aos hosts de trabalho. Quando uma fila está sem um usuário, ela é executada como o usuário agente que pode representar (sudo) qualquer usuário da fila. Dessa forma, uma fila sem um usuário pode escalar privilégios para outra fila.

## Redes

Para evitar que o tráfego seja interceptado ou redirecionado, é essencial proteger como e para onde seu tráfego de rede é roteado.

Recomendamos que você proteja seu ambiente de rede das seguintes maneiras:

- Proteja as tabelas de rotas de sub-rede da Amazon Virtual Private Cloud (Amazon VPC) para controlar como o tráfego da camada IP é roteado.
- Se você estiver usando o Amazon Route 53 (Route 53) como provedor de DNS na configuração de sua fazenda ou estação de trabalho, proteja o acesso à API do Route 53.
- Se você se conectar ao Deadline Cloud fora dela, por AWS exemplo, usando estações de trabalho locais ou outros data centers, proteja qualquer infraestrutura de rede local. Isso inclui servidores DNS e tabelas de rotas em roteadores, switches e outros dispositivos de rede.

## Vagas e dados de vagas

Os trabalhos do Deadline Cloud são executados em sessões em hosts de trabalhadores. Cada sessão executa um ou mais processos no host do trabalhador, que geralmente exigem a entrada de dados para produzir a saída.

Para proteger esses dados, você pode configurar os usuários do sistema operacional com filas. O agente de trabalho usa o usuário do sistema operacional de fila para executar subprocessos de sessão. Esses subprocessos herdam as permissões do usuário do sistema operacional de fila.

Recomendamos que você siga as melhores práticas para proteger o acesso aos dados que esses subprocessos acessam. Para obter mais informações, consulte o [Modelo de responsabilidade compartilhada](#).

## Estrutura da fazenda

Você pode organizar frotas e filas do Deadline Cloud de várias maneiras. No entanto, existem implicações de segurança em certos arranjos.

Uma fazenda tem um dos limites mais seguros porque não pode compartilhar recursos do Deadline Cloud com outras fazendas, incluindo frotas, filas e perfis de armazenamento. No entanto, você pode compartilhar AWS recursos externos dentro de uma fazenda, o que compromete o limite de segurança.

Você também pode estabelecer limites de segurança entre filas dentro da mesma fazenda usando a configuração apropriada.

Siga estas práticas recomendadas para criar filas seguras na mesma fazenda:

- Associe uma frota somente a filas dentro do mesmo limite de segurança. Observe o seguinte:
  - Depois que o trabalho é executado no host do trabalhador, os dados podem permanecer atrasados, como em um diretório temporário ou no diretório inicial do usuário da fila.
  - O mesmo usuário do sistema operacional executa todos os trabalhos em um host de trabalhadores de frota de propriedade do serviço, independentemente da fila para a qual você envia o trabalho.
  - Um trabalho pode deixar processos em execução em um host de trabalho, possibilitando que trabalhos de outras filas observem outros processos em execução.
- Certifique-se de que somente filas dentro do mesmo limite de segurança compartilhem um bucket do Amazon S3 para anexos de trabalhos.

- Certifique-se de que somente filas dentro do mesmo limite de segurança compartilhem um usuário do sistema operacional.
- Proteja todos AWS os outros recursos integrados à fazenda até o limite.

## Filas de anexação de trabalhos

Os anexos de trabalho são associados a uma fila, que usa seu bucket do Amazon S3.

- Os anexos do trabalho são gravados e lidos a partir de um prefixo raiz no bucket do Amazon S3. Você especifica esse prefixo raiz na chamada da `CreateQueue` API.
- O bucket tem um `correspondenteQueue Role`, que especifica a função que concede aos usuários da fila acesso ao bucket e ao prefixo raiz. Ao criar uma fila, você especifica o `Queue Role` Amazon Resource Name (ARN) junto com o bucket de anexos do trabalho e o prefixo raiz.
- As chamadas autorizadas para `oAssumeQueueRoleForRead`, `AssumeQueueRoleForUser`, e as operações `AssumeQueueRoleForWorker` da API retornam um conjunto de credenciais de segurança temporárias para o `Queue Role`

Se você criar uma fila e reutilizar um bucket e um prefixo raiz do Amazon S3, há o risco de as informações serem divulgadas a terceiros não autorizados. Por exemplo, `QueueA` e `QueueB` compartilham o mesmo bucket e prefixo raiz. Em um fluxo de trabalho seguro, o Artista tem acesso ao `QueueA`, mas não ao `QueueB`. No entanto, quando várias filas compartilham um intervalo, o Artista pode acessar os dados nos dados do `QueueB` porque usa o mesmo intervalo e prefixo raiz do `QueueA`.

O console configura filas que são seguras por padrão. Certifique-se de que as filas tenham uma combinação distinta de bucket e prefixo raiz do Amazon S3, a menos que façam parte de um limite de segurança comum.

Para isolar suas filas, você deve configurar o `Queue Role` para permitir apenas o acesso da fila ao bucket e ao prefixo raiz. No exemplo a seguir, substitua cada *espaço reservado* pelas informações específicas do seu 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/*"
}
]
}

```

Você também deve definir uma política de confiança para a função. No exemplo a seguir, substitua o texto do *espaço reservado* pelas informações específicas do 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"
      }
    }
  }
]
}

```

## Software personalizado: buckets Amazon S3

Você pode adicionar a seguinte declaração à sua Queue Role para acessar o software personalizado em seu bucket do Amazon S3. No exemplo a seguir, substitua *SOFTWARE\_BUCKET\_NAME* pelo nome do seu bucket do S3.

```

"Statement": [
  {
    "Action": [
      "s3:GetObject",
      "s3:ListBucket"
    ],
    "Effect": "Allow",
    "Resource": [
      "arn:aws:s3::SOFTWARE_BUCKET_NAME",
      "arn:aws:s3::SOFTWARE_BUCKET_NAME/*"
    ]
  }
]

```

Para obter mais informações sobre as melhores práticas de segurança do Amazon S3, consulte Melhores práticas de [segurança para o Amazon S3](#) no Guia do usuário do Amazon Simple Storage Service.

## Trabalhadores anfitriões

Hospedagem segura de trabalhadores para ajudar a garantir que cada usuário só possa realizar operações para a função atribuída.

Recomendamos as seguintes melhores práticas para proteger os anfitriões dos trabalhadores:

- Não use o mesmo `jobRunAsUser` valor com várias filas, a menos que os trabalhos enviados a essas filas estejam dentro do mesmo limite de segurança.
- Não defina a fila `jobRunAsUser` com o nome do usuário do sistema operacional com o qual o agente de trabalho é executado.
- Conceda aos usuários da fila as permissões de sistema operacional menos privilegiadas necessárias para as cargas de trabalho de fila pretendidas. Certifique-se de que eles não tenham permissões de gravação do sistema de arquivos para arquivos de programas do agente de trabalho ou outro software compartilhado.
- Certifique-se de que somente o usuário `root` Linux e a conta `Administrator` proprietária estejam ativos Windows e possam modificar os arquivos do programa do agente de trabalho.
- Em hosts de Linux trabalho, considere configurar uma `umask` substituição `/etc/sudoers` que permita ao usuário do agente de trabalho iniciar processos como usuários da fila. Essa configuração ajuda a garantir que outros usuários não possam acessar arquivos gravados na fila.
- Conceda a indivíduos confiáveis acesso com menos privilégios aos anfitriões dos trabalhadores.
- Restrinja as permissões aos arquivos de configuração de substituição do DNS local (`/etc/hosts` ativados Linux e `C:\Windows\system32\etc\hosts` ativados) e para rotear tabelas em estações de trabalho e sistemas operacionais de host de trabalho. Windows
- Restrinja as permissões à configuração de DNS em estações de trabalho e sistemas operacionais de host de trabalho.
- Corrija regularmente o sistema operacional e todo o software instalado. Essa abordagem inclui software usado especificamente com o Deadline Cloud, como remetentes, adaptadores, agentes de trabalho, OpenJD pacotes e outros.
- Use senhas fortes para a Windows fila. `jobRunAsUser`
- Alterne regularmente as senhas da sua fila `jobRunAsUser`.
- Garanta o menor privilégio de acesso aos segredos da Windows senha e exclua os segredos não utilizados.
- Não dê `jobRunAsUser` permissão à fila para que os comandos `schedule` sejam executados no futuro:
  - `AtivadoLinux`, negue a essas contas o acesso a `cron` at e.
  - `AtivadoWindows`, negue o acesso dessas contas ao agendador de Windows tarefas.

**Note**

Para obter mais informações sobre a importância de corrigir regularmente o sistema operacional e o software instalado, consulte o [Modelo de Responsabilidade Compartilhada](#).

## Estações de trabalho

É importante proteger as estações de trabalho com acesso ao Deadline Cloud. Essa abordagem ajuda a garantir que qualquer trabalho que você enviar para o Deadline Cloud não possa executar cargas de trabalho arbitrárias cobradas de você. Conta da AWS

Recomendamos as seguintes melhores práticas para proteger as estações de trabalho de artistas. Para mais informações, consulte o [.Modelo de responsabilidade compartilhada da](#) .

- Proteja todas as credenciais persistentes que fornecem acesso ao Deadline Cloud AWS, incluindo o Deadline Cloud. Para obter mais informações, consulte [Gerenciamento de chaves de acesso de usuários do IAM](#) no Guia do usuário do IAM.
- Instale somente software confiável e seguro.
- Exija que os usuários se federem com um provedor de identidade para acessar AWS com credenciais temporárias.
- Use permissões seguras nos arquivos do programa de envio do Deadline Cloud para evitar adulterações.
- Conceda a indivíduos de confiança acesso menos privilegiado às estações de trabalho de artistas.
- Use somente remetentes e adaptadores obtidos por meio do Deadline Cloud Monitor.
- Restrinja as permissões `/etc/hosts` e as tabelas de roteamento em estações de trabalho e sistemas operacionais de host de trabalho.
- Restrinja as permissões `/etc/resolv.conf` em estações de trabalho e sistemas operacionais hospedeiros de trabalhadores.
- Corrija regularmente o sistema operacional e todo o software instalado. Essa abordagem inclui software usado especificamente com o Deadline Cloud, como remetentes, adaptadores, agentes de trabalho, OpenJD pacotes e outros.

# Nuvem de AWS prazos de monitoramento

O monitoramento é uma parte importante para manter a confiabilidade, a disponibilidade e o desempenho do AWS Deadline Cloud (Deadline Cloud) e de suas AWS soluções. Colete dados de monitoramento de todas as partes da sua AWS solução para que você possa depurar com mais facilidade uma falha multiponto, caso ocorra. Antes de começar a monitorar o Deadline Cloud, você deve criar um plano de monitoramento que inclua respostas às seguintes perguntas:

- Quais são seus objetivos de monitoramento?
- Quais recursos você vai monitorar?
- Com que frequência você vai monitorar esses recursos?
- Quais ferramentas de monitoramento você usará?
- Quem realizará o monitoramento das tarefas?
- Quem deve ser notificado quando algo der errado?

AWS e o Deadline Cloud fornecem ferramentas que você pode usar para monitorar seus recursos e responder a possíveis incidentes. Algumas dessas ferramentas fazem o monitoramento para você, outras requerem intervenção manual. Você deve automatizar as tarefas de monitoramento o máximo possível.

- A Amazon CloudWatch monitora seus AWS recursos e os aplicativos em que você executa AWS em tempo real. É possível coletar e rastrear métricas, criar painéis personalizados e definir alarmes que o notificam ou que realizam ações quando uma métrica especificada atinge um limite definido. Por exemplo, você pode CloudWatch rastrear o uso da CPU ou outras métricas de suas instâncias do Amazon EC2 e iniciar automaticamente novas instâncias quando necessário. Para obter mais informações, consulte o [Guia CloudWatch do usuário da Amazon](#).

O Deadline Cloud tem três CloudWatch métricas.

- O Amazon CloudWatch Logs permite que você monitore, armazene e acesse seus arquivos de log a partir de instâncias do Amazon EC2 e de outras fontes. CloudTrail CloudWatch Os registros podem monitorar as informações nos arquivos de log e notificá-lo quando determinados limites forem atingidos. É possível também arquivar seus dados de log em armazenamento resiliente. Para obter mais informações, consulte o [Guia do usuário do Amazon CloudWatch Logs](#).
- A Amazon EventBridge pode ser usada para automatizar seus AWS serviços e responder automaticamente a eventos do sistema, como problemas de disponibilidade de aplicativos ou



alterações de recursos. Os eventos dos AWS serviços são entregues quase EventBridge em tempo real. Você pode escrever regras simples para indicar quais eventos são do seu interesse, e as ações automatizadas a serem tomadas quando um evento corresponder à regra. Para obter mais informações, consulte o [Guia EventBridge do usuário da Amazon](#).

- AWS CloudTrail captura chamadas de API e eventos relacionados feitos por ou em nome de sua AWS conta e entrega os arquivos de log para um bucket do Amazon S3 que você especificar. Você pode identificar quais usuários e contas ligaram AWS, o endereço IP de origem a partir do qual as chamadas foram feitas e quando elas ocorreram. Para mais informações, consulte o [Guia do usuário do AWS CloudTrail](#).

## Tópicos

- [Registrando chamadas com CloudTrail](#)
- [Monitoramento com CloudWatch](#)
- [Atuando em EventBridge eventos](#)

## Registrando chamadas com CloudTrail

AWS O Deadline Cloud é integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, função ou AWS service (Serviço da AWS) no Deadline Cloud. CloudTrail captura todas as chamadas de API para o Deadline Cloud como eventos. As chamadas capturadas incluem chamadas do console do Deadline Cloud e chamadas de código para as operações da API Deadline Cloud.

Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o Deadline Cloud. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita à Deadline Cloud, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Para saber mais sobre isso CloudTrail, consulte o [Guia AWS CloudTrail do usuário](#).

## Informações do Deadline Cloud em CloudTrail

CloudTrail é ativado no seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no Deadline Cloud, essa atividade é registrada em um CloudTrail evento junto com outros AWS service

(Serviço da AWS) eventos no histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes no seu Conta da AWS. Para obter mais informações, consulte [Visualização de eventos com histórico de CloudTrail eventos](#).

CloudTrail também registra eventos quando os usuários fazem login no monitor do Deadline Cloud e recebem AWS credenciais. Quando um usuário faz login, há um CloudTrail evento com a fonte `signin.amazonaws.com` e o nome `UserAuthentication`. Há um segundo evento quando o usuário conectado recebe as AWS credenciais da fonte `sts.amazonaws.com` e do nome `AssumeRole`. O ID do usuário é registrado em um segundo evento dentro do nome da sessão da função.

Para um registro contínuo dos eventos em seu Conta da AWS, incluindo eventos do Deadline Cloud, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, ela é aplicada a todas as Regiões da AWS. A trilha registra eventos de todas as regiões na AWS partição e entrega os arquivos de log ao bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros Serviços da AWS para analisar e agir com base nos dados do evento coletados nos CloudTrail registros.

Para mais informações, consulte:

[Visão geral da criação de uma trilha](#)

[CloudTrail serviços e integrações suportados](#)

[Configurando notificações do Amazon SNS para CloudTrail](#)

[Recebendo arquivos de CloudTrail log de várias regiões](#)

[Recebendo arquivos de CloudTrail log de várias contas](#)

O Deadline Cloud suporta o registro das seguintes ações como eventos em arquivos de CloudTrail log:

- [associate-member-to-farm](#)
- [associate-member-to-fleet](#)
- [associate-member-to-job](#)
- [associate-member-to-queue](#)
- [assume-fleet-role-for-leia](#)

- [assume-fleet-role-for-trabalhador](#)
- [assume-queue-role-for-leia](#)
- [assume-queue-role-for-usuário](#)
- [assume-queue-role-for-trabalhador](#)
- [criar orçamento](#)
- [criar fazenda](#)
- [create-fleet](#)
- [create-license-endpoint](#)
- [criar monitorar](#)
- [criar fila](#)
- [create-queue-environment](#)
- [create-queue-fleet-association](#)
- [create-storage-profile](#)
- [criar trabalhador](#)
- [excluir orçamento](#)
- [delete-farm](#)
- [delete-fleet](#)
- [delete-license-endpoint](#)
- [delete-metered-product](#)
- [excluir monitor](#)
- [fila de exclusão](#)
- [delete-queue-environment](#)
- [delete-queue-fleet-association](#)
- [delete-storage-profile](#)
- [excluir trabalhador](#)
- [disassociate-member-from-farm](#)
- [disassociate-member-from-fleet](#)
- [disassociate-member-from-job](#)
- [disassociate-member-from-queue](#)

- [get-application-version](#)
- [obter orçamento](#)
- [get-farm](#)
- [get-feature-map](#)
- [obtenha a frota](#)
- [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-fila](#)
- [list-available-metered-products](#)
- [orçamentos de lista](#)
- [list-farm-members](#)
- [listas de fazendas](#)
- [list-fleet-members](#)
- [listas de frotas](#)
- [list-job-members](#)
- [list-license-endpoints](#)
- [list-metered-products](#)
- [monitores de lista](#)
- [list-queue-environments](#)
- [list-queue-fleet-associations](#)
- [list-queue-members](#)
- [filas de listas](#)
- [list-storage-profiles](#)
- [list-storage-profiles-for-fila](#)

- [list-tags-for-resource](#)
- [put-metered-product](#)
- [start-sessions-statistics-aggregation](#)
- [tag-resource](#)
- [untag-resource](#)
- [atualizar o orçamento](#)
- [atualize-farm](#)
- [atualizar frota](#)
- [monitor de atualização](#)
- [fila de atualização](#)
- [update-queue-environment](#)
- [update-queue-fleet-association](#)
- [update-storage-profile](#)
- [operador de atualização](#)

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com credenciais de usuário root ou AWS Identity and Access Management (IAM).
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro serviço da .

Para obter mais informações, consulte o [elemento Identidade CloudTrail do usuário](#).

## Compreendendo as entradas do arquivo de log do Deadline Cloud

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contém uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte e inclui informações sobre a ação solicitada, a data e a hora da ação, os parâmetros da solicitação e assim por diante.

CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das chamadas públicas de API, portanto, eles não aparecem em nenhuma ordem específica.

Este exemplo de JSON mostra o log gerado por uma chamada para a **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",
}
```

O exemplo mostra a AWS região, o endereço IP e outros "requestParameters", como "" e displayName "kmsKeyArn", que podem ajudar você a identificar o evento.

## Monitoramento com CloudWatch

A Amazon CloudWatch (CloudWatch) coleta dados brutos e os processa em métricas legíveis, quase em tempo real. Você pode abrir o CloudWatch console em <https://console.aws.amazon.com/cloudwatch/> para ver e filtrar as métricas do Deadline Cloud.

- Em uma frota gerenciada pelo cliente do Deadline Cloud, CloudWatch envia duas métricas UnhealthyWorkerCount e RecommendedFleetSize
- O namespace para essas métricas é AWS/DeadlineCloud.
- Você pode usar as dimensões farmID e fleetID filtrar métricas.
- Ambas as métricas usam a unidadecount.

Essas estatísticas são mantidas por 15 meses para que você possa acessar informações históricas para ter uma melhor perspectiva sobre o desempenho de seu aplicativo ou serviço web. Você também pode definir alarmes que observam determinados limites e enviam notificações ou realizam ações quando esses limites são atingidos. Para obter mais informações, consulte o [Guia CloudWatch do usuário da Amazon](#).

O Deadline Cloud tem dois tipos de registros: registros de tarefas e registros de trabalhadores. Um registro de tarefas é quando você executa registros de execução como um script ou como um DCC é executado. Um registro de tarefas pode mostrar eventos como carregamento de ativos, renderização de blocos ou texturas não encontradas.

Um registro de trabalho mostra os processos do agente de trabalho. Isso pode incluir coisas como quando os agentes de trabalho são inicializados, se registram, relatam o progresso, carregam configurações ou concluem tarefas.

Para o Deadline Cloud, os trabalhadores fazem o upload desses registros para o CloudWatch Logs. Por padrão, os registros nunca expiram. Se um trabalho gerar um grande volume de dados, você poderá incorrer em custos extras. Para obter mais informações, consulte os [CloudWatch preços da Amazon](#).

Você pode ajustar a política de retenção para cada grupo de registros. Uma retenção mais curta remove registros antigos e pode ajudar a reduzir os custos de armazenamento. Para manter os registros, você pode arquivá-los no Amazon Simple Storage Service antes de remover o registro. Para obter mais informações, consulte [Exportar dados de log para o Amazon S3 usando o console no guia CloudWatch](#) do usuário da Amazon.

#### Note

CloudWatch as leituras de registro são limitadas por AWS. Se você planeja contratar muitos artistas, sugerimos que entre em contato com o suporte AWS ao cliente e solicite um aumento na `GetLogEvents` cota. Além disso, recomendamos que você feche o portal de rastreamento de registros quando não estiver depurando.

Para obter mais informações, consulte [CloudWatch Registrar cotas](#) no guia do CloudWatch usuário da Amazon.

## Atuando em EventBridge eventos

O Deadline Cloud envia eventos EventBridge para a Amazon para notificá-lo sobre mudanças no estado do serviço. Você pode usar EventBridge esses eventos para escrever regras que atuem, como notificá-lo, quando houver uma mudança em sua frota. Para obter mais informações, consulte [O que é a Amazon EventBridge](#)

## Alteração na recomendação do tamanho da frota

Quando você configura sua frota para usar o escalonamento automático baseado em eventos, o Deadline Cloud envia eventos que você pode usar para gerenciar suas frotas. Cada um desses eventos contém informações sobre o tamanho atual e o tamanho solicitado de uma frota. Para ver um exemplo de uso de um EventBridge evento e um exemplo de função Lambda para lidar



com o evento, consulte. [Escale automaticamente sua frota do Amazon EC2 com o recurso de recomendação de escala Deadline Cloud](#)

O evento de alteração da recomendação de tamanho da frota é enviado quando ocorre o seguinte:

- Quando o tamanho recomendado da frota muda e `oldFleetSize` é diferente de `newFleetSize`.
- Quando o serviço detecta que o tamanho real da frota não corresponde ao tamanho recomendado. Você pode obter o tamanho real da frota `workerCount` na resposta da [GetFleet](#) operação. Isso pode acontecer quando uma instância ativa do Amazon EC2 não consegue se registrar como funcionária do Deadline Cloud.

O evento tem o seguinte 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,
  }
}
```

Os campos a seguir definem o padrão do evento:

`"source": "aws.deadline"`

Identifica que a origem desse evento é Deadline Cloud.

`"detail-type": "Fleet Size Recommendation Change"`

Identifica o tipo de evento.

`"detail": { }`

Fornece informações sobre as mudanças recomendadas no tamanho da frota.

```
"farmId": "farm-1234567890000000000000000000000000"
```

O identificador da fazenda que contém a frota.

```
"fleetId": "fleet-1234567890000000000000000000000000"
```

O identificador da frota que precisa de uma mudança de tamanho.

```
"oldFleetSize": 1
```

O tamanho atual da frota.

```
"newFleetSize": 5
```

O novo tamanho recomendado da frota.

# Cotas para Deadline Cloud

AWS Deadline Cloud fornece recursos, como fazendas, frotas e filas, que você pode usar para processar trabalhos. Quando você cria sua Conta da AWS, definimos cotas padrão desses recursos para cada uma das Regiões da AWS.

Service Quotas é um local central onde você pode visualizar e gerenciar suas cotas. Serviços da AWS Você também pode solicitar um aumento de cota para muitos dos recursos que você usa.

Para ver as cotas de Deadline Cloud, abra o console [Service Quotas](#). No painel de navegação, escolha Serviços da AWS e selecione Deadline Cloud.

Para solicitar um aumento da cota, consulte [Requesting a quota increase](#) no Guia do usuário do Service Quotas. Se a cota ainda não estiver disponível nas Cotas de Serviço, use [o formulário de aumento da cota de serviço](#).

# Criando recursos AWS do Deadline Cloud com AWS CloudFormation

AWS O Deadline Cloud está integrado com AWS CloudFormation, um serviço que ajuda você a modelar e configurar seus AWS recursos para que você possa gastar menos tempo criando e gerenciando seus recursos e infraestrutura. Você cria um modelo que descreve todos os AWS recursos que você deseja (como fazendas, filas e frotas) e AWS CloudFormation provisiona e configura esses recursos para você.

Ao usar AWS CloudFormation, você pode reutilizar seu modelo para configurar seus recursos do Deadline Cloud de forma consistente e repetida. Descreva seus recursos uma vez e, em seguida, provisione os mesmos recursos repetidamente em várias Contas da AWS regiões.

## Deadline Cloud e AWS CloudFormation modelos

Para provisionar e configurar recursos para o Deadline Cloud e serviços relacionados, você deve entender [AWS CloudFormation os modelos](#). Os modelos são arquivos de texto formatados em JSON ou YAML. Esses modelos descrevem os recursos que você deseja provisionar em suas AWS CloudFormation pilhas. Se você não estiver familiarizado com JSON ou YAML, você pode usar o AWS CloudFormation Designer para ajudá-lo a começar a usar modelos. AWS CloudFormation Para obter mais informações, consulte [O que é o Designer AWS CloudFormation ?](#) no Manual do usuário do AWS CloudFormation .

O Deadline Cloud suporta a criação de fazendas, filas e frotas em. AWS CloudFormationPara obter mais informações, incluindo exemplos de modelos JSON e YAML para fazendas, filas e frotas, consulte o [AWS Deadline Cloud](#) no Guia do usuário.AWS CloudFormation

## Saiba mais sobre AWS CloudFormation

Para saber mais sobre isso AWS CloudFormation, consulte os seguintes recursos:

- [AWS CloudFormation](#)
- [AWS CloudFormation Guia do usuário](#)
- [AWS CloudFormation API Reference](#)
- [AWS CloudFormation Guia do usuário da interface de linha de comando](#)

# Histórico de documentos do guia do usuário do Deadline Cloud

A tabela a seguir descreve mudanças importantes em cada versão do guia do usuário do AWS Deadline Cloud.

Alteração	Descrição	Data
<a href="#">Lançamento inicial</a>	Esta é a versão inicial do guia do usuário do Deadline Cloud.	2 de abril de 2024

# AWS Glossário

Para obter a AWS terminologia mais recente, consulte o [AWS glossário](#) na Glossário da AWS Referência.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.